Groupes, Anneaux, Corps

Table des matières

Table des matières

1 Un peu d'histoire

Dès le deuxième millénaire avant l'ère chrétienne, on résolvait des problèmes sans disposer du formalisme des équations et des inconnues.

Diophante d'Alexandrie, qui vécut du début à la fin du troisième siècle, inventa la notion d'inconnue. On appelle en son honneur *équations diophantiennes* les équations entre polynômes à coefficients entiers (ou rationnels, ce qui est équivalent par réduction à un dénominateur commun) dont les solutions sont entières.

Les travaux de Diophante furent repris, au neuvième siècle, par le grand mathématicien perse Al Khawarizmi (780-850), à qui l'on doit des avancées en Algèbre, l'introduction du zéro indien, et, entre autres, la systématisation de la notion d'*algorithme* (qui lui doit son nom). Il appelait l'inconnue la *chose*, ce qui est à l'origine, après traduction, de la notation «X». Une simple notation peut être à l'origine d'une avancée importante en facilitant ou en permettant certains calculs, comme les nombres complexes d'Euler ou les conventions d'Einstein.

La structure de groupe est la structure de base en algèbre et elle est fondamentale dans nombre de domaines scientifiques ; pensons aux groupes de transformation, d'isométries, à la cristallographie, à la chimie, à la physique subatomique, à l'automatique...Une géométrie est définie par un groupe de transformations (le groupe orthogonal pour la géométrie euclidienne, le groupe de Lorentz pour la Relativité, etc.)

La notion de groupe était implicite bien avant Cauchy (1789-1857), chez les Grecs et les Arabes. Lagrange (1736-1813) démontre en 1770 que l'ordre d'un groupe est divisible par l'ordre de chacun de ses sous-groupes. Cauchy introduit le groupe des permutations des racines. Les travaux de Gauss (1777-1855), qui remarque que les groupes ne sont pas tous cycliques, d'Abel (1802-1829), de Galois (1811-1832), de Cayley (1821-1895) qui introduit la notion de groupe abstrait, défini par sa structure et non par ses éléments, sont poursuivis par le norvégien Sylow (1832-1918), qui décompose tout groupe fini en sous-groupes élémentaires. Il faut également citer plus particulièrement Mathieu (1835-1890) et les groupes éponymes (dont l'un intervient en théorie des codes), Jordan (1838-1921) et son **Traité des substitutions et des équations algébriques**, Sophus-Lie (1842-1899) et les groupes de Lie, Klein (1849-1925), etc.

Des progrès considérables ont été accomplis après 1950, et les recherches actuelles sont intenses.

Les anneaux ont été introduits, à partir de l'arithmétique, par les mathématiciens Allemands Kummer (1810-1893), Kronecker (1823-1891), Dedekind (1831-1916), à qui on doit le mot *corps*, Hilbert (1862-1943).

Galois (1811-1832) considérait déjà, mais sans le nommer, le corps des racines d'une équation.

Citons aussi les remarquables travaux d'axiomatisation d'Emmy Noether (1882-1935).

2 Groupes

2.1 Définitions

Un **groupe** est un couple $(G, *)$, formé d'un ensemble non vide G, et d'une loi de composition « $*$ » qui associe à deux éléments du groupe un élément du groupe :

$$\begin{array}{ccc} G \times G & \to & G \\ (g_1, g_2) & \mapsto & g_1 * g_2 \end{array}$$

et qui possède les propriétés suivantes, pour tous éléments écrits :

- elle est associative : $(g_1 * g_2) * g_3 = g_1 * (g_2 * g_3)$, ce qui permet de supprimer les parenthèses,
- il existe un élément **neutre** « e » :

$$\forall g \in G,\ e * g = g * e = g,$$

- à tout élément g correspond un **inverse** noté « g^{-1} » :

$$g^{-1} * g = g * g^{-1} = e.$$

Notons bien que l'inverse est unique, que e est son propre inverse, que l'inverse de $g_1 * g_2$ est $g_2^{-1} * g_1^{-1}$ et enfin que le neutre est forcément unique : si e_1 et e_2 sont neutres, on a, d'après la définition : $e_1 * e_2 = e_1 = e_2$.

Une surjection ϕ d'un groupe G, de neutre e, sur un ensemble E permet de munir E d'une structure de groupe par **transport de structure** en choisissant pour chaque $x \in E$ un élément de $\phi^{-1}(x)$, noté $\phi^{-1}(x)^\circ$,en posant :

$$\forall (x, x') \in E \times E : x * x' = \phi(\phi^{-1}(x)^\circ \phi^{-1}(x')^\circ)$$

et sous réserve que le résultat ne dépende pas du choix de $\phi^{-1}(x)^\circ$ et de $\phi^{-1}(x')^\circ$.

Si ϕ est bijective, cette condition est remplie.

Le neutre est $\phi(e)$ et l'inverse de x est $\phi((\phi^{-1}(x))^{-1})$, quel que soit le choix de $\phi^{-1}(x)$.

Un **semi-groupe** est un couple $(E, *)$ vérifiant les conditions de définition d'un groupe sauf l'existence d'un inverse pour tout élément. L'ensemble $\mathbb{N}$ des entiers naturels muni de l'addition est un semi-groupe.

Un groupe est généralement noté G, sauf si la précision $(G, *)$ est indispensable. Il est **commutatif**, ou **abélien**, si, quels que soient les éléments écrits, on a :

$$g_1 * g_2 = g_2 * g_1.$$

Il arrive que l'on utilise la notation multiplicative « $\times$», la notation de composition « $\circ$»... ou aucun symbole. On note le neutre «1», « I»... selon le contexte. On définit, pour $g \in G$, g^n comme étant le produit de n facteurs égaux à g.

Lorsque le groupe est commutatif, on choisit souvent la notation additive : l'opération est notée « + », le neutre « 0 » et l'inverse de g, ou l'opposé dans ce cas, «$-g$ ». On définit ng comme étant la somme de n termes égaux à g.

Les deux notations sont évidemment équivalentes.

Dans la suite, nous ne considérerons que les groupes finis, c'est-à-dire ayant un nombre fini d'éléments ; ce nombre, appelé pour un ensemble son **cardinal**, noté $\mathrm{Card}(E)$, ou $|E|$, est l'**ordre** du groupe G, noté $|G|$.

Soit g un élément d'un groupe et G l'ensemble des puissances de g :

$$\begin{aligned} G &= \{g^n \,|\, n \in \mathbb{Z},\, g^0 = e\} \text{ (notation multiplicative)}, \\ G &= \{ng \,|\, n \in \mathbb{Z},\, 0_{\mathbb{Z}}\, g = 0_G\} \text{ (notation additive)}. \end{aligned}$$

On vérifie immédiatement que G est un groupe. Ou bien ces puissances sont toutes distinctes et $|G|$ est infini dénombrable, ou bien il existe des entiers k tels que pour tout n on ait $g^{n+k} = g^n$, ce qui implique que :

$$g^{n+hk} = g^{n+(h-1)k} = \ldots = g^n$$

pour un entier relatif h quelconque. Il existe alors des entiers strictement positifs vérifiant la condition, et soit k_0 le plus petit d'entre eux (une partie non vide de $\mathbb{N}$ possède un plus petit élément).

On a évidemment $g^{k_0} = g^0 = e$ et $g^{-k_0} = g^0 = e$; k_0 est l'ordre de G , et aussi l'**ordre** de g, noté $|g|$.

Un tel groupe (fini et engendré par un élément) est dit **cyclique**.

Les éléments de l'ensemble $k_0\mathbb{Z}$ des multiples de k_0 vérifient tous la propriété, et ce sont les seuls ; si en effet un entier k la vérifie, on peut l'écrire par division euclidienne $k = qk_0 + r$ avec $0 \leq r < k_0$, et on a :

$$g^{n+r} = g^{n+k-qk_0} = g^{n+k} = g^n$$

de sorte que r vérifie la propriété tout en étant inférieur à k_0, ce qui impose $r = 0$, et k est bien multiple de k_0. On montre sans effort que $k_0\mathbb{Z}$ est lui-même un groupe. Le neutre de G est $g^0 = g^{nk_0}$ pour tout $n \in \mathbb{Z}$; g est un **générateur** du groupe :

$$G = \{g, g^2, \ldots, g^{k_0-1}, g^{k_0} = e\}.$$

D'après l'identité de Bézout (page 65) pour tout entier p premier avec k_0, g^p est aussi un générateur.

En effet, à partir de la relation $ap + bk_0 = 1$, on a :

$$\forall n \in \mathbb{Z} \;:\; g^n = g^{n(ap+bk_0)} = g^{nap} = (g^p)^{na}.$$

Un groupe cyclique est évidemment commutatif car $g^h g^k = g^{h+k} = g^k g^h$.

L'ensemble des rotations du plan, de même centre et d'angle multiple de $2\pi/n$, muni de la loi de composition usuelle, est un groupe cyclique d'ordre n.

Choisissons un entier $p \geq 2$ et à tout entier relatif x associons son reste $\overline{x}$ dans la division par p, qui représente la **classe modulo** p de x, classe contenant tous les entiers z tels que $x - z \in p\,\mathbb{Z}$, c'est- à-dire **congrus** à x modulo p. Notons $\mathbb{Z}/p\,\mathbb{Z}$ l'ensemble des classes.

On vérifie immédiatement qu'en définissant la somme de deux classes par la classe de la somme ($\overline{x} + \overline{y} = \overline{x+y}$) et leur produit par la classe du produit ($\overline{x}\,\overline{y} = \overline{xy}$) on obtient des lois ayant de bonnes propriétés.

Modulo 8 par exemple, les multiples de 8 forment la classe de 0, les multiples de 8 plus 1, la classe de 1 . . . jusqu'à la classe de 7 ; on a ainsi $\overline{6}+\overline{2} = \overline{0}$, $\overline{4}+\overline{5} = \overline{1}$... et $(\mathbb{Z}/8\mathbb{Z}, +)$ est un groupe cyclique (engendré par $\overline{1}$, ou $\overline{3}$, ou $\overline{5}$, ou encore $\overline{7}$).

Mais pour la multiplication cela se passe moins bien. L'élément neutre est évidemment $\overline{1}$. Nous devons d'abord enlever $\overline{0}$ qui n'a pas d'inverse. Comme $\overline{2} \times \overline{4} = \overline{0}$, l'opération n'est plus définie. Il y a donc des éléments appelés **diviseurs de zéro**, éléments qui n'admettent pas d'inverse. Supposons en effet nul le produit ab de deux éléments non nuls et l'existence de a^{-1} : en multipliant par a^{-1} on obtient : $a^{-1}ab = 0$, soit $b = 0$ ce qui est absurde, et de même si on suppose l'existence de b^{-1}. Les diviseurs de zéro dans $\mathbb{Z}/8\mathbb{Z}$, $\overline{2}$, $\overline{4}$ et $\overline{6}$, sont donc non inversibles. Les classes impaires forment le groupe de Klein de l'exercice 11.

L'ensemble $(\mathbb{Z}/p\,\mathbb{Z}) \setminus \{\overline{0}\}$ n'est un groupe que si p est premier. Dans ce cas en effet, quel que soit x, p et x sont premiers entre eux et il existe des entiers y et z tels que $xy + pz = 1$ (identité de Bézout, page 65), d'où $\overline{xy} = \overline{1}$ (si p n'est pas premier, $p = rs$ et $\overline{rs} = \overline{0}$).

Ce groupe est alors cyclique, engendré par n'importe quelle classe, sauf $\overline{1}$, qui est le neutre. Ainsi dans $\mathbb{Z}/5\mathbb{Z}$ les inverses des classes de 2, 3, 4 sont dans l'ordre les classes de 3, 2, 4 ; pour 4 par exemple on a $4 \times 4 = 3 \times 5 + 1$, et donc $\overline{4} \times \overline{4} = \overline{1}$.

Le **groupe d'une figure** est l'ensemble des isométries laissant cette figure globalement invariante. Il contient toujours au moins l'identité. Le groupe du triangle équilatéral contient, en plus de l'identité, deux rotations et trois réflexions : il est d'ordre 6.

Un **groupe abélien libre** sur une base $B \subset G$ est un groupe abélien $(G, *)$ dont tous les éléments s'écrivent de manière unique $g = a_1 * a_2 * \cdots * a_n$, $a_i \in B$, à l'ordre près et après réduction, c'est-à-dire en supprimant les paires $b_i * b_{i+1}$ lorsque $b_{i+1} = b_i^{-1}$.

Soient $(G, *)$ un groupe et B une partie de G contenant l'inverse de chaque élément. Un **mot** de longueur $n \in \mathbb{N}$ est une suite ordonnée finie d'éléments de B, réduite comme ci-dessus : $m = b_1 b_2 ... b_n$. Notons $M(B)$ l'ensemble de ces mots. La concaténation de deux mots m_1 et m_2 donne, après réduction s'il y a lieu, le mot $m_1 m_2$, ce qui définit une loi de composition sur $M(B)$, visiblement associative et non commutative. Elle admet un élément neutre : le mot vide, et chaque mot est inversible : $(b_1 b_2 \cdots b_n)^{-1} = b_n^{-1} \cdots b_1^{-1}$. Elle munit $M(B)$ d'une structure de groupe : le **groupe libre** construit sur B.

Si B est singleton, $M(B)$ est isomorphe à $\mathbb{Z}$.

Le **groupe-produit** de deux groupes $(G, .)$, de neutre e, et $(G', *)$, de neutre e', est l'ensemble $G \times G'$ muni de la loi $(x, x') \star (y, y') = (x.y, x' * y')$ (x et y dans G, x' et y' dans G'). Il est commutatif si G et G' le sont. Son ordre est le produit des ordres de G et G'. Son neutre est (e, e').

2.2 Morphisme de groupes

Un **morphisme** pour une structure est une application respectant cette structure ; ainsi une application ϕ d'un groupe G_1 dans un groupe G_2 est un morphisme de groupes si l'image d'un produit est le produit des images, l'image de l'inverse l'inverse de l'image, l'image du neutre e_1 de G_1 le neutre e_2 de G_2, ce qui peut se condenser en l'unique condition, pour tous éléments x et y dans G_1, en notation multiplicative :

$$\phi(xy) = \phi(x)\,\phi(y).$$

En effet, en posant $y = e_1$:

$$\phi(x) = \phi(x\,e_1) = \phi(x)\,\phi(e_1) = \cdots = \phi(e_1)\,\phi(x)$$

nous voyons que $\phi(e_1)$ est le neutre de G_2 ; enfin :

$$e_2 = \phi(e_1) = \phi(x^{-1}x) = \phi(x^{-1})\,\phi(x) = \cdots = \phi(x)\,\phi(x^{-1})$$

montre que $\phi(x^{-1})$ est bien l'inverse de $\phi(x)$.

L'image réciproque du neutre est le **noyau** de ϕ noté $\mathrm{Ker}(\phi)$:

$$\mathrm{Ker}(\phi) = \overset{-1}{\phi}\,(e_2) = \{x \in G_1 \,|\, \phi(x) = e_2\},$$

et l'ensemble des $\phi(x)$ quand x parcourt G_1 est l'**image** de ϕ, notée $\mathrm{Im}(\phi)$ ou $\phi(G_1)$; ϕ est **injectif** si et seulement si $\mathrm{Ker}(\phi)$ est réduit au neutre, **surjectif** si $\mathrm{Im}(\phi)$ est égale à G_2, **bijectif** s'il est injectif et surjectif.

Un morphisme bijectif de groupes est un **isomorphisme**. On vérifie sans mal que son application réciproque est aussi un isomorphisme, de même que le produit de de deux isomorphismes. On exprime que G_1 est isomorphe à G_2 par l'écriture :

$$G_1 \cong G_2.$$

Un isomorphisme d'un groupe G sur lui-même est un **automorphisme** ; l'identité est un automorphisme, et on vérifie immédiatement que l'ensemble des automorphismes de G, $\mathrm{Aut}(G)$, est lui-même un groupe.

2.3 Sous-groupe

Une partie non vide H d'un groupe G est un **sous-groupe** de G si elle est un groupe pour la même loi ; en particulier, elle doit avoir le même neutre. Ceci se condense en l'unique condition :

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

Les plus simples sont le sous-groupe réduit au neutre, dit **trivial** , et G lui-même ; les autres sont dits **stricts**. Le groupe $k_0\mathbb{Z}$ rencontré il y a peu est un sous-groupe de $\mathbb{Z}$. Avec les notations du paragraphe précédent, $\mathrm{Ker}(\phi)$ est un sous-groupe de G_1, $\mathrm{Im}(\phi)$ un sous-groupe de G_2 (exercice 2).

Le **centre** d'un groupe est l'ensemble des éléments qui commutent avec tous les autres. Le neutre appartient toujours au centre qui ne peut donc être vide ; on vérifie sans peine que le centre est un sous-groupe.

Soit H un sous-groupe de G ; la relation entre éléments de G :

$$x \,\Re\, y \iff x^{-1}y \in H$$

est réflexive :

$$x\,x^{-1} = e \in H$$

symétrique :

$$x \,\Re\, y \Rightarrow x^{-1}y \in H \Rightarrow (x^{-1}y)^{-1} = y^{-1}x \in H \Rightarrow y \,\Re\, x$$

et transitive :

$$[x \,\Re\, y,\ y \,\Re\, z] \Rightarrow [x^{-1}y \in H,\ y^{-1}z \in H] \Rightarrow x^{-1}yy^{-1}z = x^{-1}z \in H \Rightarrow x \,\Re\, z.$$

C'est donc une relation d'équivalence qui permet de partitionner G en classes d'équivalence disjointes, dites **classes modulo un sous-groupe**, en l'occurrence, classes à gauche modulo H ; la classe d'un élément g est notée gH, la classe du neutre étant H. On définit de même les classes à droite, notées Hg, la relation d'équivalence s'écrivant alors $yx^{-1} \in H$. Toutes les classes ont le même cardinal : $|H|$; s'il y a m classes on a donc :

$$|G| = m|H|,$$

m étant l'**indice** de H dans G, noté $[G : H]$, d'où le théorème de Lagrange :

Théorème 2.1. *L'ordre d'un sous-groupe divise l'ordre du groupe.* □

L'ordre d'un élément est l'ordre du groupe qu'il engendre ; il divise donc l'ordre du groupe si celui-ci est fini. Un groupe d'ordre premier est engendré par l'un quelconque de ses éléments, à l'exception du neutre (groupe cyclique).

Proposition 2.1. *L'image d'un sous-groupe par un automorphisme est un sous-groupe ayant le même ordre.*

Démonstration. Soient G un groupe de neutre e, H l'un de ses sous-groupes et ϕ un automorphisme de G. Quels que soient les éléments x et y de $\phi(H)$, il existe un unique couple (x', y') d'éléments de G tel que $x = \phi(x')$ et $y = \phi(y')$, et on a :

$$\begin{cases} e = \phi(e) \Rightarrow e \in \phi(H), \\ xy = \phi(x')\phi(y') = \phi(x'y') \Rightarrow xy \in \phi(H), \\ \phi(x')\phi(x'^{-1}) = \phi(e) = e \Rightarrow x^{-1} = \phi(x'^{-1} \in \phi(H). \end{cases}$$

L'ensemble $\phi(H)$ est donc un sous-groupe de G, de même ordre que H, ϕ étant une bijection. □

Un sous-groupe inchangé sous l'action des automorphismes est dit **caractéristique**.

Proposition 2.2. *L'intersection de sous-groupes d'un groupe G est un sous-groupe de G.*

Démonstration. Voir l'exercice 1. □

Un groupe fini est **simple** s'il n'a pas d'autre sous-groupe invariant strict que le groupe trivial (réduit à l'élément neutre).

Un sous-groupe strict d'un groupe fini G est **maximal** s'il n'est contenu dans aucun sous-groupe strict autre que lui-même. Tout sous-groupe de G est inclus dans un sous-groupe maximal.

Si H est un sous-groupe du groupe G, l'**injection canonique** est le morphisme $i : H \to G$, $i(h) = h$.

2.4 Sous-groupe engendré par une famille

Soit $X = (x_i)_{i \in I}$ une famille (non vide) d'éléments d'un groupe G, noté multiplicativement. Le **sous-groupe engendré** par X est le plus petit sous-groupe contenant X. Construisons ce sous-groupe. Complétons d'abord X en lui ajoutant les inverses x_i^{-1} de ses éléments. A chaque partie finie et ordonnée (si G n'est pas commutatif) de X (deux telles parties peuvent ne différer que par l'ordre des éléments) associons le produit (dans l'ordre) de ses éléments, et soit $[X]$ l'ensemble de ces produits. Cet ensemble contient tous les x_i, donc X, et le neutre $e = x_i x_i^{-1}$ pour l'un quelconque des $x_i \in X$. Le produit de deux éléments de $[X]$:

$$\begin{cases} x & = x_{i_1} \dots x_{i_k},\ x_{i_j} \in X,\ 1 \leq j \leq k, \\ y & = x_{n_1} \dots x_{n_h},\ x_{n_j} \in X,\ 1 \leq j \leq h, \\ xy & = x_{i_1} \dots x_{i_k}\, x_{n_1} \dots x_{n_h} \end{cases}$$

appartient à $[X]$, ainsi que l'inverse d'un élément :

$$\begin{cases} z & = x_{m_1} \dots x_{m_s}, \\ z^{-1} & = x_{m_s}^{-1} \dots x_{m_1}^{-1}, \end{cases}$$

et $[X]$ est un sous-groupe. C'est évidemment le plus petit des sous-groupes contenant X, un tel sous-groupe devant contenir tous les produits utilisés pour construire $[X]$.

Si les éléments de X commutent deux à deux, les formules du produit deviennent :

$$x = \prod x_{i_k},\ y = \prod x_{n_j},\ xy = \prod x_{i_k} \prod x_{n_j} = \prod x_{n_j} \prod x_{i_k}$$

et $[X]$ est commutatif.

Si H et K sont deux sous-groupes d'un groupe commutatif G, on a en notation additive $[H+K] = H+K$, ou en notation multiplicative $[HK] = HK$. Si G n'est pas commutatif, HK n'est pas en général un sous-groupe. Soit par exemple G le groupe des matrices réelles 2×2 de déterminant égal à 1 pour le produit matriciel, et H et K les sous- groupes des matrices de la forme, respectivement :

$$h(a) = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix},\ k(b) = \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix}.$$

La forme :

$$h(a)\,k(b) = \begin{pmatrix} 1+ab & a \\ b & 1 \end{pmatrix}$$

n'étant pas stable pour le produit :

$$\begin{pmatrix} 1+ab & a \\ b & 1 \end{pmatrix} \begin{pmatrix} 1+a'b' & a' \\ b' & 1 \end{pmatrix} = \begin{pmatrix} 1+ab+a'b'+aba'b' & a'+aba'+a \\ b+a'bb'+b' & 1+a'b \end{pmatrix}$$

si l'on regarde, par exemple, le quatrième coefficient qui n'est pas égal à 1, l'ensemble HK n'est pas un sous-groupe.

La réunion de deux sous-groupes n'est pas en général un sous-groupe. Ainsi $2\mathbb{Z}$ et $3\mathbb{Z}$ sont des sous-groupes de $(\mathbb{Z}, +)$, et le sous-groupe qu'ils engendrent contient $5 = 2 + 3$, qui n'appartient ni à l'un ni à l'autre.

Comme $1 = 2 \times 2 - 3 \in [2\mathbb{Z} + 3\mathbb{Z}]$, on a $[2\mathbb{Z} \cup 3\mathbb{Z}] = \mathbb{Z}$.

2.5 Automorphisme intérieur

A un élément quelconque g du groupe G associons la transformation :

$$\begin{array}{rccc} \phi_g : & G & \to & G \\ & x & \mapsto & g\,x\,g^{-1}. \end{array}$$

C'est un morphisme, car :

$$\begin{array}{rcl} \phi_g(xy) & = & g\,x\,y\,g^{-1} \\ & = & g\,x\,g^{-1}\,g\,y\,g^{-1} \\ & = & \phi_g(x)\,\phi_g(y), \end{array}$$

et il admet $\phi_{g^{-1}}$ pour inverse :

$$\phi_g(\phi_{g^{-1}}(x)) = g(g^{-1}xg)g^{-1} = x = g^{-1}(gxg^{-1})g = \phi_{g^{-1}}(\phi_g(x)).$$

C'est donc un automorphisme, appelé **automorphisme intérieur** ; un sous-groupe est donc **invariant** s'il est invariant sous l'action des automorphismes intérieurs. L'ensemble des automorphismes intérieurs est un groupe (exercice 4) noté $\mathrm{Int}(G)$, sous-groupe de $\mathrm{Aut}(G)$.

Si ϕ est un automorphisme intérieur, H et $\phi(H)$ sont des sous-groupes **conjugués**.

2.6 Groupe quotient

Peut-on munir l'ensemble des classes modulo le sous-groupe H de G d'une structure de groupe induite par celle de G, comme pour $\mathbb{Z}/p\mathbb{Z}$? Il suffit pour cela que la classe d'un produit soit le produit des classes :

$$xyH = xHyH.$$

Comme $HH = H$, cette condition équivaut à l'égalité des classes à gauche et à droite :

$$\forall y \in G,\ yH = Hy,$$

ou encore à :

$$\forall y \in G,\ yHy^{-1} = H.$$

On a en effet :

$$[yH = Hy] \Rightarrow [xyH = xyHH = xHyH]$$

et :

$$[xyH = xHyH] \Rightarrow [yH = HyH]$$

de sorte que yH, Hy et HyH ont le même cardinal. Comme les deux premiers sont inclus dans le troisième, ces trois ensembles sont égaux.

Un sous-groupe vérifiant cette condition ($\forall y \in G,\ yH = Hy$) est dit **invariant**, ou **distingué**, ou encore **normal**. L'ensemble des classes muni de la loi induite par celle de G est alors un groupe, le **groupe quotient**, noté G/H, dont l'ordre est évidemment le quotient de celui de G par celui de H, si G est fini. Tout sous-groupe d'un groupe commutatif est invariant.

L'ordre de G/H est encore l'**indice** de H dans G, $[G : H]$:

$$[G : H] = \frac{|G|}{|H|}.$$

Remarque : un sous-groupe est invariant si et seulement s'il est inchangé sous l'action des automorphismes intérieurs.

Théorème 2.2 (de correspondance)**.** *Si H est un sous-groupe invariant d'un groupe fini G, l'application qui associe les sous-groupes de G contenant H et les sous-groupes de G/H est bijective et conserve l'invariance.*

Démonstration. Soit $\pi : G \to G/H$ l'application canonique sur les classes modulo H. C'est un morphisme de groupes, et l'image d'un sous-groupe de G contenant H est un groupe (exercice 2), sous-groupe de G/H. Ceci définit une application de l'ensemble E des sous-groupe de G contenant H dans l'ensemble F des sous-groupe de G/H.

Si K est un sous-groupe invariant de G contenant H, $p(K) \in F$, et, $\forall g \in G$, $gK = Kg$, $\pi(g)p(K) = p(K)\pi(g)$, de sorte que, π étant surjective, $p(K)$ est invariant.

Si $L \in F$, $\pi^{-1}(L)$ est un sous-groupe M de G (exercice 2) contenant H, ce qui définit une application $q : F \to E$; $p \circ q$ est l'identité de F et $q \circ p$ est l'identité de E. Si L est invariant, $\pi(g)L = L\pi(g)$, d'où $gq(L) = q(L)g$, et q respecte l'invariance. □

2.7 Produit libre, produit libre amalgamé

Soient trois groupes, G, H et K et des morphismes quelconques $g : G \to K$ et $h : H \to K$. Nous allons construire un groupe, le **produit libre** $G * H$ de G et H, admettant ces deux groupes comme sous-groupes ($i : G \to G * H$, $j : H \to G*H$ étant les injections canoniques), et ayant la propriété universelle : il existe un morphisme unique $\phi : G * H \to K$ tel que $\phi \circ i = f$ et $\phi \circ j = h$, quels que soient f et g.

Ce produit est l'ensemble des mots $x_1 \cdots x_n$ tels que si $x_i \in G$, $x_{i+1} \in H$. On montre la structure de groupe comme pour le groupe libre.

Si $x_1 \in G$, on pose $\phi(x_1 x_2 \cdots) = g(x_1)h(x_2)\cdots \in K$, et si $x_1 \in H$, on pose $\phi(x_1 x_2 \cdots) = h(x_1)g(x_2)\cdots \in K$, de sorte que, si $x \in G$, $\phi(x) = g(x)$, et si $x \in H$, $\phi(x) = h(x)$.

Exemple 2.1. Considérons les transformation du plan complexe $\mathbb{C}$: $u(z) = -1/z$ et $v(z) = 1 - 1/z$, et le groupe G qu'elles engendrent. On a $u^2(z) = u(u(z)) = z$ et $v^3(z) = z$. Ce groupe, appelé *groupe modulaire*, important en géométrie, est donc isomorphe à $\mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/3\mathbb{Z}$. ▽

Soient trois groupes, F, G, H et et des morphismes $\phi : F \to G$ et $\psi : F \to H$. Si $G \cap H$ n'est pas le groupe trivial, on définit le **produit libre amalgamé** de G et H sur F :

$$G \underset{F}{*} H = (G * H)/N,$$

N étant le sous-groupe invariant engendré par les $\phi(f)(\psi(f))^{-1}$, $f \in F$.

Ce produit est utilisé lors du calcul du groupe fondamental d'une réunion de deux espaces topologiques d'intersection non vide (théorème de Van Kampen).

2.8 Action d'un groupe sur un ensemble

On dit qu'un groupe G de neutre e **opère** sur un ensemble E (ayant plus d'un élément) s'il existe une loi de composition :

$$\begin{array}{ccc} G \times E & \to & E \\ (g, x) & \mapsto & \tau_{\mathrm{g}}(x) = g \,.\, x \end{array}$$

telle que, quels que soient les éléments écrits :

$$\begin{cases} e \,.\, x & = x, \\ g' \,.\, (g \,.\, x) & = g'g \,.\, x. \end{cases}$$

Nous supposerons de plus que l'action est **fidèle**, c'est- à-dire que $g \,.\, x = x$ pour tout $x \in E$ implique $g = e$, et non **triviale**, c'est- à-dire qu'il n'existe pas $x_0 \in E$ tel que, pour tout couple (g, x), on ait $g \,.\, x = x_0$.

On a donc $\tau_{\mathrm{e}} = i_d$ et $\tau_{\mathrm{g'}} \circ \tau_{\mathrm{g}} = \tau_{\mathrm{g'g}}$. D'autre part, τ_{g} est une bijection de E :

$$\tau_{\mathrm{g}}(x) = \tau_{\mathrm{g}}(y) \iff g \,.\, x = g \,.\, y \iff x = g^{-1}g \,.\, y = y$$

et l'application :

$$\tau : g \mapsto \tau_{\mathrm{g}}$$

de G dans le groupe $\mathfrak{B}(E)$ des bijections de E est un morphisme de groupes. Ce morphisme est injectif :

$$\begin{array}{rcl} \tau_{\mathrm{g}} = \tau_{\mathrm{g'}} & \iff & \forall x \in E \,:\, g\,.\,x = g'\,.\,x \\ & \iff & \forall x \in E \,:\, g^{-1}g'\,.\,x = x \\ & \iff & g^{-1}g' = e \iff g' = g. \end{array}$$

L'ensemble $\tau(G) = \{\tau_{\mathrm{g}} \,|\, g \in G\}$ est un sous-groupe de $\mathfrak{B}(E)$.

La relation $x \Re y \iff \exists g \in G : y = g\,.\,x$ entre deux éléments de E est évidemment une équivalence, qui partitionne E en classes d'équivalence, appellées **orbites**. L'orbite de $x \in E$ est donc l'ensemble $\mathfrak{O}(x)$, ou $G\,.\,x$, des $g\,.\,x$ quand g parcourt G.

Le groupe G opère **transitivement** sur E s'il n'y a qu'une orbite, c'est-à-dire si, quels que soient x et y dans E, il existe $g \in G$ tel que $g\,.\,x = y$.

Le **fixateur** de $z \in E$, ou son **stabilisateur**, $\mathrm{Fix}(z)$ est l'ensemble des $g \in G$ tels que $g\,.\,z = z$. C'est un sous-groupe de G, car :

$$\begin{cases} e\,.\,z = z \Rightarrow e \in \mathrm{Fix}(z), \\ g\,.\,z = z,\ g'\,.\,z = z,\ g'g\,.\,z = g'\,.\,z = z \Rightarrow g'g \in \mathrm{Fix}(z), \\ g\,.\,z = z,\ z = g^{-1}\,.\,z \Rightarrow g^{-1} \in \mathrm{Fix}(z). \end{cases}$$

La surjection :

$$\begin{array}{rccc} \phi_z : & G & \to & \mathfrak{O}(z) \\ & g & \mapsto & g\,.\,z \end{array}$$

permet, si $\mathrm{Fix}(z)$ est invariant, de transporter la structure de groupe de G sur $\mathfrak{O}(z)$, en posant :

$$(g'\,.\,z) * (g\,.\,z) = g'g\,.\,z,$$

et devient un morphisme de groupes, dont le noyau est $\mathrm{Fix}(z)$; $\mathfrak{O}(z)$ est alors un groupe isomorphe au groupe quotient $G/\mathrm{Fix}(z)$, et on a, si G est fini :

$$|G| = |\mathfrak{O}_z|\,|\mathrm{Fix}(z)|.$$

Exemple 2.2. Si on fait opèrer le groupe additif $\mathbb{R}$ sur $\mathbb{C}^*$:

$$\mathbb{R} \times \mathbb{C} \ni (x, z) \mapsto x\,.\,z = e^{2i\pi x}z = \phi_z(x),$$

on a $\mathrm{Fix}(z) = \mathbb{Z}$, sous-groupe additif de $\mathbb{R}$, invariant, l'orbite de z est le cercle de centre O et de rayon $|z|$. Chaque orbite est en bijection avec le groupe quotient $\mathbb{R}/\mathbb{Z}$, et peut donc être munie d'une structure de groupe. $\triangledown$

2.9 Groupe dérivé

Le **commutateur** de deux éléments g et h d'un groupe G est l'élément $ghg^{-1}h^{-1}$, noté $[g,h]$. Il indique le défaut de commutativité des deux éléments :

$$gh = [g,h]\,hg,$$

et si G est commutatif, tout commutateur est égal au neutre e.

Comme :

$$[g,h]\,[h,g] = ghg^{-1}h^{-1}\,hgh^{-1}g^{-1} = e_{\mathrm{G}},$$

on a $[h,g] = [g,h]^{-1}$.

Le produit de deux commutateurs n'étant pas toujours un commutateur, l'ensemble des commutateurs n'est pas en général un sous-groupe, mais il engendre le **groupe dérivé** de G, noté $D(G)$.

Théorème 2.3. *Soit G un groupe, $D(G)$ son groupe dérivé et H un sous-groupe invariant. Alors :*
(a) $D(G)$ est invariant,
(b) $G/D(G)$ est commutatif,
(c) si G/H est commutatif, H contient $D(G)$,
(d) si H contient $D(G)$, G/H est commutatif.

Démonstration.
(a) Le groupe dérivé est stable sous l'action de $\mathrm{Aut}(G)$. En effet, si $\phi \in \mathrm{Aut}(G)$:

$$\phi([g,h]) = [\phi(g)\phi(h)(\phi(g))^{-1}(\phi(h)^{-1}) = [\phi(g),\phi(h)]$$

et l'image d'un commutateur est un commutateur. C'est donc vrai pour les automorphismes intérieurs, et $D(G)$ est donc invariant.
(b) De $gh = [g,h]\,hg$, on déduit par passage au quotient $\overline{gh} = \overline{hg}$, puisque $\overline{[g,h]} = e_{\mathrm{D(G)}}$.
(c) Considérons les classes modulo H. De $\overline{gg'} = \overline{g'g}$ on déduit l'existence d'un $h \in H$ tel que $gg' = hg'g$. Alors $h = gg'g^{-1}g'^{-1}$, et h est un commutateur : $h \in D(G)$. Ceci est vrai quels que soient g et g', donc pour tout commutateur, et pour tout élément de $D(G)$, produit de commutateurs.
(d) Si $D(G) \subset H$, G/H est un sous-groupe de $G/D(G)$, donc commutatif. □

Le groupe dérivé de $D(G)$ est noté $D^2(G)$, et $D^k(G) = D(D^{k-1}(G))$. S'il existe $n \in \mathbb{N}$ tel que $D^n(G) = \{e\}$, le groupe G est **résoluble**. Cette notion est fondamentale en théorie de Galois : le polynôme général du cinquième degré n'est pas résoluble par radicaux car, nous le verrons plus loin, le groupe des permutations sur cinq éléments n'est pas résoluble.

Proposition 2.3. *Les assertions suivantes sont équivalentes :*
(a) le groupe G est résoluble,
(b) il existe dans G une suite finie et décroissante de sous-groupes $(H_i)_{0\leq i\leq n}$ tels que :

$$\begin{cases} G = H_0 \supset H_1 \supset \ldots \supset H_n = \{e\}, \\ H_{i+1} \text{ est invariant dans } H_i, \\ H_i/H_{i+1} \text{ est commutatif.} \end{cases}$$

Démonstration. Si G est résoluble, il suffit de poser $H_i = D^i(G)$.

Réciproquement (théorème 2.2), G/H_1 étant commutatif, H_1 contient $D(G)$, et $D^2(G) \subset D(H_1)$. De même, $D(H_1) \subset H_2$, et donc $D^2(G) \subset H_2$. Poursuivant par récurrence, on arrive à $D^n(G) \subset H_n$, d'où $D^n(G) = \{e\}$.

Voir le théorème 2.5, page 15. □

2.10 Théorème de l'ordre

Les résultats prouvés dans les sept premiers exercices sont utilisés dans la démonstration du théorème suivant, fondamental pour l'étude des groupes finis, et qui permettra de démontrer que tout corps fini est commutatif.

Théorème 2.4 (de Cauchy)**.** *Pour chaque nombre premier p qui divise l'ordre d'un groupe G, il existe (au moins) un élément d'ordre p dans G.*

Démonstration. L'hypothèse se traduit par $|G| = kp$. Posons :

$$E = \{(g_1, g_2, \ldots, g_p) \mid \prod_{i=1}^{p} g_i = e\} \subset G^p.$$

On peut choisir librement les g_i de $i = 1$ à $p-1$, mais alors $g_p = g_{p-1}^{-1} \ldots g_1^{-1}$, de sorte que le cardinal de E est égal à $|G|^{p-1}$; il est donc divisible par p.

Faisons agir sur E l'opérateur de décalage τ ainsi défini :

$$\tau(g_1, \ldots, g_p) = (g_2, \ldots, g_1).$$

Il engendre un groupe cyclique d'ordre p, τ^p étant l'identité. L'*orbite* d'un élément x de E est l'ensemble des $\tau^k(x)$ pour k allant de 1 à p. Si tous les g_i sont égaux, l'orbite n'a qu'un élément. C'est le cas de $(e, \ldots, e)$. Si deux au moins des g_i sont distincts, elle en a p. Les orbites forment une partition de E, car, si deux orbites ont un élément commun, x, elles sont toutes les deux égales à $(\tau^k(x))_{1\leq k\leq p}$. S'il n'y avait qu'une orbite à un élément, le cardinal de E serait égal à un multiple de p plus 1, or c'est un multiple de p ; E contient donc plus d'une orbite à un élément ; une telle orbite est de la forme $(g, \ldots, g)$, avec $g \neq e$ et $g^p = e$. □

Corollaire. Un groupe simple commutatif est cyclique d'ordre premier.

Démonstration. Si un groupe G, d'ordre r, est commutatif, et si un nombre premier p divise r, G possède un élément d'ordre p qui engendre un sous-groupe cyclique d'ordre premier, invariant puisque G est commutatif, égal à G si G est simple. □

Théorème 2.5 (Nouvelle définition)**.** *Un groupe fini G est résoluble si et seulement s'il existe une suite de sous-groupes :*

$$G = G_0 \supset G_1 \ldots \supset G_i \supset G_{i+1} \ldots \supset G_n = \{e\},$$

telle que G_{i+1} est invariant dans G_i, $0 < i < n-1$, et G_i/G_{i+1} est cyclique d'ordre premier.

Démonstration. La seconde assertion implique trivialement la première. Montrons la réciproque. Soit, $\forall i$, $G_{i,1}$ un sous-groupe invariant maximal de G_i contenant G_{i+1}. Si $G_{i,1} = G_{i+1}$, passons au suivant. Sinon, soit $G_{i,2}$ un sous-groupe invariant maximal de $G_{i,1}$ contenant G_{i+1}... On construit ainsi une suite de sous-groupes (K_i) entre G et $\{e\}$, décroissante, chaque sous-groupe étant maximal dans le précédent. Les sous-groupes invariants K_i/k_{i+1} sont en bijection avec les sous-groupes invariants de K_i contenant K_{i+1} (théorème 2.2 de correspondance, page 11) ; K_i/K_{i+1} est donc un groupe simple, commutatif car contenu dans G_i/G_{i+1}. Il est donc cyclique d'ordre premier (corollaire, page 14). □

2.11 Le groupe symétrique $\mathfrak{S}_n$

Une permutation σ sur l'ensemble $E_n = \{1, 2, \ldots, n\}$ est une bijection de E_n sur lui-même. Elle est caractérisée par les $\sigma(i)$, et notée $(\sigma(1), \sigma(2), \ldots, \sigma(n))$. Le **support** de σ est l'ensemble des i tels que $\sigma(i) \neq i$.

L'ensemble de ces permutations sur E_n est noté $\mathfrak{S}_n$. L'identité est une permutation ; on définit le produit, ou la composée, des permutations σ_1 et σ_2, $\sigma = \sigma_2 \circ \sigma_1$ par $\sigma(i) = \sigma_2(\sigma_1(i))$. Cette opération est évidemment associative, son neutre est l'identité ; l'inverse de σ est défini par $\sigma^{-1}(i) = j$ si $\sigma(j) = i$; $(\mathfrak{S}_n, \circ)$ est un groupe, le **groupe symétrique** d'indice n. Il y a n possibilités pour $\sigma(1)$, $n-1$ pour $\sigma(2)$..., et enfin une pour $\sigma(n)$, et l'ordre de $\mathfrak{S}_n$ est égal à $n!$.

Ce groupe n'est pas commutatif ; par exemple :

$$\begin{cases} (2,3,1)\,(3,2,1) = (1,3,2), \\ (3,2,1)\,(2,3,1) = (2,1,3). \end{cases}$$

On définit la **transposition** τ_{ij}, $i < j$, ou $(i-j)$, par : $\tau_{ij}(i) = j$, $\tau_{ij}(j) = i$, $\tau_{ij}(k) = k$ si $k \notin \{i, j\}$. Une transposition est une involution $(\tau_{ij}^{-1} = \tau_{ij})$.

Il y a une **inversion** dans la permutation σ chaque fois que $\sigma(i) > i$; le nombre $r(\sigma)$ des inversions de σ est donc bien fixé. On supprime une inversion en composant convenablement avec une transposition.

Notons que deux transposition commutent si et seulement si leurs supports sont disjoints :

$$\begin{cases} (1-2)\,(3-4) = (2,1,4,3) = (3-4)\,(1-2), \\ (1-2)\,(2-4) = (4,1,3,2), \\ (2-4)\,(1-2) = (2,4,3,1). \end{cases}$$

Calculons $r(\sigma)$. Si $\sigma(1) = i > 1$, le produit $\sigma_1 = \tau_{1i} \circ \sigma$ est tel que :

$$\sigma_1(1) = \tau_{1i}(\sigma(1)) = \tau_{1i}(i) = 1.$$

On a $r(\sigma_1) = r(\sigma) - 1$ et $\sigma = \tau_{1i} \circ \sigma_1$. Si $\sigma(1) = 1$, on pose $\sigma_1 = \sigma$, et $r(\sigma_1) = r(\sigma)$.

Si $\sigma_1(2) = i > 2$, ou $\sigma_1(2) = 2$, on procède de même... jusqu'à obtenir $\sigma_k = i_d$, $r(\sigma_k) = 0$, et σ est mise sous forme d'un produit de $r(\sigma)$ transpositions.

Exemple 2.2 Partons de la permutation $\sigma = (4,3,2,1)$.

$$\begin{cases} \sigma_1 = \tau_{14} \circ \sigma = (1,3,2,4) \Rightarrow \sigma = \tau_{14} \circ \sigma_1,\ r(\sigma) = r(\sigma_1) + 1, \\ \sigma_2 = \tau_{23} \circ \sigma_1 = (1,2,3,4) \Rightarrow \sigma = \tau_{23} \circ \tau_{14},\ r(\sigma) = 2. \end{cases}$$

La **classe de conjugaison** de $\sigma \in \mathfrak{S}_n$ est l'ensemble :

$$\begin{aligned} \overline{\sigma} &= \{\phi(\sigma) \,|\, \phi \in \mathrm{Int}(\mathfrak{S}_n)\} \\ &= \{s\,\sigma\,s^{-1} \,|\, s \in \mathfrak{S}_n\}. \end{aligned}$$

Les éléments de cette classe sont les **conjugués** de σ.

Un **cycle** de degré s, de $\mathfrak{S}_n$ ($s \leq n$) ou s-cycle, $(i_1 - i_2 - \cdots - i_s)$ est une permutation σ telle que $\sigma(i_1) = i_2$, $\sigma(i_2) = i_3$,..., $\sigma(i_s) = i_1$, les i_k étant deux à deux distincts, les autres éléments conservant leur place. Une transposition est un 2-cycle, et par exemple :

$$(1-4-2) = (4,1,3,2)$$

est un 3-cycle de $\mathfrak{S}_n$ pour $n \geq 4$, qui peut aussi s'écrire $(4-2-1)$ ou $(2-1-4)$, un s-cycle étant évidemment invariant par permutation circulaire. On choisira son écriture commençant par le plus petit des i_k.

Proposition 2.4. *Un s-cycle σ engendre un sous-groupe cyclique d'ordre s. Réciproquement, un sous-groupe cyclique d'ordre s de $\mathfrak{S}_n$ ($s \leq n$) est engendré par un s-cycle.*

Démonstration. On a évidemment $\sigma^s = i_d$, et les puissances de σ de 1 à p sont deux à deux distinctes. Elles forment donc un groupe cyclique d'ordre s. Réciproquement, si σ engendre un sous-groupe cyclique d'ordre s, σ^s est l'identité et les σ^i pour $0 < i \leq s$ sont deux à deux distinctes. Il reste à voir que, si on pose $\sigma(i_1) = i_2$,..., $\sigma(i_{s-1}) = i_1$, les i_l sont deux à deux distincts. Supposons qu'il existe i_k dans le support de σ tel que $\sigma(i_k) = i_k$. On aurait alors

$\sigma^h((i_k) = i_k$ pour tout $h > k$, donc pour tout h puisque les exposants agissent modulo s, et i_k n'appartiendrait pas au support de σ, ce qui est absurde. On a $i_{s-1} = \sigma(i_{s-2} = \cdots = \sigma^{s-1}(i_1)$. Supposons qu'il existe un couple (h, k), $h > k$, tel que $i_h = i_k$. On aurait alors $\sigma^{h-k}(i_k) = i_h = i_k$, puis $\sigma^{h-k+1}(i_k) = i_{k+1}$,..., $\sigma^{2(h-k)}(i_k) = i_k$, le support de σ se réduirait à i_k, i_{k+1},..., i_h, et σ engendrerait un groupe d'ordre $h - k < s$, ce qui est absurde. □

Proposition 2.5. *L'image d'un s-cycle par un automorphisme intérieur est un s-cycle, conjugué s'il est différent.*

Démonstration. L'image d'un groupe cyclique par un automorphisme intérieur est un groupe cyclique de même ordre. Il reste à utiliser la proposition précédente. □

Soit C_σ le groupe des permutations de $\mathfrak{S}_n$ qui commutent avec σ (voir l'exercice 3).

Proposition 2.6. *Le nombre de s-cycle conjugués du s-cycle $\sigma \in \mathfrak{S}_n$ est égal à $\dfrac{n!}{|C_\sigma|}$.*

Démonstration. Les s-cycles σ' conjugués de σ sont de la forme $\tau \circ \sigma \circ \tau^{-1}$, avec $\tau \in \mathfrak{S}_n$; σ' est égal à σ si et seulement si $\tau \in C_\sigma$. Si τ et τ' sont dans la même classe modulo C_σ, ils donnent le même s-cycle. Le nombre de classes est donc égal au nombre de classes modulo C_σ. □

Un s-cycle se décompose, au vu des inversions, en un produit de $s+1$ transpositions. Ainsi :

$$(1 - 4 - 2) = (2 - 3)\,(3 - 4)\,(2 - 3)\,(1 - 2).$$

Soit $\sigma \in (S)_n$. Considérons l'espace vectoriel $Z = (\mathbb{Z}/2\mathbb{Z})^n$, (e_i) sa base canonique, l'automorphisme (d'espace vectoriel) u_σ défini par $u_\sigma(e_i) = e_{\sigma(i)}$, M_σ la matrice de u_σ, **matrice de la permutation** et ϵ_σ son déterminant, égal à ± 1, et appelé la **signature** de la permutationote. Ainsi, pour la permutation de l'exemple précédent :

$$M_\sigma = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \text{ et } \epsilon_\sigma = 1.$$

Le déterminant d'un produit étant égal au produit des déterminants, l'application $\sigma \mapsto \epsilon_\sigma$ est un morphisme du groupe $(S)_n$ sur le groupe multiplicatif $\mathbb{Z}/2\mathbb{Z}$. La signature d'une transposition est égale à -1, puisqu'en commutant deux colonnes d'un déterminant on change son signe. Il s'ensuit que la signature d'une permutation σ, produit de $r(\sigma)$ transpositions, est égale à $(-1)^{r(\sigma)}$, et que, si l'on décompose σ en produit de n transpositions, la parité de n est

celle de $r(\sigma)$, elle est donc fixée.

Exemple 2.3. :

$$\begin{aligned}(3-1-2) &= (2,3,1),\\ &= (1-2)\,(2-3),\\ &= (2-3)\,(1-3),\\ &= (1-2)\,(1-3\,(2-3)\,(1,2)\end{aligned}$$

On obtient une décomposition de σ^{-1} en inversant l'ordre d'une décomposition de σ.

Les signatures de σ et de σ^{-1} sont égales.

Si σ et σ_1 sont des éléments de $\mathfrak{S}_n$, $\sigma\circ\sigma_1\circ\sigma^{-1}$ a la même signature que σ ; la signature est donc invariante sous l'action des automorphismes intérieurs.

L'ensemble $\mathfrak{A}_n$ des permutations de signature 1, dites paires, est un sous-groupe de $\mathfrak{S}_n$, le **groupe alterné** d'indice n ; ce sous-groupe est invariant d'après la remarque précédente (voir aussi l'exercice 8), $\mathfrak{S}_n/\mathfrak{A}_n$ est isomorphe à $\mathbb{Z}/2\mathbb{Z}$, et $|\mathfrak{A}_n| = n!/2$.

La signature d'un s-cycle est égale à $(-1)^{s+1}$. Il appartient donc à $\mathfrak{S}_n$ si et seulement si s est impair.

Tout commutateur est pair, et appartient donc à $\mathfrak{S}_n$.

Exemple 2.4. Le groupe $\mathfrak{S}_3$ est d'ordre 6, $\mathfrak{A}_3$ est d'ordre 3, donc commutatif, et $\mathfrak{S}_3$ est résoluble.

Exemple 2.5. Le groupe $\mathfrak{S}_4$ est d'ordre 24, $\mathfrak{A}_4$ est d'ordre 12. Les éléments de $\mathfrak{A}_4$ sont l'identité, les produits (commutatifs) de deux 2-cycles à supports disjoints :

$$\begin{cases}\sigma_1 = (1-2)\,(3-4) = (2,1,4,3),\\ \sigma_2 = (1-3)\,(2-4) = (3,4,1,2),\\ \sigma_3 = (1-4)\,(2-3) = (4,3,2,1),\end{cases}$$

et les 3-cycles :

$$\begin{cases}\tau_1 = (1-2-3) = (2,3,1,4),\\ \tau_2 = (1-3-2) = (3,1,2,4),\\ \tau_3 = (1-2-4) = (2,4,3,1),\\ \tau_4 = (1-4-2) = (4,1,3,2),\\ \tau_5 = (1-3-4) = (3,2,4,1),\\ \tau_6 = (1-4-3) = (4,2,1,3),\\ \tau_7 = (2-3-4) = (1,3,4,2),\\ \tau_8 = (2-4-3) = (1,4,2,3).\end{cases}$$

Comme, i, j et k étant deux à deux distincts :

$$\sigma_i\circ\sigma_j = \sigma_j\circ\sigma_i = \sigma_k,$$

et :

$$\sigma_i^2 = \sigma_j^2 = \sigma_k^2 = i_d,$$

l'ensemble $K = \{i_d, \sigma_1, \sigma_2, \sigma_3\}$ est le groupe de Klein (exercice 11). Ce sous-groupe est invariant (par les automorphismes intérieurs), $\mathfrak{A}_4/K$ est d'ordre 3, donc commutatif, et $\mathfrak{S}_4$ est résoluble. En effet, on a :

$$\mathfrak{S}_4 \supset \mathfrak{A}_4 \supset K \supset \{i_d\},$$

chacun de ces groupes, à partir du deuxième, est invariant dans le précédent et les quotients sont commutatifs (proposition 2.3).

Proposition 2.7. *Si $n \geq 3$, les 3-cycles engendrent $\mathfrak{S}_n$.*

Démonstration. Toute permutation de $\mathfrak{A}_n$ est produit d'un nombre pair de transpositions, et les produits d'un nombre pair de transpositions appartiennent à $\mathfrak{A}_n$. Leur ensemble est donc $\mathfrak{A}_n$. Or, tout produit de deux transpositions distinctes, donc différent de l'identité, est un 3-cycle ou un produit de 3-cycles. En effet, si i, j, h et k sont deux à deux distincts :

$$(i-j)\,(j-k) = (j-k-i)$$

seule possibilité si $n = 3$, à laquelle il faut ajouter :

$$(i-j)\,(h-k) = (i-j-h)\,(j-h-k)$$

si $n \geq 4$. □

Proposition 2.8. *Si $n \geq 5$, les 3-cycles appartiennent à $\mathfrak{A}_n$.*

Démonstration. Soit $\sigma = (i-j-h) \in \mathfrak{A}_n$. Il existe des naturels $k \leq n$ et $l \leq n$, ces cinq nombres étant deux à deux distincts, tels que :

$$\sigma = (i-k-h)\,(j-l-h)\,(i-h-k)\,(j-h-l).$$

Or $(i-h-k) = (i-k-h)^{-1}$ et $(j-h-l) = (j-l-h)^{-1}$, de sorte que :

$$\sigma = (i-k-h)\,(j-l-h)\,(i-k-h)^{-1}\,(j-l-h)^{-1}.$$

Le 3-cycle σ, élément de $\mathfrak{A}_n$), est donc un commutateur, élément de $D(\mathfrak{A}_n)$. □

Théorème 2.6. *Si $n \geq 5$, $\mathfrak{S}_n$ n'est pas résoluble.*

Démonstration. Les 3-cycles, qui sont des commutateurs, c'est- à-dire des éléments de $D(\mathfrak{S}_n)$, engendrent à la fois $\mathfrak{A}_n$ et $D(\mathfrak{A}_n)$, qui sont donc égaux, et $D(\mathfrak{S}_n) = \mathfrak{A}_n = D(\mathfrak{A}_n)$; pour tout $m \geq 1$ $D^m(\mathfrak{S}_n) = \mathfrak{A}_n$, et $\mathfrak{S}_n$ n'est pas résoluble. □

Théorème 2.7 (de Cayley [1] 1854)**.** *Tout groupe d'ordre n est isomorphe à un sous-groupe de $\mathfrak{S}_n$.*

Démonstration. Soit G un groupe d'ordre n, noté multiplicativement, et g un élément quelconque. L'homothétie :

$$\begin{array}{rccc} \tau_{\rm g}: & G & \to & G \\ & x & \mapsto & gx \end{array}$$

est injective ($\tau_{\rm g}(x) = e \iff x = g^{-1}$), surjective ($\forall y \in G, \tau_{\rm g}(g^{-1}y) = y$), donc bijective, et c'est une permutation de G. Si l'on numérote les éléments de G, on peut représenter $\tau_{\rm g}$ comme un élément $\sigma_{\rm g}$ de $\mathfrak{S}_n$, et l'application :

$$g \mapsto \tau_{\rm g} \mapsto \sigma_{\rm g}$$

définit une injection de $i : G \to \mathfrak{S}_n$. On a alors, pour deux éléments quelconques de G, $i(g'g) = \sigma_{\rm g'} \circ \sigma_{\rm g}$, et $i(G)$ est un sous-groupe de $\mathfrak{S}_n$. □

2.12 Exercices

G et G_i désignent des groupes finis.

(1) Montrer que l'intersection finie de sous-groupes est un sous-groupe.

(2) Soit $\phi : G_1 \to G_2$ un morphisme de groupes ; montrer que :
- $\mathrm{Im}(\phi)$ est un sous-groupe de G_2 ;
- l'image réciproque d'un sous-groupe de G_2 est un sous-groupe de G_1 ;
- $\mathrm{Ker}(\phi)$ est un sous-groupe invariant ;
- ϕ induit un isomorphisme $\overline{\phi} : G_1/\mathrm{Ker}(\phi) \to \mathrm{Im}(\phi)$.

(3) Montrer que $C_x = \{y \in G \,|\, xy = yx\}$, $x \in G$, est un sous-groupe de G.

(4) Comparer $\phi_x \circ \phi_y$ et ϕ_{xy}. Montrer que $\mathrm{Int}(G)$ est un groupe.

(5) Montrer l'équivalence : $\phi_y(x) = x \iff y \in C_x$.

(6) Vérifier que la relation $x \,\Re\, y \iff [\exists \sigma \in \mathrm{Int}(G) : y = \sigma(x)]$ est une équivalence dans le groupe G. Exprimer le cardinal de la classe de x en fonction de $|C_x|$.

(7) Montrer que l'application $\phi : G \to \mathrm{Int}(G)$, $\phi(x) = \phi_x$, est un morphisme de groupes dont le noyau est le centre C de G ; en déduire que $\mathrm{Int}(G) \cong G/C$.

(8) Regardant les classes, montrer qu'un sous-groupe d'ordre n d'un groupe d'ordre $2n$ est invariant.

1. Arthur Cayley (1821-1895), mathématicien britannique.

(9) Etudier complètement le groupe de l'hexagone régulier : définir les éléments et leur ordre, les sous-groupes et les sous-groupes invariants.

(10) Comparer les groupes du triangle équilatéral et du tétraèdre régulier à, respectivement, $\mathfrak{S}_3$ et $\mathfrak{S}_4$.

(11) Construire tous les groupes d'ordre 4, 6 et 8.

(12) Montrer que dans un groupe commutatif l'ordre du produit de deux éléments engendrant des groupes dont l'intersection est triviale est le ppcm des ordres des facteurs.

(13) Si H et K sont des sous-groupes d'un groupe commutatif G, montrer que les groupes quotients $H/(H \cap K)$ et $[H + K]/K$ sont isomorphes.

2.13 Correction des exercices

(1) Soient H et K deux sous-groupes de G. L'intersection $H \cap K$ contient au moins le neutre de G. Quels que soient x et y dans $H \cap K$, ils appartiennent à H et $xy^{-1} \in H$; de même pour K, et $xy^{-1} \in H \cap K$; $H \cap K$ est donc un sous-groupe.

Soit $(H_i)_{1 \leq i \leq n}$ une famille de sous-groupes de G, et posons $K_p = \cap_{i=1}^{p} H_i$, $1 \leq p \leq n$. D'après la première partie, si l'un des K_p est un sous-groupe, $K_{p+1} = K_p \cap H_{i+1}$ en est un. Or $K_1 = H_1$ est un sous-groupe, donc les K_p sont tous des sous-groupe, jusqu'à K_n.

(2) Soient e_1 et e_2 les neutres respectifs de G_1 et G_2, y_1 et y_2 deux éléments de $\mathrm{Im}(\phi)$; il existe donc deux éléments, x_1 et x_2 de G_1 tels que $y_i = \phi(x_i)$. Alors :

$$y_1 y_2 = \phi(x_1)\, \phi(x_2) = \phi(x_1 x_2)$$

et $y_1 y_2$ appartient à $\mathrm{Im}(\phi)$. Comme :

$$y_1^{-1} = (\phi(x_1))^{-1} = \phi(x_1^{-1}) \in \mathrm{Im}(\phi)$$

et :

$$e_2 = \phi(e_1) \in \mathrm{Im}(\phi),$$

$\mathrm{Im}(\phi)$ est bien un sous-groupe de G_2. Soient x_1 et x_2 deux éléments de $\mathrm{Ker}(\phi)$: $\phi(x_1) = \phi(x_2) = e_2$; alors :

$$\phi(x_1 x_2) = \phi(x_1)\, \phi(x_2) = (e_2)^2 = e_2$$

et $x_1 x_2$ appartient, ainsi que e_1, à $\mathrm{Ker}(\phi)$, qui est donc un sous-groupe. Ce sous-groupe est invariant ; en effet, $x \in G$ et $k \in \mathrm{Ker}(\phi)$ étant des éléments quelconques, $x^{-1} k x$ appartient à $\mathrm{Ker}(\phi)$:

$$\phi(x^{-1} k x) = \phi(x^{-1})\, \phi(k)\, \phi(x) = (\phi(x))^{-1}\, \phi(x) = e_2.$$

Le morphisme ϕ prend la même valeur sur tous les éléments d'une classe modulo ϕ et induit donc une application :

$$\overline{\phi} : G_1/\mathrm{Ker}(\phi) \to \mathrm{Im}(\phi),$$

surjective par hypothèse, injective car si deux éléments de G_1 ont la même image, $\phi(x_1) = \phi(x_2)$, on a :

$$\phi(x_1\, x_2^{-1}) = \phi(x_1)\,(\phi(x_2))^{-1} = e_2,$$

et ils sont dans la même classe. Si on note $\overline{x}$ la classe de x, on a par définition $\overline{\phi}(\overline{x}) = \phi(x)$, d'où :

$$\overline{\phi}(\overline{x}\,\overline{y}) = \phi(x\,y) = \phi(x)\,\phi(y) = \overline{\phi}(\overline{x})\,\overline{\phi}(\overline{y}),$$

et $\overline{\phi}$ est bien un morphisme de groupes bijectif, donc un isomorphisme.

(3) Soient e le neutre de G et y et z des éléments commutant avec x ; alors leur produit commute avec x :

$$x(yz) = (xy)z = (yx)z = y(xz) = y(zx) = (yz)x,$$

e également : $ex = x = xe$, et enfin y^{-1} :

$$xy = yx \Rightarrow x = yxy^{-1} \Rightarrow y^{-1}x = xy^{-1}.$$

(4) Pour un élément quelconque z du groupe, on a :

$$(\phi_x \circ \phi_y)(z) = x(yzy^{-1})x^{-1} = (xy)z(xy)^{-1} = \phi_{xy}(z),$$

d'où :

$$\phi_x \circ \phi_y = \phi_{xy},$$

et le produit de deux automorphismes intérieurs est un automorphisme intérieur. L'élément neutre est ϕ_e, et ϕ_x a pour inverse $\phi_{x^{-1}}$.

(5) Ceci découle de la suite d'équivalences :

$$\phi_y(x) = x \iff yxy^{-1} = x \iff yx = xy \iff y \in C_x.$$

(6) La relation étant réflexive (pour σ égal à l'identité), symétrique :

$$\begin{array}{rcl} x\,\Re\,y & \iff & \sigma(x) = y \text{ (pour un } \sigma \in \mathrm{Int}(G)) \\ & \iff & x = \sigma^{-1}(y) \\ & \iff & y\,\Re\,x \ (\sigma \in \mathrm{Int}(G) \Rightarrow \sigma^{-1} \in \mathrm{Int}(G)) \end{array}$$

et transitive :

$$\begin{array}{l} x\,\Re\,y \\ y\,\Re\,z \end{array} \quad \Rightarrow \quad \begin{array}{l} y = \sigma_1(x) \\ z = \sigma_2(y) \end{array} \quad \Rightarrow z = \sigma_2 \circ \sigma_1(x) \Rightarrow x\,\Re\,z \ (\sigma_2 \circ \sigma_1 \in \mathrm{Int}(G))$$

est une équivalence. Le cardinal de la classe de x est égal au nombre d'automorphismes intérieurs donnant de x des images différentes de x ; comme (exercice 5) :

$$\sigma_y(x) = x \iff y \in C_x$$

ce nombre est égal à celui des classes modulo C_x, soit à $|G| \,/\, |C_x|$.

(7) On a vérifié dans l'exercice 4 que $\phi_x \circ \phi_y = \phi_{xy}$. Il reste à voir que ϕ_x est égal à l'identité si et seulement si x appartient au centre de G :

$$\phi_x = I_d \iff \forall y \in G,\, xyx^{-1} = y \iff xy = yx \iff x \in C.$$

On en déduit que ϕ est défini et injectif sur les classes modulo C ; or l'ensemble de ces classes, le centre étant un sous-groupe invariant, est muni d'une structure de groupe : le groupe quotient G/C.

(8) Il y a deux classes à gauche : celle du neutre formée des éléments du sous-groupe et une autre, et deux classes à droite : celle du neutre formée des éléments du sous-groupe et une autre ; ces classes étant disjointes et la première des classes à gauche étant confondue avec la première des classes à droite, les secondes sont aussi confondues, et la condition d'existence du groupe quotient est remplie.

(9) La rotation r d'angle $\pi/3$, engendre un sous-groupe R, d'ordre 6, qui a lui-même un sous-groupe d'ordre 2 engendré par r^3 et un sous-groupe d'ordre 3 engendré par r^2.

Les points étant nommés dans l'ordre circulaire, il y a trois symétries, s_1, s_2, s_3 par rapport, respectivement, aux diagonales A_1A_4, A_2A_5, A_3A_6 et trois autres, t_1, t_2, t_3, par rapport aux médiatrices des segments, dans l'ordre, A_1A_2, A_2A_3, A_3A_4.

Les calculs donnent, 1 étant le successeur de 3 pour l'indice i :

$$s_i \circ r = t_{i+2},\ r \circ s_i = t_i,$$

$$t_i \circ r = s_i,\ r \circ t_i = s_{i+1},$$

$$t_i \circ s_i = s_i \circ t_{i+2} = r,$$

$$t_i \circ s_{i+1} = s_i \circ t_i = r^5,$$

$$t_i \circ s_{i+2} = s_i \circ t_{i+1} = r^3,$$

$$s_i \circ s_{i+1} = r^4,\ s_i \circ s_{i+2} = r^2,$$

$$t_i \circ t_{i+1} = r^4,\ t_i \circ t_{i+2} = r^2,$$

$$s_i \circ s_i = t_i \circ t_i = r^6 = I.$$

De l'écriture ensembliste $RS = SR = T$, $ST = TS = R$, $TR = RT = S$, $SS = TT = R$ (R étant l'ensemble des r^i, S, celui des s_i, T, celui des t_i), on déduit que R est l'unique sous-groupe invariant non trivial (exercice 8).

Le groupe de l'hexagone régulier est visiblement résoluble.

(10) Les sommets du tétraèdre régulier T sont A_1, A_2, A_3 et A_4 ; chaque segment est une arête de longueur l ; toute permutation sur les A_i donne donc une isométrie de T, et le groupe des isométries de T est isomorphe au groupe $\mathfrak{S}_4$ des permutations sur quatre éléments ; ce n'est pas vrai pour le carré, dont les deux diagonales mesurent $l\sqrt{2}$ si les quatre côtés sont de longueur l : le groupe du carré est un sous-groupe de $\mathfrak{S}_4$. Les éléments de $\mathrm{Isom}(T)$ sont :

- l'identité, d'ordre 1,

- les six symétries $s_{i,j}$ ($s_{i,j}$ laisse invariants A_i et A_j et permute les deux autres sommets), d'ordre 2,

- les trois demi-tours $d_1 = s_{1,2} \circ s_{3,4}$, $d_2 = s_{1,3} \circ s_{2,4}$, $d_3 = s_{2,3} \circ s_{1,4}$ d'ordre 2,

- les huit rotations d'ordre 3 : quatre r_i (d'angle $2\pi/3$, laissant A_i invariant) et leurs carrés,

- les six composées d'ordre 4 en $s_{i,j} \circ r_h$: $t_1 = s_{1,2} \circ r_3$, $t_3 = s_{2,4} \circ r_1$, $t_5 = s_{1,3} \circ r_4$ et leurs inverses $t_{i+1} = t_i^{-1}$.

Pour établir la table de multiplication du groupe, le plus simple est de travailler dans la base affine formée des quatre points et de représenter les éléments par des matrices à quatre lignes et autant de colonnes, la colonne d'indice i donnant la nouvelle place de A_i ; ainsi, la rotation r_1, qui effectue le déplacement :

$$(A_1\, A_2\, A_3\, A_4) \to (A_1\, A_3\, A_4\, A_2),$$

est représentée par la matrice :

$$R_1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

Les calculs sont assez rapides à la main mais beaucoup plus avec un ordinateur et un logiciel approprié. Les sous-groupes sont, à part le centre réduit à l'identité, les trois groupes D_i engendrés par les demi-tours (d'ordre 2), les six groupes $S_{i,j}$ engendrés par les symétries (d'ordre 2), les quatre groupes R_i engendrés par les rotations (d'ordre 3), les trois groupes T_1, T_3, T_5, engendrés respectivement par t_1, t_3, t_5, (d'ordre 4), T_i admettant D_i comme sous-groupe ; tous ces sous-groupes sont cycliques ; il y a le sous-groupe engendré par toutes les rotations et tous les demi-tours, d'ordre 12, donc invariant d'après l'exercice 8, les sous-groupes d'ordre 6 : G_1 engendré par r_1 et les $s_{1,j}$, G_2 engendré par r_2 et les $s_{2,j}$, G_3 engendré par r_3 et les $s_{3,j}$, avec $G_i \cap G_j = S_{i,j}$ ...

Le groupe du triangle équilatéral, isomorphe à $\mathfrak{S}_3$, est engendré par une rotation d'ordre 3 et les symétries par rapport à chacune des trois médiatrices, engendrant des sous-groupes d'ordre 2.

(11) Le groupe cyclique $\mathbb{Z}/4\mathbb{Z}$ est d'ordre 4 ; la seule autre possibilité est un groupe ayant trois éléments d'ordre 2 en plus du neutre, c'est le groupe de Klein (commutatif) :

$$K = \{e, a, b, c \,|\, ab = c,\ bc = a,\ ca = b,\ a^2 = b^2 = c^2 = e\}.$$

Il est isomorphe au groupe additif de l'espace vectoriel $\mathbb{F}_4$ de dimension 2 sur $\mathbb{F}_2$.

Pour les groupes d'ordre 6, il y a d'abord $\mathbb{Z}/6\mathbb{Z}$, cyclique, puis $\mathfrak{S}_3$; il n'y en a pas d'autre car un tel groupe doit avoir au moins un élément d'ordre 3 et un élément d'ordre 2 ; l'élément d'ordre 3, a, engendre le sous-groupe invariant :

$$A = \{a, a^2, a^3 = e\},$$

et il reste trois éléments dont les classes modulo A sont d'ordre 2, et dont les carrés sont donc dans A ; si ces trois éléments, b, c, d, ont pour carré a ou a^2, ils sont d'ordre 6, le groupe est alors cyclique, donc isomorphe à $\mathbb{Z}/6\mathbb{Z}$ (deux groupes cycliques de même ordre sont évidemment isomorphes : il suffit de faire correspondre un générateur de l'un avec un générateur de l'autre) ; si leur carré est le neutre, ils sont d'ordre 2, le produit de deux d'entre eux est égal au troisième, les autres choix menant à des absurdités, et on retrouve la rotation d'ordre 3 et les trois symétries du triangle équilatéral ; le groupe est isomorphe à $\mathfrak{S}_3$ (exercice 10).

Pour les groupes d'ordre 8, les ordres maximum possibles des éléments sont 2, 4 et 8 ; s'il y a un élément d'ordre 8, le groupe est isomorphe à $\mathbb{Z}/8\mathbb{Z}$.

Si l'ordre maximal est 4, l'élément correspondant h engendre un sous-groupe invariant (exercice 8) H isomorphe à $\mathbb{Z}/4\mathbb{Z}$, et les possibilités sont :

$$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{(a, b) \,|\, a \in \mathbb{Z}/4\mathbb{Z},\ b \in \mathbb{Z}/2\mathbb{Z}\},$$

$$\Big(\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}\Big) \,/\, H,\ H \cong \mathbb{Z}/2\mathbb{Z},$$

$$(K \times \mathbb{Z}/4\mathbb{Z}) \,/\, (\mathbb{Z}/2\mathbb{Z}),\ K \text{ étant le groupe de Klein.}$$

La première convient ; pour la deuxième, H doit être le sous-groupe engendré par $(2, 2)$ si l'on ne veut pas retrouver le premier cas ; la troisième redonne la première si l'on veut avoir un élément d'ordre 4.

Si l'ordre maximal est 2, le groupe est isomorphe au groupe additif de l'espace vectoriel F_8 de dimension 3 sur F_2.

Le groupe Q engendré par les matrices :

$$a = \begin{pmatrix} i & 0 \\ 0 & 1 \end{pmatrix} \text{ et } b = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

est le **groupe des quaternions**.

Posant $ab = c$, $Id = 1$, on a :

$$a^2 = b^2 = c^2 = abc = -1.$$

Ses éléments sont donc ± 1, $\pm a$ et $\pm b$, $\pm c$. Il a six éléments d'ordre 4 ($\pm a$, $\pm b$ et $\pm c$), un seul d'ordre 2 (-1) en plus du neutre.

(12) Soient a et b, $a \neq b$, respectivement d'ordre p et q dans un groupe commutatif ; quel est l'ordre de ab ? Comme :

$$(ab)^m = a^m b^m = e \iff a^m = b^{-m} = e,$$

m doit être à la fois multiple de p et de q ; l'ordre de ab, la plus petite valeur possible non nulle de m, est donc le ppcm de p et q. Ce n'est plus vrai pour un groupe non commutatif (exercice 9).

(13) Rappelons que, G étant commutatif, $[H + K] = H + K$. Soient :

$$i : H \to [H + K]$$

l'injection canonique ($i(x) = x$, tout élément de H appartenant à $[H + K]$) et :

$$\pi : [H + K] \to [H + K]/K$$

la surjection canonique associant un élément à sa classe modulo le sous-groupe K de $[H + K]$. Soit ϕ le morphisme composé :

$$\phi = \pi \circ i : H \to [H + K]/K.$$

Un élément h de H est dans $\mathrm{Ker}(\phi)$ si $i(h)$ est dans K ; il s'ensuit que :

$$\mathrm{Ker}(\phi) = H \cap K.$$

D'autre part, ϕ est surjectif, car un élément de $[H + K]$ non congru à 0 modulo K doit appartenir à H. D'après l'exercice 2, ϕ induit un isomorphisme :

$$\overline{\phi} : H/\mathrm{Ker}(\phi) \to \mathrm{Im}(\phi)$$

et les groupes $H/(H \cap K)$ et $[H + K]/K$ sont isomorphes.

Si G, H et K sont des espaces vectoriels, et les morphismes des applications linéaires, le résultat est conservé, avec la même démonstration.

3 Sous-groupes d'un groupe fini

La décomposition d'un groupe fini en sous-groupes est importante en automatisme, en chimie, en recherche médicale... et en Mathématiques.

3.1 Définitions

Les définitions basiques sont données dans Groupes. G désigne un groupe fini de neutre e_{G} (ou simplement e) et p un nombre premier. Rappelons que l'**ordre** de G, noté $|G|$, est le nombre de ses éléments (son cardinal), que l'**ordre** d'un élément g de G, noté $|g|$, est le plus petit entier naturel $k > 0$ tel que $g^k = e$. Enfin, deux sous-groupes H et H' de G sont **conjugués** s'il existe $g \in G$ tel que $H' = gHg^{-1}$, et H est **distingué**, **invariant** ou encore **normal** si, pour tout $g \in G$, $gHg^{-1} = H$.

Le **groupe diédral** D_n est le groupe des isométries du polygone régulier à n sommets. Les isométries de D_n sont des isométries du plan, donc des rotations ou des réflexions (voir *Systèmes et Matrices*, même page web). Les rotations seront dites **positives** et les réflexions **négatives**, d'après le signe de leur déterminant. Si r est la rotation d'angle $2\pi/n$, il contient les n puissances de r (r^n est l'identité). Si n est impair, il contient les n symétries d'axe passant par un sommet et le milieu du côté opposé ; si n est pair, il contient les $n/2$ symétries d'axe passant par deux sommets opposés et les $n/2$ symétries d'axe passant par les milieux de deux côtés opposés. L'ordre de D_n est donc dans tous les cas égal à $2n$.

Si p est un nombre premier, un groupe d'ordre p^n, $n \geq 1$, est un p-**groupe**. Tous ses sous-groupes stricts sont d'ordre p^k, $0 < k < n$.

Un p-**sous-groupe de Sylow**, ou p-Sylow, d'un groupe d'ordre $p^n m$, p (premier) ne divisant pas m et $n \geq 1$, est un sous-groupe d'ordre p^n, donc un p-sous-groupe maximal. Rappelons que la **valuation** en p d'un entier q, $\text{val}_p(q)$ est le plus grand entier n tel que p^n divise q, et que $\text{val}_p(q'q) = \text{val}_p(q') + \text{val}_p(q)$, $\text{val}_p(q'/q) = \text{val}_p(q') - \text{val}_p(q)$.

Remarque : un sous-groupe d'un groupe d'ordre $p^n m$, avec les conditions ci-dessus, est un p-Sylow si et seulement si sa valuation en p est égale à celle du groupe.

Soient H et K deux sous-groupes d'un groupe G, $H \cap K$ étant réduit à l'élément neutre et H étant distigué. Le **produit direct** de H et K, noté $H \times K$, est l'ensemble produit muni de la loi de composition, quels que soient les couples (h, k) et (h', k') de $H \times K$, $(h, k)(h', k') = (hh', kk')$.

Si $f : K \to \text{Aut}(H)$ est un morphisme de groupes, on définit leur **produit semi-direct** selon f, $G \times_f H$, comme étant le même ensemble muni de la loi $(h, k)\,(h', k') = (h\, f(k)(h'), kk')$. Si l'image de f est réduite à l'identité de H, on a $f(k)(h') = h'$, et on retrouve le produit direct.

Montrons que $G \times_f H$ est un groupe. L'élément neutre est $(e_{\text{H}}, e_{\text{K}})$ puisque $f(e_{\text{K}})$ est l'identité de H. L'inverse de (h, k) est $(f\,(k^{-1})(h^{-1}), k^{-1})$. Montrons

l'associativité, en notant f_k pour $f(k)$:

$$\begin{aligned}(h,k)\Big((h',k')\,(h",k")\Big) &= (h,k)\,(h'\,f_{k'}(h"),k'k") \\ &= (h\,f_k\Big((h'f_{k'}(h")\Big),kk'k") \\ &= (h\,f_k(h')\,f_{kk'}(h"),kk'k")\end{aligned}$$

et :

$$\begin{aligned}\Big((h,k)\,(h',k')\Big)\,(h",k") &= (h\,f_k(h'),kk')\,(h",k") \\ &= (h\,f_k(h')\,f_{kk'}(h"),kk'k").\end{aligned}$$

3.2 Théorèmes

Théorème 3.1. *Le centre d'un p-groupe G n'est pas réduit à l'élément neutre.*

Démonstration. Supposons le centre C réduit au neutre, et donc $\mathrm{Int}(G)$ isomorphe à G, et $|G| = p^n$, $n \geq 2$, car, si $n = 1$, G est cyclique, donc commutatif, et $C = G$; à tout élément x de G associons sa classes d'équivalence modulo la relation définie dans l'exercice 6 sur les groupes :

$$\overline{x} = \{\sigma(x) \,|\, \sigma \in \mathrm{Int}(G)\}$$

dont le nombre d'éléments est :

$$|\overline{x}| = \frac{|\mathrm{Int}(G)|}{|C_x|}$$

C_x étant le sous-groupe $\{y \in G \,|\, xy = yx\}$ (voir l'exercice 3 sur les groupes), d'ordre p^k, $1 \leq k \leq n$:

$$|\overline{x}| = p^{n-k}.$$

La classe du neutre est réduite à lui-même puisque $C_e = G$: $|\overline{e}| = 1$.

Si x n'est pas le neutre, C_x est le sous-groupe strict (e étant par hypothèse l'unique élément à commuter avec tous les autres) constitué des éléments de G commutant avec x (il contient au moins e et les puissances de x) ; son ordre est une puissance de p, p^k, $1 \leq k < n$, et $|\overline{x}| = p^h$, $h = n - k \geq 1$. Les classes constituent une partition de G, et $|G|$ est égal à la somme de leurs cardinaux ; toutes les classes, à l'exception de $|\overline{e}| = 1$, ont pour cardinal une puissance non nulle de p ; $|G|$ est donc égal à un multiple de p plus 1, ce qui est absurde : le centre ne peut doncêtre réduit au neutre. □

Les p-groupe d'ordre p (cycliques) ou p^2 (exercice 9) sont commutatifs.

Rappelons enfin les théorèmes de Lagrange (th.2.1), de Cauchy (th.2.3) et de Cayley (th.2.5) :

Théorème 3.2. *L'ordre d'un élément de G divise $|G|$.* □

Théorème 3.3. *Si p divise $|G|$, G contient un élément d'ordre p.* □

Théorème 3.4. *Tout groupe fini est isomorphe à un sous-groupe de $\mathfrak{S}_n$.* □

3.3 Théorèmes de Sylow

Théorème 3.5 (Premier théorème de Sylow)**.** *Si p, premier, divise $|G|$, G possède un p-sous-groupe de Sylow.*

Démonstration. Il existe des naturels m, non multiple de p, et $n \geq 1$, tels que $|G| = N = p^n m$. Nous allons décomposer la démonstration en plusieurs parties.

Nous prouvons d'abord (lemme 3.1.) que si un groupe possède la propriété, ses sous-groupes la possèdent également, ainsi d'ailleurs que tout groupe qui lui est isomorphe.

Nous prouvons ensuite (lemme 3.3.2.) que, $\mathbb{F}_p$ étant le corps $\mathbb{Z}/p\mathbb{Z}$ des classes d'entiers modulo p et E l'espace vectoriel $(\mathbb{F}_p)^N$, le groupe $\mathrm{Aut}(E)$ possède la propriété.

Le groupe symétrique $\mathfrak{S}_N$, isomorphe à un sous-groupe de $\mathrm{Aut}(E)$ possède la propriété.

On termine en se rappelant que G est isomorphe à un sous-groupe de $\mathfrak{S}_N$.

Lemme 3.1. Supposons que G possède un p-Sylow S, et soit H un sous-groupe de G dont l'ordre a une valuation en p non nulle. Notons que, $\forall g \in G$, gSg^{-1}, sous-groupe du même ordre que S, est un p-Sylow de G. Faisons opérer G sur l'ensemble G/S des classes à gauche modulo S :

$$(g', gS) \mapsto g'gS.$$

Le fixateur de la classe gS est l'ensemble des $g' \in G$ tels que $g'gS = gS$, ou $g^{-1}g'gS = S$, c'est- à-dire tels que $g^{-1}g'g \in S$, ou encore tels que $g' \in gSg^{-1}$:

$$\mathrm{Fix}(gS) = gSg^{-1}.$$

L'ensemble $gSg^{-1} \cap H$ est un sous-groupe de H. Si on fait opérer H sur G/S, on aura :

$$\mathrm{Fix}(gS) = gSg^{-1} \cap H,$$

et on obtient une partition de G/S en classes modulo H, et le cardinal de G/S est la somme de leurs cardinaux.

Le cardinal d'une classe est égal à $\dfrac{|H|}{|gSg^{-1} \cap H|}$.

Le cardinal de G/S étant premier avec p, il y a au moins une classe, c, dont le cardinal n'est pas multiple de p : $\mathrm{val}_p(\mathrm{Card}(c)) = 0$. Comme :

$$\mathrm{Card}(c) = \frac{|H|}{|gSg^{-1} \cap H|},$$

on a :

$$0 < \mathrm{val}_p(H) = \mathrm{val}_p(|gSg^{-1} \cap H|),$$

ce qui prouve que $gSg^{-1} \cap H$ est un p-Sylow de H.

Lemme 3.2. Les groupes $\mathrm{Aut}(E)$ et $\mathrm{GL}_N(\mathbb{F}_p)$ sont isomorphes, une matrice de déterminant non nul étant associée bijectivement à un automorphisme (voir

Systèmes et Matrices, même page web), les colonnes de la matrice étant les images par l'automorphisme des vecteurs de la base canonique (ou d'une base quelconque). Ainsi, l'automorphisme u de $\mathbb{F}_p^2$ tel que :

$$u(e_1) = a\,e_1 + b\,e_2,\ u(e_2) = c\,e_1 + d\,e_2,$$

avec $D = ad - bc \neq 0$, dont l'application réciproque est définie par :

$$u^{-1}(e_1) = \frac{1}{D}(de_1 - be_2),\ u^{-1}(e_2) = \frac{1}{D}(-ce_1 + ae_2),$$

est représenté par la matrice :

$$M(u) = \begin{pmatrix} a & c \\ b & d \end{pmatrix}.$$

Calculons l'ordre de $\mathrm{GL}_N(\mathbb{F}_p)$, donc de $\mathrm{Aut}(E)$, sachant chaque vecteur-colonne est non nul et indépendant des précédentes, et qu'il y a p^N vecteurs distincts dans E. Les k premières colonnes choisies étant indépendantes, elles engendrent un espace vectoriel de dimension k sur $\mathbb{F}_p$, dont le nombre d'éléments non nuls est égal à $p^k - 1$. Il y a donc $(p^N - 1) - (p^k - 1) = p^k\,(p^{N-k} - 1)$ choix possibles pour la $(k+1)^{\text{ième}}$ colonne.

Choix de la première colonne : $p^N - 1$.

Choix de la deuxième colonne : $p\,(p^{N-1} - 1)$.

...

Choix de la dernière colonne : $p^{N-1}\,(p - 1)$.

La valuation en p des termes $p^{N-k} - 1$ est nulle, et celle du produit de ces choix est égale à $p\,p^2 \cdots p^{N-1} = p^{N\,(N-1)/2}$, et donc :

$$\mathrm{val}_p(\mathrm{Aut}(E)) = p^{N\,(N-1)/2}.$$

Considérons maintenant le groupe $\mathfrak{T}_N$ des matrices de $\mathrm{GL}_N(\mathbb{F}_p)$ triangulaires supérieures à diagonale principale de 1, c'est- à-dire de la forme :

$$T = \begin{pmatrix} 1 & t_{1\,2} & \cdots & \cdots & t_{1\,N} \\ 0 & 1 & t_{2\,2} & \cdots & t_{2\,N} \\ \vdots & \ddots & \ddots & \cdots & \cdots \\ \vdots & \cdots & \ddots & 1 & t_{N-1\,N} \\ 0 & \cdots & \cdots & 0 & 1 \end{pmatrix}$$

stable par inversion et par produit. Il y a $1 + 2 + \cdots + N - 1 = N\,(N-1)/2$ coefficients $t_{i\,j}$ à choisir sans conditions ; l'ordre de $\mathfrak{T}_N$ est donc $p^{N\,(N-1)/2}$, et sa valuation en p est égale à celle de $\mathrm{GL}_N(\mathbb{F}_p)$, ce qui montre que $\mathfrak{T}_N$ est un p-Sylow de $\mathrm{GL}_N(\mathbb{F}_p)$, et donc, par isomorphisme, que $\mathrm{Aut}(E)$ possède un p-Sylow.

Lemme 3.3 A toute permutation $\sigma \in \mathfrak{S}_N$ on peut associer l'automorphisme défini par $u_\sigma(e_i) = e_{\sigma(i)}$, dont le déterminant est égal à $\epsilon_\sigma = \pm 1$. L'application :

$$\begin{array}{rccc} u: & \mathfrak{S}_N & \to & \mathrm{Aut}(E) \\ & \sigma & \mapsto & u_\sigma \end{array}$$

est injective, et telle que :

$$\begin{cases} u(i_d) = I_E, \\ u(\sigma' \circ \sigma) = u(\sigma') \circ u(\sigma) \end{cases}$$

puisque, quels que soient les éléments écrits :

$$u(\sigma' \circ \sigma)(e_i) = e_{\sigma' \circ \sigma(i)} = u(\sigma')(e_{\sigma'(i)} = \big(u(\sigma') \circ u(\sigma)\big)(e_i).$$

C'est donc un morphisme injectif de groupes, et $\mathfrak{S}_N$ est isomorphe à un sous-groupe de $\mathrm{Aut}(E)$.

Le groupe G, enfin, est isomorphe à un sous-groupe de $\mathfrak{S}_N$ (théorème 2.5, de Cayley), et possède donc un p-Sylow. □

Théorème 3.6 (deuxième théorème de Sylow)**.** *Les p-sous-groupe de Sylow de G sont conjugués et leur nombre divise $|G|$.*

Démonstration. Soient S et S' deux p-Sylow de G, d'ordre p^n. Il existe $g \in G$ tel que gSg^{-1} soit un p-Sylow de S', donc égal à S', ce qui prouve le premier point.

Le groupe G agit transitivement sur l'ensemble Σ de ses p-Sylow d'après le premier point, et donc $\mathrm{Card}(\Sigma)$ divise $|G|$. □

Théorème 3.7 (troisième théorème de Sylow)**.** *Le nombre des p-sous-groupes de Sylow de G est congru à 1 modulo p.*

Démonstration. Faisons opérer un p-Sylow S sur Σ par conjugaison ; S est évidemment fixe pour cette action. Le cardinal d'une orbite divisant $|S|$, c'est une puissance de p, éventuellement $1 = p^0$. Soit S' un p-Sylow fixe, et $H = [S \cup S']$ le sous-groupe engendré par les éléments de S et de S'. On sait que $H \cap S = S$ et $H \cap S' = S'$ sont des p-Sylow de H ; ils donc conjugués modulo H :

$$\exists h \in H \ : \ hS'h^{-1} = S.$$

Le fixateur de S' dans H, qui contient évidemment S', contient S par hypothèse : c'est donc H ; on a donc $hS'h^{-1} = S'$, et $S' = S$. L'orbite de S a un seul élément, S ; c'est la seule orbite à un élément, les autres ayant un cardinal divisible par p ; le cardinal de Σ est donc un multiple de p plus 1. □

3.4 Exercices

(1) Donner tous les groupes d'ordre 4.
(2) Etudier le groupe $\mathfrak{S}_3$
(3) Etudier le groupe D_3.
(4) Donner tous les groupes d'ordre 6.
(5) Etudier le groupe D_4.
(6) Etudier le groupe D_6.
(7) Montrer que les groupes d'ordre pq, p et q premiers, $p > q$, sont commutatifs.
(8) Montrer qu'un groupe à centre cyclique est commutatif
(9) Montrer que les groupes d'ordre p^2 sont commutatifs.
(10) Donner tous les p-Sylow de $\mathfrak{S}_4$.

3.5 Correction des exercices

(1) Si le groupe a un élément d'ordre 4, c'est $\mathbb{Z}/4\mathbb{Z}$. Sinon, il a, en plus de l'élément neutre e, trois éléments d'ordre 2, a, b et c, tels que le produit de deux d'entre eux donne le troisième. Il est commutatif. C'est le **groupe de Klein**. C'est aussi celui du rectangle non carré, dont les isométries sont les deux réflexions d'axe joignant les milieux des côtés opposés et leur composée, le demi-tour.

(2) Le groupe des permutations sur trois éléments est d'ordre 6. La permutation circulaire $r(ABC) = BCA$ est d'ordre 3. Les permutations $s_{\mathrm{A}}(ABC) = ACB$, $s_{\mathrm{B}}(ABC) = CBA$ et $s_{\mathrm{C}}(ABC) = BAC$, qui laissent un point fixe, sont d'ordre 2. Le groupe a trois 2-sous-groupes de Sylow (3 divise 6 et est congru à 1 modulo 2), engendrés respectivement par s_{A}, s_{B} et s_{C}, et un 3-sous-groupes de Sylow, engendré par r.

(3) Le groupe des isométries D_3 du triangle équilatéral ABC est d'ordre 6. Il est isomorphe à $\mathfrak{S}_3$ (puisque toute permutation de l'ensemble $\{A, B, C\}$ est une isométrie) et nous conservons les notations. Ses sous-groupes sont d'ordre 2 et 3. Le sous-groupe d'ordre 3, R, engendré par la rotation r d'angle $2\pi/3$ (et isomorphe à $\mathbb{Z}/3\mathbb{Z}$) est invariant (Groupes, exercice 8 ; voir aussi l'exercice 9, plus loin) et il est l'unique 3-sous-groupe de Sylow, car, d'après les théorèmes de Sylow, le nombre de sous-groupes d'ordre 3 divise 6 et est congru à 1 modulo 3.

La réflexion s_{A}, d'axe passant par le sommet A (et commutant B et C), engendre le sous-groupe S_{A}, d'ordre 2 (donc isomorphe à $\mathbb{Z}/2\mathbb{Z}$). On a de même les sous-groupes S_{B} et S_{C}, engendrés respectivement par les symétrie s_{B} et s_{C}. L'identité est notée id. Le nombre des 2-sous-groupes de Sylow divise 6 et est congru à 1 modulo 2. Il y en a un ou trois : c'est donc trois.

Le produit de deux réflexions, étant positif, est une rotation.

Comme $s_{\rm A}\circ s_{\rm B}(A)=B$, on a $s_{\rm A}\circ s_{\rm B}=r$. De même :

$$\begin{array}{rcl} s_{\rm B}\circ s_{\rm A}(A)=C & \Rightarrow & s_{\rm B}\circ s_{\rm A}=r^2 \\ s_{\rm A}\circ s_{\rm C}(A)=C & \Rightarrow & s_{\rm A}\circ s_{\rm C}=r^2, \\ s_{\rm C}\circ s_{\rm A}(A)=B & \Rightarrow & s_{\rm C}\circ s_{\rm A}=r, \\ s_{\rm B}\circ s_{\rm C}(A)=B & \Rightarrow & s_{\rm B}\circ s_{\rm C}=r, \\ s_{\rm C}\circ s_{\rm B}(A)=C & \Rightarrow & s_{\rm C}\circ s_{\rm B}=r^2. \end{array}$$

On voit que D_3 n'est pas commutatif.

Le produit d'une réflexion et d'une rotation, négatif, est une réflexion. On a donc :

$$\begin{array}{rcl} r\circ s_{\rm A}(A)=B & \Rightarrow & r\circ s_{\rm A}=s_{\rm C}, \\ s_{\rm A}\circ r(A)=C & \Rightarrow & s_{\rm A}\circ r=s_{\rm B}, \\ r\circ s_{\rm B}(A)=A & \Rightarrow & r\circ s_{\rm B}=s_{\rm A}, \\ s_{\rm B}\circ r(A)=B & \Rightarrow & s_{\rm B}\circ r=s_{\rm C}, \\ r\circ s_{\rm C}(A)=C & \Rightarrow & r\circ s_{\rm C}=s_{\rm B}, \\ s_{\rm C}\circ r(A)=A & \Rightarrow & s_{\rm C}\circ r=s_{\rm A}. \end{array}$$

On a enfin :

$$\begin{array}{c} r\circ s_{\rm A}\circ r^2=s_{\rm B}, \\ r^2\circ s_{\rm A}\circ r=s_{\rm C}, \\ r\circ s_{\rm B}\circ r^2=s_{\rm C}, \\ r^2\circ s_{\rm B}\circ r=s_{\rm A}, \\ r\circ s_{\rm C}\circ r^2=s_{\rm A}, \\ r^2\circ s_{\rm C}\circ r=s_{\rm B}. \end{array}$$

Le groupe non commutatif D_3 n'est pas isomorphe au produit direct $R\times S_{\rm A}$ qui est commutatif et isomorphe à $\mathbb{Z}/6\mathbb{Z}$ ($(r,s_{\rm A})$ est d'ordre 6). Mais il est isomorphe au produit semi-direct $R\rtimes S_{\rm A}$. Soit en effet $\phi : R\rtimes S_{\rm A}\to D_{\rm A}$ dont les images respectives de $(id,s_{\rm A})$, $(r,s_{\rm A})$, $(r^2,s_{\rm A})$, (id,id), (r,id) et (r^2,id) sont $s_{\rm A}$, $s_{\rm B}$, $s_{\rm C}$, id, r^2 et r. On vérifie que $\phi(x)\phi(y)=\phi(xy)$ quels que soient les éléments écrits. Par exemple $(r^2,id)(id,s_{\rm A})=(r^2,s_{\rm A})$ or $r\circ s_{\rm A}=s_{\rm C}$. Ou encore :

$$(r,s_{\rm A})(r,id)=(r\circ s_{\rm A}\circ r\circ s_{\rm A},s_{\rm A})=(id,s_{\rm A})$$

or $s_{\rm B}\circ r^2=s_{\rm A}$.

Ceci est le modèle pour l'étude de D_{2n+1}, isomorphe au produit semi-direct $\mathbb{Z}/(2n+1)\mathbb{Z}\rtimes\mathbb{Z}/2\mathbb{Z}$.

(4) Si le groupe a un élément d'ordre 6, c'est $\mathbb{Z}/6\mathbb{Z}$. Sinon, il a un élément a d'ordre 2 et un élément b d'ordre 3. Il y a donc les éléments $e=a^2=b^3$, le neutre, a et b^2. Il y a ensuite ab, qui ne peut être égal à l'un des trois premiers, car si $ab=e$, $b=a$, si $ab=a$, $b=e$ et si $ab=b$, $a=e$. Il y a pour des raisons identiques ab^2. On peut avoir $ba=ab^2$, $b^2a=ab$, et on retrouve $\mathfrak{S}_3$, ou $ba=ab$ et $b^2a=ab^2$, et le groupe est commutatif.

Ce dernier groupe est le groupe de la figure F suivante. Considérons sur le cercle unité les neufs points $A_k=e^{2ik\pi/9}$ pour $1\leq k\leq 9$, et le polygone régulier P de sommets A_1, A_2, A_4, A_5, A_7 et A_8. Le groupe de P est engendré par la

rotation r d'angle $2\pi/3$. Il est isomorphe à $\mathbb{Z}/3\mathbb{Z}$. Les points B_1, B_2, B_4, B_5, B_7 et B_8 sont obtenus à partir des A_i par une translation de vecteur v orthogonal au plan de P. Les points A_i et B_i sont les sommets de F. Le groupe de F est engendré par r et par la réflexion s dont le plan est le translaté du plan de P par le vecteur $v/2$. La vérification est aisée ($s = a$ et $r = b$).

(5) L'ordre de D_4, groupe des isométries du carré $ABCD$, est égal à $8 = 2^3$. Il est donc son unique 2-sous-groupe de Sylow. C'est un sous-groupe de $\mathfrak{S}_4$, puisque certaines permutations sur les sommets, par exemple $ABDC$, ne conservent pas les distances.

Le groupe a un unique sous-groupe d'ordre 4, distingué, engendré par la rotation r d'angle $\pi/4$, isomorphe à $\mathbb{Z}/4\mathbb{Z}$.

Les réflexions s_{A}, d'axe AC, s_{B}, d'axe BD, s', d'axe joignant les milieux des côtés AB et CD et s'', d'axe joignant les milieux des côtés BC et AD, engendrent chacune un sous-groupe d'ordre 2, respectivement S_{A}, S_{B}, S' et S''.

Le produit de deux réflexions, positif, est une rotation, celui d'une rotation et d'une réflexion, négatif, est une réflexion. A partir des produits :

$$\begin{array}{rcl}
s_{\mathrm{A}}\circ s_{\mathrm{B}}(A) = C & \Rightarrow & s_{\mathrm{A}}\circ s_{\mathrm{B}} = r^2,\\
s_B\circ s_{\mathrm{A}}(A) = C & \Rightarrow & s_B\circ s_{\mathrm{A}} = r^2,\\
s_{\mathrm{A}}\circ s'(A) = D & \Rightarrow & s_{\mathrm{A}}\circ s' = r^3,\\
s'\circ s_{\mathrm{A}}(A) = B & \Rightarrow & s'\circ s_{\mathrm{A}} = r^2,\\
s_{\mathrm{A}}\circ s''(A) = B & \Rightarrow & s_{\mathrm{A}}\circ s'' = r,\\
s''\circ s_{\mathrm{A}}(A) = D & \Rightarrow & s''\circ s_{\mathrm{A}} = r^3,\\
s_{\mathrm{B}}\circ s'(A) = B & \Rightarrow & s_{\mathrm{B}}\circ s' = r,\\
s'\circ s_{\mathrm{B}}(A) = D & \Rightarrow & s'\circ s_{\mathrm{B}} = r^3,\\
s_{\mathrm{B}}\circ s''(A) = D & \Rightarrow & s_{\mathrm{B}}\circ s'' = r^3,\\
s''\circ s_{\mathrm{B}}(A) = B & \Rightarrow & s''\circ s_{\mathrm{B}} = r,\\
s'\circ s''(A) = C & \Rightarrow & s'\circ s'' = r^2,\\
s''\circ s'(A) = C & \Rightarrow & s''\circ s' = r^2,\\
s'\circ r(A) = A & \Rightarrow & s'\circ r = s_{\mathrm{A}},\\
r\circ s'(A) = C & \Rightarrow & r\circ s' = s_{\mathrm{B}},\\
s''\circ r(A) = C & \Rightarrow & s''\circ r = s_{\mathrm{B}},\\
r\circ s''(A) = A & \Rightarrow & r\circ s'' = s_{\mathrm{A}},\\
s_{\mathrm{A}}\circ r(A) = D & \Rightarrow & s_{\mathrm{A}}\circ r = s'',\\
r\circ s_{\mathrm{A}}(A) = B & \Rightarrow & r\circ s_{\mathrm{A}} = s',\\
s_{\mathrm{B}}\circ r(A) = B & \Rightarrow & s_{\mathrm{B}}\circ r = s',\\
r\circ s_{\mathrm{B}}(A) = D & \Rightarrow & r\circ s_{\mathrm{B}} = s''.
\end{array}$$

On obtient tous les autres. Ainsi $r^2\circ s' = r\circ s_{\mathrm{B}} = s''$, $s_{\mathrm{A}}\circ s_{\mathrm{B}}\circ s_{\mathrm{A}} = s_{\mathrm{B}}$ (puisque $s_{\mathrm{A}}\circ s_{\mathrm{B}} = s_{\mathrm{B}}\circ s_{\mathrm{A}}$), et :

$$r\circ s'\circ r^3 = s_{\mathrm{B}}\circ r^3 = s'\circ r^2 = s_{\mathrm{A}}\circ r = s''.$$

(6) C'est le groupe de l'hexagone régulier $ABCDEF$. Il est d'ordre 12 et contient un ou quatre 3-sous-groupes de Sylow et un ou trois 2-sous-groupes de Sylow. La rotation r d'angle $\pi/3$ engendre un sous-groupe d'ordre 6, distingué

(12=2.6). La rotation r^2 engendre l'unique 3-sous-groupe de Sylow, distingué puisqu'unique. Les réflexions $s_{\rm A}$, $s_{\rm B}$, $s_{\rm C}$ (d'axes respectifs AD, BE, CF), s_1, s_2, s_3 (d'axes passant par les milieux des côtés opposés, $s_1(A) = B$, $s_2(A) = D$, $s_3(A) = F$), et la rotation r^3 engendrent les sept sous-groupes d'ordre 2.

Le groupe n'ayant pas d'élément d'ordre 4, un 2-sous-groupes de Sylow est isomorphe au groupe de Klein. Il nous faut donc trouver trois éléments d'ordre 2, a, b et c, tels que $ab = ba = c$, $ac = ca = b$ et $bc = cb = a$.

On a $s_{\rm A}\circ s_2 = s_2\circ s_{\rm A} = r^3$, $s_{\rm A}\circ r^3 = r^3\circ s_{\rm A} = s_2$ et $s_2\circ r^3 = r^3\circ s_2 = s_{\rm A}$, d'où le 2-sous-groupe de Sylow $\{s_{\rm A}, s_2, r^3\}$. On obtient de même $\{s_{\rm B}, s_3, r^3\}$ et $\{s_{\rm C}, s_1, r^3\}$. Il y a donc trois 2-sous-groupes de Sylow.

(7) Il existe dans un groupe G, de neutre $e_{\rm G}$, d'ordre pq, un élément a d'ordre p, engendrant un groupe cyclique A, de neutre $e_{\rm A}$, isomorphe à $\mathbb{Z}/p\mathbb{Z}$ et un élément b d'ordre q, engendrant un groupe cyclique B, de neutre $e_{\rm B}$, isomorphe à $\mathbb{Z}/q\mathbb{Z}$. L'intersection $A\cap B$ est triviale car un élément d'ordre p et d'ordre q a pour ordre le pgcd de p et q, soit 1. Dans le groupe $A\times B$, on a $(a,b)^p = (a^p, b^p) = (e_{\rm A}, b^p)$ et $(a,b)^{pq} = (e_A, b^{pq}) = (e_A, e_B)$. Le groupe $A\times B$ est donc cyclique d'ordre pq, isomorphe à $\mathbb{Z}/pq\mathbb{Z}$.

L'application $u : A\times B \to G$, $u(a^i, b^j) = a^i b^j$ est un morphisme de groupes. Elle est injective car $u(a^i, b^j) = e_{\rm G}$ équivaut à $a^i b^j = e_{\rm G}$ donc à $a^i = b^{q-j}$; a^i et b^{q-j} appartenant à $A\cap B$ sont égaux à $e_{\rm G}$ et $i = 0$ et $j = q$. Elle est surjective à cause de la finitude et c'est un isomorphisme.

(8) Si le centre C du groupe G est cyclique, soit $\gamma \in G$ tel que $\overline{\gamma}$ engendre C. On a alors :

$$\forall g \in G, \exists k \in \mathbb{N} : \overline{g} = \overline{\gamma}^k$$

de sorte que :

$$\exists h \in C : g\,\gamma^{-k} = h$$

et que $g = h\,\gamma^k = \gamma^k\,h$, puisque h commute avec tous les éléments. Si g_1 et g_2 sont deux éléments quelconques de G, il existe des naturels k_1 et k_2 et des éléments h_1 et h_2 de C tels que $g_1 = h_1\,\gamma^{k_1}$ et $g_2 = h_2\,\gamma^{k_2}$, et l'on a :

$$\begin{array}{rcl} g_1 g_2 & = & h_1\,\gamma^{k_1}\,\gamma^{k_2}\,h_2 \\ & = & h_1 h_2 \gamma^{k_1}\gamma^{k_2} \\ & = & h_2\,\gamma^{k_2}\,h_1\,\gamma^{k_1} \\ & = & g_1 g_2. \end{array}$$

(9) Le centre C d'un groupe G d'ordre p^2 est d'ordre p ou p^2. S'il est d'ordre p^2, $C = G$ et G est commutatif. Supposons G non commutatif, donc différent de son centre C. Son centre n'étant pas réduit au neutre est d'ordre p, et G/C étant de cardinal p ($|G/C| = p^2/p = p$) est cyclique, ce qui implique la commutativité de G (exercice précédent), contrairement à l'hypothèse.

Le groupe G est donc commutatif, égal à $\mathbb{Z}/p^2\mathbb{Z}$ s'il a un élément d'ordre p^2 ou à $\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}$ sinon.

(10) L'ordre de $\mathfrak{S}_4$ est égal à $24 = 3 \times 2^3$. Les sous-groupes d'ordre 3 sont des 3-Sylow, et ceux d'ordre 8 des 2-Sylow.

D'après les théorèmes de Sylow, il y a trois 2-Sylow et un ou quatre 3-Sylow.

Les sous-groupes d'ordre 3 sont engendrés par les quatre 3-cycles $(1-2-3)$, $(1-2-4)$, $(1-3-4)$ et $(2-3-4)$. Ainsi le 3-cycle $(1-2-3)$ engendre le sous-groupe $\{i_d,\, (1-2-3),\, (1-3-2)\}$.

L'ordre maximum des éléments est 4, et il y a six 4-cycles. Considérons le sous-groupe H_σ, d'ordre 4, engendré par $\sigma = (1-2-3-4)$. On a :

$$\begin{cases} \sigma^2 = \tau_1 \circ \tau_2 = \tau_2 \circ \tau_1, \\ \sigma^3 = (1-4-3-2), \\ \sigma^4 = i_d. \end{cases}$$

Essayons de le compléter en un sous-groupe d'ordre 8 par des transpositions.

Ajoutons d'abord $\tau_1 = (1-3)$ et $\tau_2 = (2-4)$, puis $\nu_1 = (1-2)\,(3-4)$ et $\nu_2 = (1-4)\,(2-3)$.

Nous obtenons la table :

$\circ$	σ	σ^2	σ^3	τ_1	τ_2	ν_1	ν_2
σ	σ^2	σ^3	i_d	ν_2	ν_1	τ_1	τ_2
σ^2	σ^3	i_d	σ	τ_2	τ_1	ν_2	ν_1
σ^3	i_d	σ	σ^2	ν_1	ν_2	τ_2	τ_1
τ_1	ν_1	τ_2	ν_2	i_d	σ^2	σ	σ^3
τ_2	ν_2	τ_1	ν_1	σ	i_d	σ^3	σ
ν_1	τ_2	ν_2	τ_1	σ^3	σ	i_d	σ^2
ν_2	τ_1	ν_1	τ_2	σ	σ^3	σ^2	i_d

On obtient les deux autres 2-Sylow en procédant de même, d'une part avec :

$$\sigma' = (1-3-2-4),\ \sigma'^2 = (1-2)\,(3-4),\ \sigma'^3 = (1-4-2-3)$$

et d'autre part :

$$\sigma\text{"} = (1-3-4-2),\ \sigma\text{"}^2 = (1-4)\,(3-2),\ \sigma\text{"}^3 = (1-2-4-3).$$

On a ainsi utilisé tous les 4-cycles.

4 Suite exacte, complexe, homologie

Soit $(E, d) = (E_i, d_i)$ une suite, finie ou non, de groupes commutatifs E_i (ou d'espaces vectoriels sur un même corps ou encore de modules sur un même anneau), et de morphismes de groupes d_i (ou d'applications linéaires dans le cas des espaces vectoriels ou des modules) :

$$d_i \ : \ E_i \ \rightarrow \ E_{i+1}$$

ou :

$$d_i \ : \ E_i \ \rightarrow \ E_{i-1}.$$

Remarquons que l'on passe du premier cas au second en changeant i en $-i$. On conserve cependant les deux notations à cause d'une dualité.

Si d respecte la condition $\mathrm{Im}(d) = \mathrm{Ker}(d)$ ($\mathrm{Im}(d_i) = \mathrm{Ker}(d_{i+1})$ dans le premier cas ou $\mathrm{Im}(d_i) = \mathrm{Ker}(d_{i-1})$ dans le second), la suite est appelée **suite exacte**. Elle est dite *courte* si elle est de la forme :

$$\{0\} \rightarrow E_1 \xrightarrow{i} E_2 \xrightarrow{s} E_3 \rightarrow \{0\}$$

i étant un morphisme injectif, car de noyau $\{0\}$, et s étant la surjection canonique sur les classes modulo E_1 ($\mathrm{Ker}(s) = \mathrm{Im}(i)$). Remarquons que, dans le cas d'espaces vectoriels, E_3 est isomorphe à un complémentaire de $i(E_1)$ dans E_2, d'où, si les dimensions sont finies :

$$\dim(E_2) = \dim(E_1) + \dim(E_3)\,.$$

Si $E_3 = \{0\}$ (ou $E_1 = \{0\}$), la suite exacte est encore plus courte, mais ne présente guère d'intérêt ; elle exprime que i (ou s) est un isomorphisme.

4.1 Complexe, homologie, cohomologie

Si la suite (E, d) vérifie seulement $d \circ d = 0$ ($\mathrm{Im}(d_i) \subset \mathrm{Ker}(d_{i+1})$ dans le premier cas ou $\mathrm{Im}(d_i) \subset \mathrm{Ker}(d_{i-1})$ dans le second), c'est un **complexe de groupes** et la suite des quotients, dans le premier cas, $\mathrm{H}^i = \mathrm{Ker}(d_{i+1})/\mathrm{Im}(d_i)$, donc le *défaut d'exactitude* de la suite, est la suite de **cohomologie** du complexe : $H^*(E) = (\mathrm{H}^i(E))$. Dans le second cas, $\mathrm{H}_i = \mathrm{Ker}(d_i)/\mathrm{Im}(d_{i+1})$ est la suite d'**homologie** du complexe : $H_*(E) = (\mathrm{H}_i(E))$.

Un exemple de cohomologie, la *cohomologie de De Rham*, est donné dans *Géométrie différentielle*, même page web. Nous allons voir un exemple d'homologie.

4.2 Simplexe ordonné, ensemble simplicial

Un n-**simplexe ordonné** S est l'enveloppe convexe dans $\mathbb{R}^n$ de $n+1$ points $(A_0, \ldots, A_n)$, ses **sommets**, formant une base affine et définissant une orientation de l'espace. On le note $[A_0, \ldots, A_n]$. On pourra écrire A pour $[A]$.

Précisons :
- les n vecteurs A_0A_i forment une base de $\mathbb{R}^n$,
- $S = \{\lambda_0 A_0 + \cdots + \lambda_n A_n \,|\, \lambda_i \geq 0, \sum \lambda_i = 1.$

Si on enlève le sommet A_i, à l'ensemble des $n+1$ sommets du n-simplexe S, on obtient le $n-1$-simplexe orienté :

$$d_i S = [A_0, \ldots, A_{i-1}, A_{i+1}, \ldots, A_n] = [A_0, \ldots, \widehat{A}_i, \ldots, A_n],$$

qui est une **face**, ou $n-1$-face, du n-simplexe.

L'ensemble des faces d'un simplexe est son **bord**.

Un simplexe privé d'une ou plusieurs faces par une relation d'équivalence ($\sim$) est un **simplexe dégénéré**, noté $[\ ]^{\sim}$, en mettant entre crochets ses sommets restants ainsi que les perdus. C'est lors du calcul de son bord que la perte apparaîtra.

L'ensemble des $d_i S$, $0 \leq i \leq n$, est le n-**simplexe creux** (ordonné), noté S°. C'est le bord du n-simplexe.

Les A_i d'un n-simplexe, des 0-simplexes, sont ses *sommets*, les $[A_i, A_j]$, $i \neq j$, des 1-simplexes, sont ses *arêtes*. Les $[A_{i_1}, \ldots, A_{i_k}]$ sont ses $(k-1)$-faces.

Un **ensemble simplicial** est un ensemble E de simplexes, y compris les dégénérés, tel que :
- $S \in E \Rightarrow \forall i : d_i S \in E$,
- $S, S' \in E,\ S \cap S' \neq \emptyset \Rightarrow S \cap S'$ est une face commune à S et S'.

Il est naturellement muni de la topologie de $\mathbb{R}^n$.

On note E_i l'ensemble des i-simplexes, dégénérés ou non, de E. Ses éléments sont aussi des i-chaînes.

Partons par exemple du tétraèdre (plein) $[A, B, C, D]$:
- $E_3 = \{[A, B, C, D]\}$,
- $E_2 = \{[B, C, D], [A, C, D], [A, B, D], [A, B, C]\}$, ses faces,
- $E_1 = \{[A, B], [A, C], [A, D], [B, C], [B, D], [C, D]\}$, ses arêtes,
- $E_0 = \{A, B, C, D\}$, ses sommets.

Le tétraèdre creux a l'ensemble simplicial précédent avec $E_3 = \emptyset$.

Si une figure de $\mathbb{R}^n$ a plus de $n+1$ points, notons-la sans les crochets et les virgules. Ainsi, $ABCD$ désigne le carré plein, dans $\mathbb{R}^2$, $ABCD^{\circ}$ s'il est creux, ce qui évite la confusion avec le tétraèdre $[A, B, C, D]$, dans $\mathbb{R}^3$.

On peut coller deux simplexes disjoints de même dimension par une relation d'équivalence ($\sim$), en conservant l'orientation ou en l'inversant. La topologie est alors la topologie quotient par $\sim$. Ainsi, en identifiant les arêtes opposées $[A, B]$ et $[D, C]$ ($[A, B] \sim [D, C]$) du carré $ABCD$ on obtient un tube fini, de façon plus simple que celle que nous exposerons un peu plus loin. On a alors :

$$\begin{cases} E_0 = \{A, B\}, \\ E_1 = \{[A, B] = [D, C]^{\sim}, [B, C]^{\sim}, [A, C]^{\sim}, [A, D]^{\sim}\}, \\ E_2 = \{[A, B, C]^{\sim}, [A, C, D]^{\sim}\}. \end{cases}$$

Si l'on inverse l'orientation ($[A,B] \sim [C,D]$), on obtient, donc très simplement, le *ruban de Moebius*, pour lequel :

$$\begin{cases} E_0 = \{A, B\}, \\ E_1 = \{[A,B] = [C,D]^{\sim}, [B,C]^{\sim}, [A,C]^{\sim}, [A,D]^{\sim}\}, \\ E_2 = \{[A,B,C]^{\sim}, [A,C,D]^{\sim}\}. \end{cases}$$

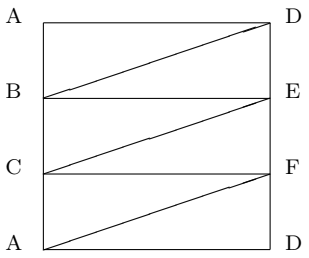
4.3 Triangulation

Un polyèdre définit un ensemble simplicial. Si une variété est homéomorphe (un homéomorphisme est une bijection bicontinue, que nous noterons $\simeq$) à un polyèdre, l'ensemble simplicial de ce polyèdre est une **triangulation** de cette variété, qui est alors *triangulable*.

La triangulation d'une variété est constituée d'un nombre minimum de points de cette variété, mais on obtient une triangulation *équivalente* en ajoutant d'autres points de la variété, puisque le polyèdre obtenu est encore homéomorphe à la variété. Ainsi, un disque de $\mathbb{R}^2$ est-il triangulé par un triangle (plein), mais également par un carré, un pentagone...

Le cylindre plein et la 3-boule sont homéomorphes au tétraèdre (plein).

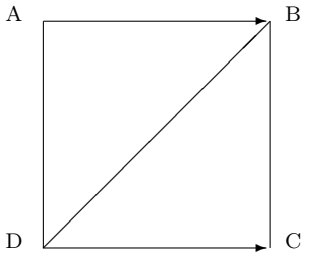
Triangulons le tube (ou cylindre creux fini). Première méthode :



Son bord est constitué de deux cercles triangulés respectivement par ABC° et DEF°.

Sa surface (ci-contre) est constituée d'un rectangle dont les bords inférieurs et supérieurs sont collés. On obtient les six triangles : $[A,B,D]$, $[D,B,E]$, $[E,B,C]$, $[C,F,E]$, $[F,C,A]$ et $[F,A,D]$.

Deuxième méthode :

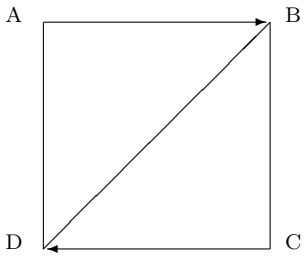


On identifie $[A,B]$ et $[D,C]$ (selon les flèches). On a :

$$\begin{cases} E_0 = \{A, B\}, \\ E_1 = \{[A,B], [A,D]^{\sim}, [B,C]^{\sim}, [B,D]^{\sim}\}, \\ E_2 = \{[A,D,B], [B,D,C]^{\sim}\}; \end{cases}$$

$[A,D]^{\sim}$ et $[B,C]^{\sim}$ (cercles) forment le bord.

Triangulons le ruban de Mœbius, variété non orientable (voir *Géométrie différentielle*, même page web) en identifiant $[A, B]$ et $[D, C]$, toujours selon les flèches :

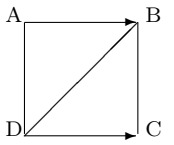


Son bord circulaire est constitué des deux segments latéraux $[A, D]$ et $[B, C]$ collés en $B \sim D$ et en $C \sim A$.

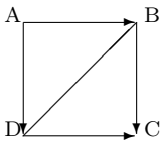
Sa surface (ci-contre) est constituée d'un rectangle dont les bords inférieurs et supérieurs sont collés après retournement.

Son ensemble simplicial est égal au précédent.

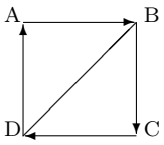
Les triangulations du tube, du tore creux et des variétés non orientables, comme le plan projectif P^2 et de la bouteille de Klein BK, (voir *Géométrie différentielle*, même page web) sont également obtenues à partir du carré $ABCD$:



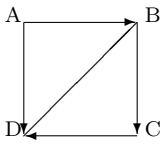
tube,



tore,



P^2



BK.

4.4 Complexe simplicial, homologie simpliciale

Soit G_i le groupe libre engendré par E_i, c'est- à-dire l'ensemble des combinaisons linéaires à coefficients dans $\mathbb{Z}$ d'éléments de E_i :

$$G_i = \{\sum n_k s_k \,|\, n_k \in \mathbb{Z}, s_k \in E_i\} = \mathbb{Z}^{|E_i|},$$

$|E_i|$ désignant le cardinal de E_i. Posons $G_{-1} = 0$, 0 mis pour $\{0\}$.

L'**opérateur de bord** ∂, $\partial_{G_i} = \partial_i$, est le morphisme de groupes :

$$\begin{array}{rccl} \partial_i : & G_i & \to & G_{i-1} \\ & \mathbb{Z}\, S & \mapsto & \mathbb{Z}\,(\sum_{0\le j\le i}(-1)^j d_j S). \end{array}$$

Ainsi, pour $[A, B, C]$ on obtient :

$$\partial(\mathbb{Z}\,[A, B, C]) = \mathbb{Z}\,([B, C]-[A, C]+[A, B]) = \{n([B, C]-[A, C]+[A, B]) \,|\, n \in \mathbb{Z}\},$$

et, si $A \sim B$, $\partial(\mathbb{Z}\,[A, B]^{\sim}) = 0$ ($[A, B]^{\sim}$ est un cercle).

Il nous arrivera de noter, pour alléger l'écriture, par exemple :

$$\partial[A, B, C] = [B, C] - [A, C] + [A, B]$$

au lieu de :

$$\partial\,\mathbb{Z}[A, B, C] = \mathbb{Z}([B, C] - [A, C] + [A, B]).$$

Proposition 4.1. $\partial_{n-1} \circ \partial_n = 0,\ n \geq 1.$

Démonstration. Soit $S = [A_0, \ldots, A_n]$. calculons le coefficient de $d_i d_j S$ dans $\partial_{n-1} \circ \partial_n S$ $(0 \leq i < j \leq n)$. On applique ∂_n. Les termes intéressants sont $(-1)^i d_i(S)$ et $(-1)^j d_j(S)$. Puis on applique ∂_{n-1}. Le premier terme donne le coefficient $(-1)^i(-1)^{j-1}$, et le second $(-1)^i(-1)^j$. La somme des deux est nulle. □

On a donc le **complexe simplicial** de S :

$$0 \to G_n \xrightarrow{\partial_n} G_{n-1} \xrightarrow{\partial_{n-1}} G_{n-2} \xrightarrow{\partial_{n-2}} \ldots \xrightarrow{\partial_1} G_0 \to 0,$$

dont l'homologie, notée $H_*(S)$, est dite **simpliciale**.

Si on fait agir la permutation $\sigma \in \Sigma_{n+1}$ sur les $n+1$ sommets d'un n-simplexe s, on obtient le n-simplexe $\epsilon_\sigma\, s$, ϵ_σ étant la signature de σ (voir *Systèmes et Matrices*, même page web). On obtient le même simplexe si $\epsilon_\sigma = 1$ ou son opposé si $\epsilon_\sigma = -1$.

On a $\partial \circ \sigma = \epsilon_\sigma\, \partial$:

$$\partial[\ldots, A_{\sigma(i)}, \ldots] = \epsilon_\sigma\, \partial[\ldots, A_i, \ldots].$$

Les éléments de $\operatorname{Ker} \partial$ sont des **cycles**, ceux de $\operatorname{Im} \partial$ sont des **bords**.

Lemme 4.1 Si $u : E \to F$, $E \cong \mathbb{Z}^p$, $F \cong \mathbb{Z}^r$, est un morphisme de groupes dont l'image est isomorphe à $\mathbb{Z}^q$ $(q \leq r)$ son noyau est isomorphe à $\mathbb{Z}^{p-q}$.

Démonstration. Soient $(e_1, \ldots, e_p)$ une base de E et $(f_1, \ldots, f_q)$ une base de $\operatorname{Im} u$. Les équations de u sont :

$$L_i\ :\ u(e_i) = a_{i1} f_1 + \cdots + a_{iq} f_q,\ 1 \leq i \leq p.$$

Nous pouvons supposer $a_{11} \neq 0$, quitte à permuter les (f_j), u étant surjectif. Remplaçons ces équations par :

$$L'_i = a_{11} L_i - a_{1i} L_1,\ 2 \leq i \leq p.$$

Nous obtenons ainsi $p-1$ équations portant sur $q-1$ f_j, conservant la surjectivité. En répétant cette transformation q fois, nous obtenons $p-q$ équations homogènes :

$$u(\sum \alpha_{ij} e_i) = 0,\ 1 \leq j \leq p-q$$

caractérisant les éléments du noyau de u, de sorte que les $\sum \alpha_{ij} e_i$ en sont une famille génératrice. Si ces équations étaient liées, on pourrait en supprimer, et $\operatorname{Ker} u$ serait de dimension inférieure à $p-q$, $E/\operatorname{Ker} u$ serait de dimension supérieure à q, or $E/\operatorname{Ker} u$ est isomorphe à $\operatorname{Im} u$ (exercice 2, Groupes), donc de dimension q. La famille est donc libre, et $\operatorname{Ker} u \cong \mathbb{Z}^{p-q}$. □

Lemme 4.2. Pour le calcul de l'homologie simpliciale, $[B,A]+[A,B]]$ équivaut à 0, comme $[A,B_1]+[B_1,B_2]+\cdots+[B_n,A]$.

Démonstration. Si $\mathbb{Z}([B,A]+[A,B])$ est dans $\operatorname{Im}\partial_{i+1}$, $\mathbb{Z}\,[B,A]+[A,B]]\cong\mathbb{Z}$. Mais l'image par ∂_i de ce sous-groupe est nulle, il appartient à $\operatorname{Ker}\partial_i$, sa contribution est donc isomorphe à $\mathbb{Z}$, et elle donne 0 dans H_i. On peut donc considérer que $[B,A]+[A,B]]=0$. De même pour $[A,B_1]+[B_1,B_2]+\cdots+[B_n,A]$. □

L'homologie simpliciale est invariante par homéomorphisme, d'après la définition de la triangulation. Ceci permet de définir l'homologie simpliciale d'un espace triangulable.

4.4.1 Homologie du cercle S^1

Le cercle est homéomorphe au triangle creux. Calculons donc l'homologie de ABC°.

On obtient trois sommets : A, B et C, et trois arêtes : $[A,B]$, $[B,C]$ et $[C,A]$, de bords respectifs $B-A$, $C-B$ et $A-C=-(B-A)-(C-B)$, d'où :

$$\begin{cases}\operatorname{Ker}\delta_0=\mathbb{Z}\,(A)\oplus\mathbb{Z}\,(B)\oplus\mathbb{Z}\,(C)\cong\mathbb{Z}^3,\\ \operatorname{Im}\delta_1=\mathbb{Z}\,[B-A]+\mathbb{Z}\,[C-B]\cong\mathbb{Z}^2,\\ \operatorname{Im}\delta_2=0.\end{cases}$$

On a donc :

$$H_0=\operatorname{Ker}\delta_0/\operatorname{Im}\delta_1\cong\mathbb{Z}.$$

La somme des dimensions de $\operatorname{Ker}\delta_1$ et de $\operatorname{Im}\delta_1$ valant 3, on a $\operatorname{Ker}\delta_1\cong\mathbb{Z}$, d'où :

$$H_1=\operatorname{Ker}\delta_1/\operatorname{Im}\delta_2\cong\mathbb{Z}.$$

Les autres groupes sont nuls.

On obtent plus simplement S^1 à partir du segment $[A,B]$ en identifiant A et B. On a alors $E_1=[A,B]^\sim$, $E_0=A$, $G_1\cong\mathbb{Z}$, $G_0\cong\mathbb{Z}$, $\operatorname{Im}\partial_1=0$, $\operatorname{Ker}\partial_1\cong\mathbb{Z}$, et on obtient évidemment la même homologie.

4.4.2 Homologie du tube

Reprenons la figure précedente : le tube est obtenu en identifiant $[A,B]$ et $[D,C]$. On a :

$$\begin{cases}E_2=\{[A,D,B]^\sim,[B,D,C]^\sim\}\\ E_1=\{[A,B],[B,C]^\sim,[B,D]^\sim,[A,D]^\sim\},\\ E_0=\{A,B\},\end{cases}\qquad\begin{cases}G_2\cong\mathbb{Z}^2,\\ G_1\cong\mathbb{Z}^4,\\ G_0\cong\mathbb{Z}^2,\end{cases}$$

d'où $\operatorname{Im}\partial_2\cong\mathbb{Z}^2$, $\operatorname{Ker}\partial_2=0$ et $H_2=0$; puis $\operatorname{Im}\partial_1\cong\mathbb{Z}$ $(D-A=B-C=0)$, d'où $\operatorname{Ker}\partial_1\cong\mathbb{Z}^3$ et $H_1\cong\mathbb{Z}$, enfin $\partial_0=0$, $\operatorname{Ker}\partial_0\cong\mathbb{Z}^2$ et $H_0\cong\mathbb{Z}$.

4.4.3 Homologie du n-simplexe S_n

L'ensemble E_n ne contient que $[A_0, \ldots, A_n]$; comme $\partial E_n \neq 0$, $\operatorname{Ker} \partial_n = 0$ et $H_n(S_n) = 0$.

Comme $\partial_0 = 0$ et $G_0 \cong \mathbb{Z}^{n+1}$, on a $\operatorname{Ker} \partial_0 \cong \mathbb{Z}^{n+1}$. Evaluons $\operatorname{Im} \partial_1$. Combien G_1 a-t-il de générateurs ? Les vecteurs A_0A_i sont linéairement indépendants par hypothèse ; comme $A_j - A_i = (A_0 - A_i) - (A_0 - A_j)$, les n $\partial\,[A_0, A_i]$, qui sont indépendants, engendrent $\operatorname{Im} \partial_1$ qui est donc isomorphe à $\mathbb{Z}^n$, et $H_0(S_n) \cong \mathbb{Z}$.

Calculons les $H_k(S_n)$, pour $1 \leq k \leq n-1$. L'ensemble E_k est la réunion de k-faces qui sont des k-simplexes et $\operatorname{Ker} \partial_k$ est la somme des noyaux de ∂_k restreint à chacune des faces, or ces noyaux sont nuls (comme dans le cas n), et donc $H_k(S_n) = 0$. Le seul groupe d'homologie non nul est donc H_0.

4.4.4 Homologie du n-simplexe creux, ou de l'hyper-sphère S^{n-1}

Son ensemble simplicial est celui du n-simplexe privé de E_n. Dans le cas du n-simplexe, $\operatorname{Ker} \partial_{n-1}$ est égal à $\operatorname{Im} \partial_n$, tous deux isomorphes à $\mathbb{Z}$. Maintenant $\operatorname{Im} \partial_n = 0$, et H_{n-1}, égal à $\operatorname{Ker} \partial_{n-1}$, est isomorphe à $\mathbb{Z}$. Les autres groupes d'homologie sont ceux du n-simplexe :

$$H_{n-1}(S^{n-1}) \cong \mathbb{Z},\ H_k(S^{n-1}) = 0,\ 1 \leq k \leq n-2,\ H_0(S^{n-1}) \cong \mathbb{Z}.$$

4.4.5 Homotopie, espace contractile

On dit que deux sous-espaces X et Y d'un espace topologique E sont **homotopes** s'il existe une application continue :

$$\phi : [0,1] \times E \to E,\ \phi(t,x) = \phi_t(x),$$

telle que, $\forall t \in [0,1]$, $\phi_t : E \to E$ est un homéomorphisme, et si $x \in X$ et $y \in Y$, on a $\phi(0,x) = x$ et $\phi(1,y) = y$.

Deux chemins fermés dans E sont **homotopes** s'il existe un homéomorphisme de E transformant le premier en le second.

Ainsi, dans $\mathbb{C}^*$, tous les chemins entourant une fois l'origine sont homotopes deux à deux, mais non contractiles. Les chemins n'entourant pas l'origine sont contractiles.

Soit $\phi : [0,1] \times E \to E$ une application continue.

L'espace E est **contractile** s'il existe $x_0 \in E$ tel que, $\forall x \in E$, $\phi(0,x) = x$, $\phi(1,x) = x_0$, $\phi(t,x_0) = x_0$ ($t \in [0,]$). Tout espace convexe est contractile. Tout espace connexe par arcs est contractile, et réciproquement.

Une partie F de E est contractile si $\forall x \in F$, $\phi(0,x) = x$, $\phi(1,x) = x_0$, $\phi(t,x_0) = x_0$, pour un certain $x_0 \in E$.

Le n-simplexe est contractile, le n-simplexe creux ne l'est pas.

Nous verrons que l'homologie d'un espace contractile est égale à celle d'un point, et que E et $[0,1] \times E$ ont la même homologie.

4.4.6 Interprétation de l'homologie

Avec les notations précédentes, si un élément non nul $a \in G_p(X)$, $p \geq 1$, $a \notin \partial G_{p+1}(X)$, est tel que $\partial a = 0$, il représente le bord d'un élément manquant à $G_{p+1}(X)$, c'est- à-dire un trou dans X de dimension $p+1$, puisque la dimension locale de son bord est p. C'est un $p+1$-trou, pouvant contenir un $p+1$-cube.

Si $H_0 \cong \mathbb{Z}$ et si $E_0 = \{A_1, \ldots, A_n\}$, les $A_{i+1} - A_i$ sont liés par une seule relation, et les $[A_i, A_{i+1}]$ sont les bords d'une figure connexe par arcs, et si $H_0 \cong \mathbb{Z}^p$, il y a p relations indépendantes, chacune caractérisant une figure connexe par arcs, et X est formé de p composantes connexes par arcs. Un 0-trou est donc un point, ou une composante connexe par arcs. Si $H_0(X) = 0$, X est l'ensemble vide. Il est trivial que $H_0(\emptyset) = 0$.

Pour le tore simple T, $H_0(T) \cong \mathbb{Z}$ signifie qu'il est connexe ; $H_1(T) \cong \mathbb{Z}^2$ signifie que l'on peut tracer sur sa surface deux cercles, et deux seulement, non contractiles et non homotopes entre eux, le tore étant homéomorphe à leur produit ; $H_2(T) \cong \mathbb{Z}$ signifie qu'il a un volume intérieur, et un seul.

Si $H_p(X) \cong \mathbb{Z}/2\mathbb{Z}$ ($p \geq 1$), il y a dans $G_{p+1}(X)$ un élément a qui n'est pas un bord mais tel que $2a$ en est un (voir l'homologie de P^2 et l'exercice 3 (b)).

4.4.7 Homologie des espaces projectifs réels P^n, $n \in \mathbb{N}$

L'espace projectif P^n est l'ensemble des droites de $\mathbb{R}^{n+1}$ (un point de $\mathbb{R}^{n+1}$ est repéré par ses coordonnées $(x_0, \ldots, x_n)$) privées de l'origine. Il est homéomorphe à l'hyper-sphère S^n ($\sum_{0 \leq i \leq n} x_i^2 = 1$) de $\mathbb{R}^{n+1}$ quotientée par la fonction antipodale $a(x) = -x$. En effet, chaque droite intersecte l'hyper-sphère en deux points diamétralement opposés. Il est donc homéomorphe à la demi-hyper-sphère supérieure ($x_n \geq 0$) dont le bord (l'équateur $\sum_{0 \leq i \leq n-1} x_i^2 = 1$, $x_n = 0$, homéomorphe à l'hyper-sphère S^{n-1}) est quotienté par a. Quotienté par a, ce bord est homéomorphe à P^{n-1}.

Les H_p pour $p > n$ ou $p < 0$ sont nuls.

Voyons les cas particuliers $n = 0, 1, 2$.

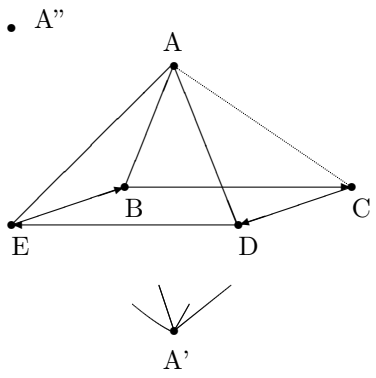
L'espace P^0, quotient par a de $S^0 = \{\pm 1\}$, dans $\mathbb{R}$, est donc réduit à un élément, et son unique groupe d'homologie (non nul) est $H_0 \cong \mathbb{Z}$.

L'espace P^1 est homéomorphe à S^1. En effet le demi-équateur de S^1, d'équation $x^2 + y^2 = 1$, $y \geq 0$, est bordé par les deux points $(\pm 1, 0)$ de S^0, et, en identifiant ces deux points, on obtient un espace homéomorphe à S^1 :

$$H_0(P^1) \cong \mathbb{Z},\ H_1(P^1) \cong \mathbb{Z}.$$

L'homologie de P^2 est calculée autrement dans l'exercice 3 (b).

La figure suivante est une triangulation de P^1 et de P^2 permettant d'en obtenir une de P^3 grâce aux points A' et A''.



Le carré (de centre O, non figuré), $BCDE^\circ$ (creux) est une triangulation de S^1, et, quotienté par a, de P^1.

Les triangles issus de A (pleins) (bordés par le carré creux) donnent une triangularisation de la demi-sphère supérieure S^2_+.

Si on quotiente le carré par antipodie, on obtient une triangularisation de P^2.

Le point A' est l'antipode de A ; A'' est tel que (OB, OC, OA, OA'') soit une base de $\mathbb{R}^4$.

En reliant A' à B, C, D et E, en quotientant par l'antipodie de $\mathbb{R}^3$, et en reliant A'' aux six autres points, on obtient une triangulation de P^3.

L'ensemble simplicial de P^2 est :

$$\begin{cases} E_2 = \{[A,B,C],[A,C,D],[A,D,E]^\sim,[A,E,B]^\sim\}\},\\ E_1 = \{[A,B],[A,C],[A,D]^\sim,[A,E]^\sim,[B,C],[C,D]^\sim\},\\ E_0 = \{A,B,C\}, \end{cases}$$

donne les groupes $G_2 = \mathbb{Z}^4$, $G_1 = \mathbb{Z}^6$ et $G_0 = \mathbb{Z}^3$.

Notons que faire, par exemple, $[E,B] = [C,D]$ n'identifie pas les triangles $[A,E,B]$ et $[A,C,D]$, chacun conservant une surface intérieure propre. On a :

$$\begin{array}{rcl} \partial[A,B,C] &=& [B,C]-[A,C]+[A,B],\\ \partial[A,C,D]^\sim &=& [C,D]^\sim-[A,D]^\sim+[A,C],\\ \partial[A,D,E]^\sim &=& [D,E]^\sim-[A,E]^\sim+[A,D]^\sim,\\ \partial[A,E,B]^\sim &=& [E,B]^\sim-[A,B]+[A,E]^\sim, \end{array}$$

Les triangles ont des images par ∂ indépendantes, $\operatorname{Ker}\partial_2 = 0$ et $H_2 = 0$. La somme de ces images est $2([B,C]+[C,D]^\sim)$, et c'est la seule relation les liant. On peut donc remplacer l'une des images par $2([B,C]+[C,D]^\sim)$, et conserver les trois autres, de sorte que $\operatorname{Im}\partial_2 = \mathbb{Z}^3 + 2\mathbb{Z}$.

Calculons ∂G_1. Comme $D-A = B-A$, $E-A = C-A$, $D-C = B-C$, puis $(B-A)-(C-A)+(C-B) = 0$ (unique relation), on a $\operatorname{Im}\partial_1 = \mathbb{Z}^2$ et $\operatorname{Ker}\partial_1 \cong \mathbb{Z}^4$. Enfin, $\operatorname{Ker}\partial_0 = \mathbb{Z}^3$. Finalement :

$$H_0(P^2) \cong \mathbb{Z},\ H_1(P^2) \cong \mathbb{Z}/2\mathbb{Z},\ H_2(P^2) = 0.$$

Pour trianguler P^n, $n > 2$, on utilisera la triangulation de S^n, on calculera $H_n(P^n)$ et $H_{n-1}(P^n)$, et on montrera que $H_i(P^n) \cong H_i(P^{n-1})$ pour $i \leq n-2$, ce qui ramenera, en descendant, à l'homologie de P^2.

Pour trianguler S^n, de centre O et d'équateur S^{n-1}, il faut ajouter à une triangulation de son équateur son pôle Nord, le sommet principal A_0. Supposons que $OA_1, \ldots, OA_n$ forment une base de $\mathbb{R}^n$. Pour pouvoir appliquer l'antipodie, il faut que chaque A_i ait un opposé A_{n+i} ($OA_{n+i} = -OA_i$). Les $A_1, \ldots, A_{2n}$ triangulent S^{n-1} et permettent d'appliquer l'antipodie. Il faut donc en tout pour trianguler P^n $2n+1$ points : $A_0, A_1, \ldots, A_{2n}$.

On passe d'une triangulation de P^{n-1} à une de P^n en ajoutant l'antipode de A_0 et le pôle Nord de S^n. On double ainsi (avant d'appliquer l'antipodie) le nombre des i-faces issues de A_0 (en ajoutant celles obtenues en remplaçant A_0 par son antipode), et on obtient des (i+1)-faces de la triangulation de P^n en ajoutant le nouveau pôle Nord à chaque i-face.

Il peut être pratique de changer ensuite les numéros des points :
- A_i devient A_{i+1} pour $0 \leq i \leq n$,
- A_{n+2} est l'antipode de A_1,
- A_i devient A_{i+2} pour $n+1 \leq i \leq 2n$,
- A_0 est le nouveau pôle Nord.

Construisons les n-faces, toutes issues de A_0, à partir des points A_0,..., A_{2n}. La première est $[A_0, A_1, \ldots, A_n]$, la deuxième est $[A_0, A_2, \ldots, A_{n+1}]$, la i-ème ($i \leq 2n$) est $[A_0, A_i, \ldots, A_{n+i}]$, les indices étant pris modulo $2n$ lorsqu'ils dépassent $2n$.

Les (n-1)-faces sont de la forme $[A_0, A_i, \ldots, A_{n-i-1}$, et appartiennent aux bords de deux n-faces consécutives, la (i-1)-ième et la i-ème, affectées de signes différents étant respectivement en troisième et en deuxième position, et à aucun autre bord. On en déduit que la somme Σ des bords des n-faces se réduit à la somme des (n-1)-faces ne contenant pas A_0. Ces dernières se correspondent deux à deux par antipodie, de sorte que leur somme est nulle si n est impair, ces bords étant dans $\mathbb{R}^n$, et égale au double de la somme des n premières si n est pair. En effet, le jacobien de a étant égal à $(-1)^{n+1}$ (voir *Géométrie différentielle*, même page web), a conserve l'orientation si et seulement si n est impair : P^n.

On en déduit que $\operatorname{Ker} \partial_n = 0$ et $H_n(P^n) = 0$ si n est pair, et que $\operatorname{Ker} \partial_n \cong \mathbb{Z}$ et $H_n(P^n) \cong \mathbb{Z}$ si n est impair.

Les espaces projectifs sont connexes par arcs, $H_0(P^n) \cong \mathbb{Z}$, $\forall n$; P^n est orientable si et seulement si n est impair.

Si P^{n-1}, $n \geq 2$, a un hypervolume intérieur, $H_{n-1}(P^{n-1}) \cong \mathbb{Z}$, cet hypervolume, dans $\mathbb{R}^n$, n'a plus d'intérieur dans $\mathbb{R}^{n+1}$ (comme le cercle quand on passe de $\mathbb{R}^2$ à $\mathbb{R}^3$), de sorte que P^n n'est pas fermé par P^{n-1} et n'a pas d'hypervolume intérieur : $H_n(P^n) = 0$. C'est le cas pour $n = 2$.

Si P^{n-1} n'a pas d'hypervolume intérieur, donc $H_{n-1}(P^{n-1}) = 0$, il referme P^n, qui en a alors un, et $H_n(P^n) \cong \mathbb{Z}$. C'est le cas pour $n = 1$ ou 3.

On retrouve ainsi, par récurrence, à partir de $H_1(P^1) \cong \mathbb{Z}$, que $H_n(P^n) \cong \mathbb{Z}$ si n est impair, et $H_n(P^n) = 0$ si n est pair.

Nous noterons A_0 le sommet principal représentant le pôle Nord de S^n, et E_n les n-faces, toutes issues de A_0. Dans E_i, $i \leq n$, nous aurons les i-faces contenant P_0 et les autres. L'ensemble de ces dernières est E'_i, qui engendre le groupe libre G'_i, et $\partial : G'_i \to G'_{i-1}$, d'où une homologie H'.

Pour faire de même avec les i-faces contenant A_0, il faut ajouter à leur ensemble E''_i l'image $\partial\, E''_{i+1}$.

L'ensemble E''_i engendre le groupe libre G''_i, et $\partial : G''_i \to G''_{i-1}$, d'où une homologie H''. Le sous-groupe engendré par $\partial\, E''_{i+1}$ est annulé par ∂.

Notons $\partial'_i = \partial_{|G'_i}$ et $\partial''_i = \partial_{|G''_i}$.

Il n'y a dans $\operatorname{Ker}\partial'_i$ que des i-faces ne contenant pas A_0 et dans $\operatorname{Ker}\partial''_i$ que des i-faces le contenant plus $\partial\, E''_{i+1}$ qui est annulé par ∂''_i ; $\operatorname{Ker}\partial_i = \operatorname{Ker}\partial'_i \oplus \operatorname{Ker}\partial''_i$, et $H_i(P^n) = H'_i \oplus H''_i$.

La relation d'antipodie n'agit pas sur les H''_i pour $i \leq n-2$ (elle agit bien sur $\operatorname{Im}\partial''_{i+1}$, mais ce groupe est dans $\operatorname{Ker}\partial''_i$). Si par exemple $a(A_j) = A_i$, la surface $[A_0, A_i, A_j]^\sim$ est conservée, de même que les arêtes issues de A_0. Elle agit sur H''_n puisque $\operatorname{Im}\partial''_n = 0$.

Ensuite, $\partial[A_0, A_i] = A_i - A_0 = A_j - A_0 = \partial[A_0, A_j]$, de sorte que $\operatorname{Im}\partial''_1 \cong G_0$, comme $\operatorname{Ker}\partial''_0$, et on a $H''_0 = 0$, $\forall n \in \mathbb{N}$.

Appliquons ce qui précède à S^n. Les $H'_i(S^n)$ et les $H''_i(S^n)$ sont nuls pour $1 \leq i \leq n-2$, étant facteur direct de $H_i(S^n)$, qui est nul. Or S^n et P^n ont le même H''_i, puisque la relation d'antipodie n'agit pas sur ces H''_i. Les $H''_i(P^n)$ sont donc nuls, $0 \leq i \leq n-2$. Si n est pair, un facteur $\mathbb{Z}$ de $\operatorname{Im}\partial''_n$ pour S^n est remplacé par $2\mathbb{Z}$, de sorte que l'on passe de $H''_{n-1}(S^n) = 0$ à $H''_{n-1}(P^n) \cong \mathbb{Z}/2\mathbb{Z}$. Si n est impair, $H''_{n-1}(P^n) = H''_{n-1}(S^n) = 0$.

Pour $i \in [2, n-2]$, $H''_i = 0$, $H'_i = H_i(P^{n-1})$, on a $H_i(P^n) = H_i(P^{n-1})$.

On a finalement, à partir de l'homologie de P^2 :

$$n \text{ pair } \Rightarrow \begin{cases} H_n(P^n) = 0) \\ H_{n-1}(P^n) \cong \mathbb{Z}/2\mathbb{Z}, \end{cases} \qquad n \text{ impair } \Rightarrow \begin{cases} H_n(P^n) = \mathbb{Z} \\ H_{n-1}(P^n) = 0, \end{cases}$$

$$k \geq 1 \Rightarrow H_{2k}(P^n) = 0,\ H_{2k-1}(P^n) \cong \mathbb{Z}/2\mathbb{Z}.$$

4.4.8 Homologie des espaces projectifs complexes $P^n_{\mathbb{C}}$, $n \in \mathbb{N}$

L'espace projectif $P^n_{\mathbb{C}}$ est l'ensemble des droites de $\mathbb{C}^{n+1}$ privées de l'origine, **droites pointées**. Notons D^* une droite pointée. Un point P de $\mathbb{C}^{n+1} \setminus \{0\}$ est repéré par ses coordonnées $(z_0, \ldots, z_n)$ (non toutes nulles) avec $z_k = x_k + iy_k$, une droite vectorielle est engendrée, sur $\mathbb{C}$, par un tel point, qui la représente ; elle est isomorphe à un plan réel.

Remarquons d'abord que, par connexité par arcs, $H_0(P^n_{\mathbb{C}}) \cong \mathbb{Z}$.

Si le point P appartient à une droite pointée D^* de $\mathbb{C}^{n+1}$, le point λP, $\forall \lambda \in \mathbb{C}^*$ appartient aussi à D^*. Si $z_n \neq 0$, le point $P_0 = (z_i/z_n)$ appartient donc à D^*, et de telles droites sont représentées par les points de $\mathbb{C}^n \times \{1\}$; leur ensemble est isomorphe à $\mathbb{C}^n$. Si $z_n = 0$, P appartient au sous-espace $\mathbb{C}^n$ de $\mathbb{C}^{n+1}$, et on peut recommencer avec z_{n-1}, ainsi de suite.

Considérons la relation d'équivalence sur $\mathbb{C}^{n+1}$:

$$(z_i)_{0\leq i\leq n} \sim (z'_i)_{0\leq i\leq n} \iff \exists \lambda \in \mathbb{C}^* \ : \ (z_i) = \lambda(z'_i).$$

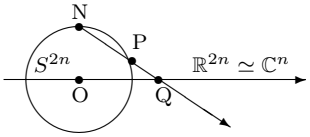
Si $z_n \neq 0$, (z_i) est représenté par $(\ldots, z_i/z_n, \ldots, 1)$, l'ensemble de ces points étant isomorphe à $\mathbb{C}^n$. Si $z_n = 0$, on obtient les **points à l'infini** de $\mathbb{C}^{n+1}$, dont nous noterons l'ensemble ∞_n.

Ces points, de la forme $(z_0, \ldots, z_{n-1}, 0)$, sont équivalents à $(z'_0, \ldots, z'_{n-2}, 1, 0)$ si $z_{n-1} \neq 0$, ou à $(z'_0, \ldots, 0, 0)$, et dans ce cas à $(z''_0, \ldots, z''_{n-3}, 1, 0, 0)$, ainsi de suite.

Ceci montre que $P^n_{\mathbb{C}}$ est homéomorphe à $\mathbb{C}^n \cup \{\infty_n\}$, et finalement :

$$P^n_{\mathbb{C}} \simeq \mathbb{C}^n \cup \mathbb{C}^{n-1} \cup \ldots \cup \mathbb{C} \cup \{\infty\},$$

$\infty = \infty_0$ étant le point à l'infini de $\mathbb{C}$.



La $2n$-sphère :

$$S^{2n} = \{(x_i) \in \mathbb{R}^{2n+1} \mid \sum x_i^2 = 1\}$$

privée de son pôle Nord :

$$N = (0, \ldots, 0, 1)$$

est homéomorphe à $\mathbb{R}^8$, donc à $\mathbb{C}^4$. Considérons en effet l'application :

$$\begin{array}{rccc} \phi \ : & S^{2n} \setminus \{N\} & \to & \mathbb{R}^{2n} \\ & P & \mapsto & Q \end{array}$$

appelée **projection stéréographique** (les points N, P et Q sont alignés). Elle est bijective, continue, et peut être prolongée en un homéomorphisme de S^{2n} dans $P^n_{\mathbb{C}} \cup \{\infty\}$ en posant $\phi(N) = \infty$. Les voisinages de ∞ sont les ensembles de points de module supérieur à une valeur donnée, aussi grande que l'on veut. Ceci assure la continuité de ϕ et de ϕ^{-1}. En effet, l'image par ϕ d'un voisinage de N contient un voisinage de ∞, et réciproquement (si $(z_i) \to \infty$, $\phi^{-1}(z_i) \to N$).

Commençons par l'étude de $P^1_{\mathbb{C}}$, homéomorphe à $\mathbb{C} \cup \{\infty\}$, donc à S^2. Ses groupes d'homologie non nuls sont ceux de S^2 : $H_2(P^1_{\mathbb{C}}) \cong \mathbb{Z}$, $H_0(P^1_{\mathbb{C}}) \cong \mathbb{Z}$.

Comme :

$$\begin{aligned} P^2_{\mathbb{C}} &\simeq \mathbb{C}^2 \cup \mathbb{C} \cup \{\infty\} \\ &\simeq (\mathbb{C}^2 \cup \{\infty\}) \cup (\mathbb{C} \cup \{\infty\}) \\ &\simeq S^4 \cup S^2, \end{aligned}$$

les groupes d'homologie de $P^2_{\mathbb{C}}$ sont ceux de S^4 en degré 4 et 3, et de S^2 pour les premiers.

Précisons : partons du 5-simplexe $[P_0, P_1, \ldots, P_5]$ triangulant l'hypercube de dimension 5, ou la 5-boule, et son ensemble simplicial E. Son homologie en degré $n > 0$ est nulle. Supprimons dans cet ensemble la 5-face $[P_0, \ldots, P_5]$, en conservant son bord, pour faire apparaître le trou de S^4, et la 3-plaque $[P_2, \ldots, P_5]$, en conservant son bord, pour faire apparaître le trou de S^2. Nous diminuons ainsi d'une unité la dimension de $\mathrm{Im}\,\partial_5$ et de $\mathrm{Im}\,\partial_3$, sans changer les dimensions de $\mathrm{Ker}\,\partial_4$ et de $\mathrm{Ker}\,\partial_2$, ce qui donne $\mathrm{Ker}\,\partial_4/\mathrm{Im}\,\partial_5 \cong \mathbb{Z}$ et $\mathrm{Ker}\,\partial_2/\mathrm{Im}\,\partial_3 \cong \mathbb{Z}$, sans autre changement, d'où le résultat annoncé.

Procédons de même pour $P^n_{\mathbb{C}}$:

$$P^n_{\mathbb{C}} \simeq (S^{2n} \cup \{\infty\}) \cup (S^{2n-2} \cup \{\infty\}) \cup \ldots \cup (S^2 \cup \{\infty\})$$

en partant de l'ensemble simplicial du $(2n+1)$-simplexe $[P_0, \ldots, P_{2n+1}]$, auquel nous enlevons successivement les $(2(n-i)+1)$-faces, $0 \leq i \leq n-1$, $[P_{2i}, \ldots, p_{2n+1}]$, ce qui abaisse de 1 la dimension de $\mathrm{Im}\,\partial_{2(n-i)+1}$ sans modifier celle de $\mathrm{Ker}\,\partial_{2(n-i)}$, ce qui fait apparaître les groupes d'homologie en degré pair :

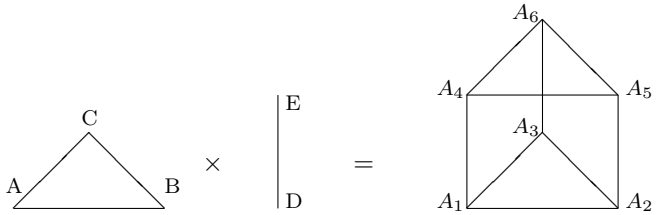
$$H_{2i}(P^n_{\mathbb{C}}) \cong \mathbb{Z} \ \text{ pour } 0 \leq i \leq n,$$

puisque nous connaissons déjà $H_0(P^n_{\mathbb{C}})$, les autres groupes étant nuls.

4.4.9 Homologie d'un produit

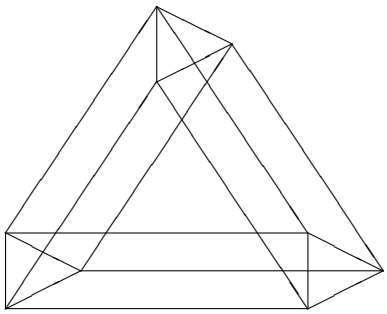
Deux exemples introductifs : le produit $X \subset \mathbb{R}^3$ du triangle creux $V = ABC^\circ$ et du segment $W = CD$ est homéomorphe au tube, dont nous venons de calculer l'homologie : $H_1(X) \cong \mathbb{Z}$, $H_0(X) \cong \mathbb{Z}$. D'autre part, $H_1(V) \cong \mathbb{Z}$, $H_0(V) \cong \mathbb{Z}$, $H_0(W) \cong \mathbb{Z}$ sont les groupes d'homologie non nuls.

Rappelons que $\mathbb{Z}^p \bigotimes \mathbb{Z}^q \cong \mathbb{Z}^{pq}$ et que $\mathbb{Z}^n \bigotimes \mathbb{Z}/2\mathbb{Z} \cong (\mathbb{Z}/2\mathbb{Z})^n$ (cf. *produit tensoriel de modules* dans *Espaces vectoriels, Modules, Matrices*, Modules exercice 13, même page web. Les groupes commutatifs $\mathbb{Z}^p$ sont des $\mathbb{Z}$-modules). On a donc $\mathbb{Z}^p \bigotimes \mathbb{Z} \cong \mathbb{Z}^p$, $\mathbb{Z}^p \bigotimes \mathbb{Z}^0 \cong \mathbb{Z}^0 = 1$ et $\mathbb{Z}^p \bigotimes 0 = 0$.



On vérifie que $H_1(X) \cong H_1(V) \bigotimes H_0(W)$ et que $H_0(X) \cong H_0(V) \bigotimes H_0(W)$.

Deuxième exemple : le produit T de deux triangles creux T_1 et T_2, homéomorphe au tore creux.



On obtient 9 carrés pleins, d'où 18 triangles pleins, autant d'arêtes et 9 sommets.

On vérifie que :

$$\begin{cases} H_2(T) \cong H_1(T_1) \bigotimes H_1(T_2), \\ H_1(T) \cong H_1(T_1) \bigotimes H_0(T_2) \\ \qquad\qquad \times H_0(T_1) \bigotimes H_1(T_2), \\ H_0(T) \cong H_0(T_1) \bigotimes H_0(T_2). \end{cases}$$

Théorème 4.1. *L'espace produit de deux variétés réelles triangulables V et W, $X = V \times W$, est triangulable et son homologie est le produit tensoriel de leurs homologies : $H_*(X) = H_* \bigotimes(V) H_*(W)$, soit, pour tout n :*

$$H_n(X) = \sum_{p+q=n} H_p(V) \bigotimes H_q(W).$$

Démonstration. Le produit X d'un p-simplexe $[A_0, \ldots, A_p]$ et d'un q-simplex $[B_0, \ldots, B_q]$, ordonnés, est un **prisme** de $\mathbb{R}^{p+q}$, ayant $(p+1)(q+1)$ sommets, les $A_i \times B_j$, suivant l'ordre lexicographique, est un **prisme**, que l'on peut trianguler en complétant son ensemble simplicial. Ainsi, le produit $AB \times CD$ est un carré que l'on triangularise par ajout d'une diagonale.

Passons maintenant à $V \times W$, et supposons que $H_p(V) \cong \mathbb{Z}^r$ et $H_q(W) \cong \mathbb{Z}^s$, $p + q = n$. Le produit d'un p-trou de V et d'un q-trou de W est un $p + q$-trou de X. En effet, le produit d'un p-cube (cube de dimension p) et d'un q-cube est un $p + q$-cube.

Réciproquement, un n-trou dans $X \times Y$ contient un hyper-cube parallèle à X et à Y, c'est- à-dire produit d'un p-cube de X et d'un q-cube de Y obtenus par projection, avec $p + q = n$.

Les n-trous de X sont donc les produits des p-trous de V et des q-trou de W avec $p+q = n$. On en déduit $H_n(X \times Y)$, comme produit des $H_P(X) \bigotimes H_q(Y)$, pour tous les couples (p, q) tels que $p + q = n$. □

Corollaire. Si l'homologie de W est réduite à H_0, l'homologie de $V \times W$ est égale à celle de V. C'est le cas si $W = [0, 1]$, si $W = S_n$ ou plus généralement si W est contractile, car un espace contractile ne pouvant contenir de trou, a une homologie réduite à $H_0(W) \cong \mathbb{Z}$.

4.5 Exercices

(1) Calculer l'homologie du trèfle creux.

(2) Calculer directement l'homologie de S^2.

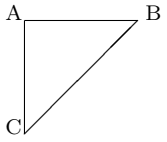
(3) Calculer l'homologie :
(a) du tore,
(b) du plan projectif,
(c) de la bouteille de Klein,
d'après les figures à la fin de 4.3.

(4) Trianguler le tore double (à deux trous) creux, en utilisant le tétraèdre creux et deux tube de section triangulaire. Calculer son homologie.

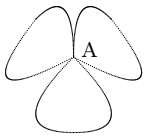
(5) Calculer directement :
(a) l'homologie de P^3,
(b) l'homologie de P^4.

4.6 Correction des exercices

(1) Si nous quotientons le triangle creux ABC° par les relations d'équivalence $A \sim B$ et $B \sim C$, nous obtenons le trèfle creux :



$\xrightarrow{A \sim B \sim C}$



$$\begin{cases} E_1 = \{[AB]^\sim, \\ [BC]^\sim, [CA]^\sim\}, \\ E_0 = \{[A]\}. \end{cases}$$

Son ensemble simplicial est :

$$\begin{cases} E_1 = \{[AB]^\sim, [BC]^\sim, [CA]^\sim\}, \\ E_0 = \{[A]\}, \end{cases}$$

d'où $G_1 \equiv \mathbb{Z}^3$, $G_0 \equiv \mathbb{Z}$.

Les simplexes $[AB]^\sim$, $[BC]^\sim$ et $[CA]^\sim$ sont chacun homéomorphes à un cercle, et leur bord est nul ; $\operatorname{Im} \partial_1 = 0$, $\ker \partial_1 \cong \mathbb{Z}^3$, $\ker \partial_0 \cong \mathbb{Z}$. D'où $G_1 \cong \mathbb{Z}^3$, $G_0 \cong \mathbb{Z}$, $H_1 \cong \mathbb{Z}^3$, $H_0 \cong \mathbb{Z}$.

(2) Comme S^2 est homéomorphe au tétraèdre creux $ABCD$, calculons directement l'homologie de ce dernier :
- son ensemble simplicial :

$$\begin{cases} E_2 = \{[ABC], [ACD], [ABD], [BCD]\}, \\ E_1 = \{[AB], [AC], [AD], [BC], [BD], [CD]\}, \\ E_0 = \{[A], [B], [C], [D]\}, \end{cases}$$

- ses groupes simpliciaux $G_2 \equiv \mathbb{Z}^4$, $G_1 \equiv \mathbb{Z}^6$, $G_0 \equiv \mathbb{Z}^4$,
- les images des opérateurs de bord :

$$\begin{array}{rcl} \operatorname{Im}\partial_2 & = & \mathbb{Z}([BC]-[AC]+[AB])+\mathbb{Z}([CD]-[AD]+[AC]) \\ & & +\mathbb{Z}([BD]-[AD]+[AB])+\mathbb{Z}([CD]-[BD]+[BC]) \\ & \equiv & \mathbb{Z}^3 \end{array}$$

puisque :

$$\begin{array}{rcl} 0 & = & ([BC]-[AC]+[AB])+([CD]-[AD]+[AC]) \\ & & -([BD]-[AD]+[AB])-([CD]-[BD]+[BC]), \end{array}$$

puis :

$$\begin{array}{rcl} \operatorname{Im}\partial_1 & = & \mathbb{Z}([B]-[A])+\mathbb{Z}([C]-[A])+\mathbb{Z}([D]-[A]) \\ & & +\mathbb{Z}([C]-[B])+\mathbb{Z}([D]-[B])+\mathbb{Z}([D]-[C]) \\ & = & \mathbb{Z}([C]-[A])+\mathbb{Z}([D]-[A])+\mathbb{Z}([D]-[B]) \\ & \equiv & \mathbb{Z}^3 \end{array}$$

et $\operatorname{Im}\partial_0 = 0$, d'où leurs noyaux :

$$\begin{cases} \operatorname{Ker}\partial_2 \cong \mathbb{Z}, \\ \operatorname{Ker}\partial_1 \cong \mathbb{Z}^3, \\ \operatorname{Ker}\partial_0 \cong \mathbb{Z}^4, \end{cases}$$

et l'homologie $H_2 \cong \mathbb{Z}$, $H_1 \cong 0$, $H_0 \cong \mathbb{Z}$.

(3) (a) Pour le tore T, les relations d'équivalence sont $AB \sim DC$ et $AD \sim BC$. Ecrivons l'ensemble simplicial :

$$\begin{cases} E_2 & = \{[ABD]^\sim, [DBC]^\sim\}, \\ E_1 & = \{[AB]^\sim, [BC]^\sim, [CD]^\sim, [AD]^\sim, [BD]^\sim\} \\ & = \{[AB]^\sim, [BC]^\sim, \ ([BD]^\sim\}, \\ E_0 & = \{[A]\} \quad (\text{puisque } [B]^\sim = [C]^\sim = [D]^\sim = [B]), \end{cases}$$

et les groupes simpliciaux $G_2 \cong \mathbb{Z}^2$, $G_1 \cong \mathbb{Z}^3$, $G_0 \cong \mathbb{Z}$, puis les images des opérateurs de bord :

$$\begin{cases} \operatorname{Im}\partial_2 & = \mathbb{Z}([BD]^\sim - [AD]^\sim + [AB]^\sim) + \mathbb{Z}([BC]^\sim - [DC]^\sim + [DB]^\sim) \\ & = \mathbb{Z}([BD]^\sim - [AD]^\sim + [AB]^\sim) \\ & \cong \mathbb{Z}, \\ \operatorname{Im}\partial_1 & = \mathbb{Z}([B]^\sim - [A]^\sim) + \mathbb{Z}([C]^\sim - [B]^\sim) + \mathbb{Z}([D]^\sim - [B]^\sim) \\ & 0, \\ \operatorname{Im}\partial_0 & = 0, \end{cases}$$

et leurs noyaux : $\operatorname{Ker}\partial_2 \cong \mathbb{Z}$, $\operatorname{Ker}\partial_1 \cong \mathbb{Z}^3$, $\operatorname{Ker}\partial_0 \cong \mathbb{Z}$, puis les groupes d'homologie : $H_2(T) \cong \mathbb{Z}$, $H_1(T) \cong \mathbb{Z}^2$ et $H_0(T) \cong \mathbb{Z}$.

C'est plus compliqué que le calcul de l'homologie de $S^1 \times S^1$!

(b) Pour le plan projectif P^2, les relations d'équivalence sont $AB \sim CD$ et $BC \sim DA$. Il est homéomorphe à la demi-sphère supérieure de $\mathbb{R}^3$, correspondant à $z > 0$, complétée par la moitié de l'équateur, refermée sur elle-même en un cercle. Il n'y a donc pas de volume intérieur, et $H_2(P^2) = 0$. ∂_2 est d'ailleurs injective.

Si l'on commence par coller AB et CD, on obtient le ruban de Mœbius, dont le bord correspond à BC et AD ($C = A$). Puis on colle BC et DA ($[B]^\sim = [D]^\sim$, $[BD]^\sim$ devenant un cercle, $[C]^\sim = [A]^\sim$).

Ecrivons l'ensemble simplicial de P^2 :

$$\begin{cases} E_2 &= \{[ABD]^\sim, [BCD]^\sim\}, \\ E_1 &= \{[AB]^\sim, [BC]^\sim, [BD]^\sim, \\ E_0 &= \{[A], [B]\}, \end{cases}$$

et les groupes simpliciaux $G_2 \cong \mathbb{Z}^2$, $G_1 \cong \mathbb{Z}^2$, $G_0 \cong \mathbb{Z}^2$, puis les images des opérateurs de bord :

$$\begin{cases} \operatorname{Im}\partial_2 &= \mathbb{Z}([BD]^\sim - [AD]^\sim + [AB]^\sim) - \mathbb{Z}([CD]^\sim - [BD]^\sim + [BC]^\sim) \\ &= \mathbb{Z}([BD]^\sim + [BC]^\sim + [AB]^\sim) + \mathbb{Z}([AB]^\sim - [BD]^\sim + [BC]^\sim) \\ &= \mathbb{Z}([AB]^\sim + [BC]^\sim + [BD]^\sim) + \mathbb{Z}(2\,[BD]^\sim) \\ &\cong \mathbb{Z} + 2\mathbb{Z}, \\ \operatorname{Im}\partial_1 &= \mathbb{Z}([B]^\sim - [A]^\sim) + \mathbb{Z}([C]^\sim - [B]^\sim) \\ &\cong \mathbb{Z}, \\ \operatorname{Im}\partial_0 &= 0, \end{cases}$$

et leurs noyaux : $\operatorname{Ker}\partial_2 = 0$ car ∂_2 est injective, $\operatorname{Ker}\partial_1 \cong \mathbb{Z}^2$, $\operatorname{Ker}\partial_0 \cong \mathbb{Z}^2$, puis les groupes d'homologie : $H_2(P^2) = 0$, $H_1(P^2) \cong \mathbb{Z}/2\mathbb{Z}$ et $H_0(P^2) \cong \mathbb{Z}$.

(c) Pour la bouteile de Klein, les relations d'équivalence sont $AB \sim CD$ et $BC \sim AD$, d'où $A \sim C$, $B \sim D$, $B \sim A$ et $C \sim D$, et il ne reste que la classe de A.

En collant BC et AD, on obtient le tube ; AB et DC donnent deux cercles constituant le bord du tube. En collant AB et CD, on colle les cercles-bords du tube en inversant l'orientation, ce qui donne le bord de la bouteile de Klein. On ne peut le faire dans $\mathbb{R}^3$ puisque le tube devrait se traverser lui-même. On peut entrer dans le tube ainsi recollé, le parcourir puis en sortir par le même endroit, de sorte qu'il n'a pas de volume intérieur ($H_2 = 0$).

Ecrivons l'ensemble simplicial :

$$\begin{cases} E_2 &= \{[ABD]^\sim, [BCD]^\sim\}, \\ E_1 &= \{[AB]^\sim, [BC]^\sim, [BD]^\sim, \\ E_0 &= \{[A]\}, \end{cases}$$

et les groupes simpliciaux $G_2 \cong \mathbb{Z}^2$, $G_1 \cong \mathbb{Z}^3$, $G_0 \cong \mathbb{Z}$, puis les images des opérateurs de bord :

$$\begin{cases} \operatorname{Im}\partial_2 & = \mathbb{Z}([BD]^\sim - [AD]^\sim + [AB]^\sim) + \mathbb{Z}([CD]^\sim - [BD]^\sim + [BC]^\sim) \\ & = \mathbb{Z}([BD]^\sim - [AD]^\sim + [AB]^\sim) + \mathbb{Z}(-[BD]^\sim + [AB]^\sim + [AD]^\sim) \\ & = \mathbb{Z}([AB]^\sim - [AD]^\sim + [BD]^\sim) + \mathbb{Z}(2[AB]^\sim) \\ & = \mathbb{Z} \oplus 2\mathbb{Z}, \\ \operatorname{Im}\partial_1 & = \mathbb{Z}([B]^\sim - [A]^\sim) + \mathbb{Z}([D]^\sim - [B]^\sim) + \mathbb{Z}([C]^\sim - [B]^\sim) \\ & = 0, \\ \operatorname{Im}\partial_0 & = 0, \end{cases}$$

et leurs noyaux : $\operatorname{Ker}\partial_2 = 0$, $\operatorname{Ker}\partial_1 \cong \mathbb{Z}^3$, $\operatorname{Ker}\partial_0 \cong \mathbb{Z}$,puis les groupes d'homologie : $H_2(K) = 0$, $H_1(K) \cong \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ et $H_0(K) \cong \mathbb{Z}$.

(4) Partons des arêtes du tétraèdre $ABCD$, son *squelette*, et des deux tubes de bords respectifs $E_1E_2E_3$, $F_1F_2F_3$ pour le premier et $A_1A_2A_3$ $B_1B_2B_3$ pour le second. Collons le premier tube au squelette du tétraèdre en identifiant E_1E_2 à AB, E_2E_3 à BC, puis E_3E_1 à CA, puis $F_1F_2F_3$ à ACD, et de même ABD et BCD aux bords du second tube.

La figure obtenue est homéomorphe au tore double. Elle a six faces rectangulaires, donc douze faces triangulaires, douze arêtes et quatre sommets. L'image de ∂_2 est engendrée par le bord du tétraèdre (AB, AC, BC, CD et DB, la somme des six étant nulle) donc $\operatorname{Im}\partial_2 \cong \mathbb{Z}^5$, d'où $\operatorname{Ker}\partial_2 \cong \mathbb{Z}$ et $H_2 \cong \mathbb{Z}$. L'image de ∂_1 est engendrée par $B - A$, $B - C$ et $C - D$, les autres ($A - C$, $A - D$ et $B - D$ étant combinaisons des trois premiers), et $\operatorname{Im}\partial_1 \cong \mathbb{Z}^3$, $\operatorname{Ker}\partial_1 \cong \mathbb{Z}^9$ et $H_1 \cong \mathbb{Z}^4$. Enfin, $\operatorname{Ker}\partial_0 \cong \mathbb{Z}^4$ et $H_0 \cong \mathbb{Z}$.

(5) (a) Pour P^3, quotient de $S^3 \subset \mathbb{R}^4$, il faut sept points, $A_0, \ldots, A_6$. Construisons une triangulation à partir de celle donnée pour P^2, d'après la figure précédente.

Le pôle Nord sera A_0, A sera noté A_1, B, A_2, C, A_3, l'antipode de A, A_4, D, A_5 et E, A_6. L'antipode de A_i pour $1 \leq i \leq 3$ est donc A_{i+3}.

Nous savons que $H_3(P^3) \cong \mathbb{Z}$, $H_2(P^3) = 0$,$H_1(P^3) \cong \mathbb{Z}/2\mathbb{Z}$ et $H_0(P^3) \cong \mathbb{Z}$, mais nous allons retrouver ces résultats.

Les 3-faces (E_3) sont obtenues à partir des 2-faces de la triangulation de P^2, puis en remplaçant A_1 par A_4, enfin en ajoutant A_0 à chacune. Ainsi, $[A, B, C]$ devient $[A_1, A_2, A_3]$ et donne $[A_0, A_1, A_2, A_3]$ et $[A_0, A_4, A_2, A_3]$. Ce faisant, on obtient les huit tétraèdres :

$$\begin{aligned} E_3 \quad = \quad & \{[A_0, A_1, A_6, A_2], [A_0, A_1, A_2, A_3], [A_0, A_1, A_3, A_5], [A_0, A_1, A_5, A_6], \\ & [A_0, A_4, A_6, A_2], [A_0, A_4, A_2, A_3], [A_0, A_4, A_3, A_5], [A_0, A_4, A_5, A_6]\}. \end{aligned}$$

On voit que $E_3'' = E_3$ et que $E_3' = \emptyset$, d'où $H_3' = 0$.

Les bords opposés à A_0 donnent une triangulation de S^2 compatible avec l'antipodie, d'où, une fois quotientés par a, une triangulation de P^2.

Calculons $\partial E_3 \subset E_2''$, ensemble des images de ces tétraèdres, et Σ la somme de ces images. On a par exemple :

$$\partial[A_0, A_1, A_6, A_2] = [A_1, A_6, A_2] - [A_0, A_6, A_2] + [A_0, A_1, A_2] - [A_0, A_1, A_6].$$

Le premier triangle s'annule avec le premier de $\partial[A_0, A_4, A_3, A_5]$ car a inverse l'orientation (elle agit sur S^2 qui est dans $\mathbb{R}^3$) ; le second, avec le second du cinquième, etc.

Ceci montre que $\Sigma = 0$, cette relation de dépendance étant la seule possible, chaque triangle ne figurant que deux fois, ce qui impose les coefficients de la relation. On a donc :

$$\operatorname{Im}\partial_3 = \mathbb{Z}^7,\ \operatorname{Ker}\partial_3 = \mathbb{Z},\ H_3'' \cong \mathbb{Z},\ H_3(P^3) = H_3' \oplus H_3'' \cong \mathbb{Z}.$$

Les 2-faces (E_2) sont les quatre contenant A_0 et A_1, les quatre contenant A_0 et A_4, et les quatre contenant A_0 mais ni A_1 ni A_4 :

$$\begin{aligned} E_2'' \quad = \quad & \{[A_0, A_1, A_i],\ i \in \{2,3,5,6\} \ \cup\ \{[A_0, A_4, A_i],\ i \in \{2,3,5,6\}\} \\ & \cup \{[A_0, A_2, A_3], [A_0, A_3, A_5], [A_0, A_5, A_6], [A_0, A_6, A_2]\}, \end{aligned}$$

plus les huit ne contenant pas A_0 et triangulant S^2 :

$$E_2' = \{[A_i, A_2, A_3], [A_i, A_3, A_5], [A_i, A_5, A_6],\ i \in \{1,4\}\}$$

sur lesquels on fera agir l'antipodie, après quoi il en restera deux, $[A_1, A_2, A_3]$ et $[A_1, A_3, A_5]$. L'homologie de E_2' est celle de P^2. Celle de E_2'' est facteur direct de $H_2(S^3)$, elle est donc nulle.

Finalement :

$$H_0(P^3) \cong \mathbb{Z},\ H_1(P^3) \cong \mathbb{Z}/2\mathbb{Z},\ H_2(P^3) = 0,\ H_3(P^3) \cong \mathbb{Z}.$$

(b) Passons à P^4, toujours avec les mêmes notations et avec neuf points, $A_0, \ldots, A_8$. Renumerotons les points de la triangulation de P^3 : A_i devient A_{i+1} pour $0 \leq i \leq 3$, et A_{i+2} pour $4 \leq i \leq 6$, A_5 étant l'antipode de A_1, de sorte que A_{i+4} est l'antipode du nouveau A_i pour $1 \leq i \leq 4$, et A_0 est le pôle Nord de S^4.

L'ensemble E_4 est obtenu en ajoutant A_0 aux huit tétraèdres de E_3 et aux huit autres obtenus en remplaçant A_1 par A_5. Il est donc constitué de seize pentaèdres. Il triangule la demi-hyper-sphère supérieure S^4_+. Les bords inférieurs de ces pentaèdres, obtenus en enlevant A_0, triangulent S^3, et c'est sur eux qu'agit l'antipodie.

La somme Σ des éléments de ∂E_4 contenant A_0 est nulle car chacune de ces 3-faces est commune à deux pentaèdres, avec des signes opposés, et c'est donc l'unique relation.

Les huit 3-faces ne contenant pas A_0 sont opposées deux à deux par antipodie, elles s'ajoutent, a conservant l'orientation dans $\mathbb{R}^4$.

Le noyau de ∂_4 est donc nul, $H_4(P^4) = 0$, et son image est isomorphe à $\mathbb{Z}^{15} + 2\mathbb{Z}$.

Les H'_3, $i \leq 3$, facteur direct des $H_3(S^4)$, est nul. Quant à H''_3, il serait nul pour la même raison si $\operatorname{Im} \partial_4 \cong \mathbb{Z}^{16}$. L'un des facteurs $\mathbb{Z}$ n'est pas annulé, mais quotienté par $2\mathbb{Z}$. Pour $i \leq 2$, les H''_i sont nuls et les H'_i sont ceux de P^2.

L'homologie de P^4 est donc :

$$H_0(P^4) \cong \mathbb{Z},\ H_1(P^4) \cong \mathbb{Z}/2\mathbb{Z},\ H_2(P^4) = 0,\ H_3(P^4) \cong \mathbb{Z}/2\mathbb{Z},\ H_4(P^4) = 0.$$

5 Anneaux et Corps

5.1 Anneau

Un **anneau** est un triplet $(A, +, \times)$ dans lequel A est l'ensemble des éléments, « + » est une loi de composition telle que $(A, +)$ soit un groupe commutatif (de neutre 0_A ou 0, s'il n'y a pas de confusion possible) et « × » est une loi de composition associative, admettant un neutre 1_A (ou simplement 1) et distributive par rapport à l'addition, à gauche et à droite :

$$a \times (b + c) = a \times b + a \times c,$$

$$(b + c) \times a = b \times a + c \times a,$$

quels que soient les éléments a, b, c de A. L'anneau est non nul si $1 \neq 0$; cette condition sera toujours supposée remplie.

Si la multiplication est commutative, l'anneau est **commutatif** ; l'anneau $\mathbb{Z}$ des nombres entiers relatifs, l'anneau $\mathbb{Z}[X]$ des polynômes à coefficients dans $\mathbb{Z}$, sont des anneaux commutatifs. Les anneaux de matrices ne sont pas en général commutatifs.

On omet chaque fois que cela est possible le symbole $\times$, et on écrit ab pour $a \times b$.

S'il existe des entiers naturels $n \geq 2$ tels que :

$$\forall x \in A, nx = x + \cdots + x = 0,$$

leur ensemble E_+ est une partie non vide de $\mathbb{N}$, et a donc un plus petit élément n_0. Si $n \in E$, il existe des naturels a et $r < n_0$, tels que $n = an_0 + r$; on a alors $rx = (n - an_0)x = 0$, $r \in E$, et $r = 0$. Comme on peut rajouter 0 et les opposés des élémets de E_+, l'ensemble des entiers n tels que, pour tout x dans A, $nx = 0$ est égal à $n_0\mathbb{Z}$, et n_0 est la **caractéristique** de l'anneau. Sinon, l'anneau est de caractéristique nulle. Les anneaux $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont de caractéristique nulle.

L'ensemble des classes modulo n dans $\mathbb{Z}$, muni des opérations naturelles est un anneau de caractéristique n, commutatif, noté $\mathbb{Z}/n\mathbb{Z}$. Une classe est généralement représentée par le plus petit entier positif a qu'elle contient. On la notera $\dot{a}$. Ses autres éléments sont de la forme $a + nb$, $n \in \mathbb{Z}$.

L'ensemble des polynômes à coefficients dans un anneau A est un anneau, contenant A, noté $A[X]$. Les majuscules désignent toujours les indéterminées, les minuscules, des variables.

Un **morphisme d'anneaux** est une application ϕ d'un anneau A dans un anneau B qui respecte les deux structures d'anneaux :

$$\forall x \in A,\ \forall y \in A,\ \phi(x + y) = \phi(x) + \phi(y),\ \phi(xy) = \phi(x)\phi(y).$$

Il vérifie donc $\phi(0_A) = 0_B$ et $\phi(1_A) = 1_B$. C'est un **isomorphisme** s'il admet un morphisme réciproque, et un **automorphisme** si $B = A$.

Un **sous-anneau** d'un anneau A est une partie de A qui est un anneau pour les mêmes lois que A, et qui contient donc les deux éléments neutres de A : $\mathbb{Z}$ est un sous-anneau de $\mathbb{Q}$. Si A est de caractéristique nulle, tout sous-anneau, contenant 1, contient un sous-anneau isomorphe à $\mathbb{Z}$. S'il est de caractéristique n, tout sous-anneau contient, pour la même raison, un sous-anneau isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Considérons, dans un anneau commutatif A, l'équation $ax = b$; si elle admet une solution $x \neq 0$ lorsque $b = 0$, l'élément a est un **diviseur de zéro** ; sinon il est **régulier**, et $x = 0$ est solution unique. Si elle admet une solution dans le cas $b = 1$, a est **inversible** et la solution, notée a^{-1}, est l'**inverse** de a ; l'ensemble des éléments inversibles de A est un groupe pour la multiplication, noté U_A, pour réserver la notation A^* à A privé de 0. Un élément inversible est évidemment régulier, sans réciproque : dans $\mathbb{Z}$, 2 est régulier mais non inversible.

L'image par un morphisme ϕ d'un élément inversible x est inversible, et $\phi(x^{-1})$ est l'inverse de $\phi(x)$, car $\phi(x)\phi(x^{-1}) = \phi(1) = 1$.

Un anneau commutatif est **intègre** si un produit ne peut être nul que si l'un des facteurs au moins est nul, c'est- à-dire si tout élément non nul est régulier. L'anneau $\mathbb{Z}/4\mathbb{Z}$ n'est pas intègre car $\dot{2} \times \dot{2} = \dot{4} = \dot{0}$; $\dot{2}$ est donc un diviseur de zéro ; ses éléments inversibles sont $\dot{1}$, le neutre, et $\dot{3}$ qui est son propre inverse ($\dot{3} \times \dot{3} = \dot{9} = \dot{1}$). L'anneau $\mathbb{Z}/p\mathbb{Z}$ est intègre si et seulement si p est premier. Dans ce cas, tout élément non nul est inversible ; il peut en effet être représenté par un naturel q, $0 \leq q < p$, évidemment premier avec p, et il existe alors (identité de Bézout, page 65) un couple d'entiers (r, s) tel que $rq + sp = 1$. On a alors $rq =\equiv 1 \pmod{p}$, $\dot{r}\,\dot{q} = \dot{1}$ dans $\mathbb{Z}/p\mathbb{Z}$, et la classe de r est l'inverse de celle de q.

Un élément a d'un anneau A est **irréductible** s'il n'est pas nul, pas inversible, et si ses seuls diviseurs sont les $u \in U_A$ et les ua. Ainsi -3 est irréductible dans $\mathbb{Z}$, dont les éléments inversibles sont 1 et -1 et les éléments irréductibles sont les nombres premiers.

Un anneau commutatif intègre est **factoriel** si tous ses éléments sont produits de puissances d'éléments irréductibles, cette décomposition étant unique à des facteurs inversibles près. Ainsi $\mathbb{Z}$ est un anneau factoriel.

L'**anneau-produit** de deux anneaux A et B est l'ensemble $A \times B$ muni des lois $(a, b) + (a', b') = (a + a', b + b')$ et $(a, b)(a', b') = (aa', bb')$. le neutre est $(1, 1)$. Les vérifications sont immédiates. Ce produit n'est jamais intègre car $(1, 0)(0, 1) = (0, 0)$.

Si A et B sont de même caractéristique différente de 2, le produit (celui de $\mathbb{C}$) $(a, b)(a', b') = (aa' - bb', ab' + a'b)$ conserve l'intégrité et la commutativité. Le neutre est $(1, 0)$. En caractéristique 2, on a $(1, 1)(1, -1) = (0, 0)$.

5.2 Anneau de polynômes

Si A est un anneau intègre, l'ensemble des suites $(a_0, a_1, \ldots) = (a_i)$ d'éléments de A ne contenant qu'un nombre fini de termes non nuls muni de l'addition :

$$(a_i) + (b_i) = (a_i + b_i)$$

et du produit :

$$(a_i)(b_i) = (c_i),\ c_i = \sum_{j+k=i} a_j\, b_k$$

est un anneau commutatif, la vérification est facile. On note a_0 la suite réduite à un terme (a_0), $a_n X^n$ la suite réduite à un terme (a_n), et on appelle X l'**indéterminée canonique**, que l'on peut aussi bien noter Y, Z,...

Les éléments de cet anneau sont les scalaires (a_0), les **monômes** à une indéterminée $a_n X^n$ pour $i \geq 1$, les **polynômes** à une indéterminée si la suite n'est pas réduite à un seul terme, et l'anneau est noté $A[X]$. Soit $P \in A[X]$, dont le premier coefficient non nul est a_h et le dernier est a_k ; h est alors la **valuation** de P, notée $\mathrm{val}(P)$, k est son **degré**, noté $\deg(P)$, et P s'écrit $a_h X^h + \cdots + a_k X^k$.

Le terme de plus haut degré du produit de deux polynômes quelconques P et Q est le produit des termes de plus haut degré de chaque polynôme, produit non nul puisque A est intègre, de sorte que $\deg(PQ) = \deg(P) + \deg(Q)$ et que l'anneau $A[X]$ est intègre. De même pour les termes de plus bas degré. Quant à leur somme, les termes de plus haut degré, comme de plus bas, peuvent s'annuler s'ils sont opposés. Les propriétés du degré :

$$\begin{cases} \deg(PQ) = \deg(P)\ \deg(Q), \\ \deg(P+Q) \leq \sup(\deg(P), \deg(Q)) \end{cases}$$

et de la valuation :

$$\begin{cases} \mathrm{val}(PQ) = \mathrm{val}(P)\,\mathrm{val}(Q), \\ \mathrm{val}(P+Q) \geq \inf(\mathrm{val}(P), \mathrm{val}(Q)) \end{cases}$$

sont ainsi de vérification facile.

On définit l'anneau des polynômes à deux indéterminées $A[X,Y] = A[X][Y]$, polynômes en Y à coefficients dans $A[X]$ (ou l'inverse : $A[Y][X]$), et, par récurrence, l'anneau des polynômes à n indéterminées :

$$A[X_1, \cdots, X_n] = A[X_1, \ldots, X_{n-1}][X_n].$$

Le degré total d'un monôme $aX_1^{p_1} \ldots X_n^{p_n}$, $a \neq 0$, est égal à $p_1 + \cdots + p_n$, et son degré (partiel) en X_i est égal à p_i. Les propriétés du degré sont conservées.

Théorème 5.1. *Si A est un anneau intègre, l'anneau $A[X_1, \ldots, X_n]$, n étant un entier naturel non nul, est factoriel.*

Démonstration. Soit $P \in A[X_1, \ldots, X_n]$ de degré (total), $\deg(P)$, non nul. L'ensemble des suites $P_0 = P$, P_1,..., P_k d'éléments de $A[X_1, \ldots, X_n]$ telles que P_{i+1} divise P_i et :

$$0 = \deg(P_k) \leq \deg(P_{k-1}) \leq \cdots \leq \deg(P_0),$$

n'est pas vide : il contient au moins la suite $P_0 = P$, $P_1 = 1$. Considérons dans cet ensemble une suite de longueur maximale (donc comprise entre 2 et $\deg(P)+1$). Les $Q_i = P_{i+1}/P_i$ sont des éléments irréductibles de $A[X_1, \ldots, X_n]$. Si en effet Q_j était égal au produit $Q'Q''$ de deux polynômes non constants, on pourrait intercaler dans la suite $Q'P_j$ entre P_j et P_{j+1}, et elle ne serait donc pas de longueur maximale. On a alors :

$$P = P_k\, Q_0\, Q_1 \ldots Q_{k-1}.$$

L'unicité, aux éléments inversibles près, provient du fait que, si l'on a deux décompositions :

$$P = P_k\, Q_0 \ldots Q_{k-1} = P_k\, R_0 \ldots R_{k-1},$$

de même longueur puisque maximales, chaque R_i, divisant P, et étant irréductible, doit diviser l'un des Q_j (et réciproquement) et le quotient doit être un inversible, Q_j étant irréductible. □

Si $P(X)$ désigne un polynôme, $x \mapsto P(x)$ désigne la fonction associée, obtenue en substituant la variable x à l'indéterminée X.

5.3 Corps

Un **corps** est un anneau non nul ($1 \neq 0$) dont tous les éléments, 0 excepté, sont inversibles (dans l'anneau) ; il est donc intègre. Si on le note $\mathbb{K}$, $\mathbb{K}^*$ désigne le groupe multiplicatif des éléments non nuls ($\mathbb{K}^* = U_{\mathbb{K}}$). Un **morphisme de corps** est un morphisme d'anneaux, et de même pour un **isomorphisme**. Un corps est commutatif s'il l'est en tant qu'anneau.

Soit A un anneau commutatif intègre. On définit sur $A \times A^*$ la relation :

$$(a, b)\, \Re\, (c, d) \iff ad - bc = 0,$$

qui est une équivalence. On vérifiera (exercice 18) que l'ensemble des classes muni des lois quotient est un corps, le **corps des fractions** de A ; (a, b) est noté a/b. Ainsi $\mathbb{Q}$ est-il le corps des fractions de l'anneau $\mathbb{Z}$.

Lorsqu'un anneau A de caractéristique n est un corps, n est premier, car, sinon, nous avons vu que A n'est pas intègre. Ce corps est de **caractéristique** n. Mais la réciproque est fausse : si n est premier, $(\mathbb{Z}/n\mathbb{Z})[X]$ est un anneau intègre de caractéristique n qui n'est pas un corps.

Le corps $\mathbb{Z}/p\mathbb{Z}$, p premier, est noté $\mathbb{F}_p$.

Les principaux corps, à part les corps finis, sont $\mathbb{Q}$, le corps des nombres rationnels, $\mathbb{R}$, celui des nombres réels et $\mathbb{C}$, celui des nombres complexes.

Un **sous-corps** de $\mathbb{K}$ est un corps pour les mêmes opérations (et les mêmes neutres) contenu dans $\mathbb{K}$. Un corps $\mathbb{L}$ est une **extension** de $\mathbb{K}$ si $\mathbb{K}$ est un sous-corps de $\mathbb{L}$. Ainsi $\mathbb{C}$ est une extension de $\mathbb{R}$, et $\mathbb{Q}$ est un sous-corps de $\mathbb{R}$.

Soit $\mathbb{K}$ un corps de caractéristique p. Il contient les éléments non nuls $k1_K$ pour k allant de 1 à $p-1$, et $p1_K = 0_K$. Un morphisme de corps tel que $\phi(1) = 1_K$ a pour noyau $p\mathbb{Z}$, et $\phi(\mathbb{Z}/pZ)$ est un sous-corps de $\mathbb{K}$ isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

Un raisonnement analogue montre que tout corps de caractéristique 0 contient un sous corps isomorphe à $\mathbb{Q}$.

Remarque : un polynôme de degré d à coefficients dans un anneau non intègre peut s'annuler pour plus de n valeurs de la variable. Ainsi, le polynôme $P = X^2 + 1$ s'annule une infinité de fois dans l'anneau $\mathrm{M}_2(\mathbb{R})$ des matrices à deux lignes et deux colonnes, à coefficients réels ; dans l'anneau $\mathrm{M}_2(\mathbb{Z}/2\mathbb{Z})$, il s'annule quatre fois. Si les coefficients appartiennent à un corps, le polynôme a au plus d racines dans ce corps.

En effet, si :

$$M = \begin{pmatrix} a & c \\ b & d \end{pmatrix},\ x, y, z, t \in \mathbb{K},$$

on a :

$$P(M) = \begin{pmatrix} x^2 + yz & z\,(x+t) \\ y\,(x+t) & t^2 + yz \end{pmatrix}$$

et $P(M) + I = 0$ équivaut à :

$$\begin{cases} x, y \in \mathbb{K}, \\ z = -(x^2+1)/y, \\ t = -x, \end{cases} \quad .$$

Si $\mathbb{K} = \mathbb{R}$, on obtient une infinité de solutions. Si $\mathbb{K} = \mathbb{Z}/2\mathbb{Z}$, les valeurs de x et de y sont 0 ou 1, et il n'y en a plus que quatre. Pour que M appartiene à $\mathbb{K}$, ce doit être une matrice scalaire, donc de la forme $\lambda\, I$, et $\lambda = \pm 1$. ▽

Un élément d'une extension d'un corps $\mathbb{K}$ est **algébrique** sur $\mathbb{K}$ s'il est racine d'un polynôme à coefficients dans $\mathbb{K}$, et **transcendant** sinon. Ainsi $\sqrt{2}$ et le nombre complexe i sont algébriques sur $\mathbb{Q}$ car racine, respectivement, des polynômes $X^2 - 2$ et $X^2 + 1$, à coefficients dans $\mathbb{Q}$, et π est transcendant sur $\mathbb{Q}$. Une extension dont les éléments sont algébriques est une **extension algébrique**. Sinon, elle est **transcendante** : $\mathbb{R}$ est une extension transcendante de $\mathbb{Q}$ car π, par exemple, n'est pas algébrique sur $\mathbb{Q}$, et $\mathbb{C}$ est une extension algébrique de $\mathbb{R}$. On note $\mathbb{K}(t)$ la plus petite extension de $\mathbb{K}$ contenant t ; $\mathbb{C}$ est donc égal à $\mathbb{R}(i)$.

Un corps $\mathbb{K}$ est **algébriquement clos** si tout polynôme de $\mathbb{K}[X]$ de degré d a exactement d racines dans $\mathbb{K}$, chacune comptée avec son ordre de mutiplicité.

Tout corps commutatif admet une extension algébriquement close (théorème de Steinitz [2]), sa **clôture algébrique**, corps engendré par la réunion de ses extensins algébriques. Ainsi $\mathbb{C}$ est la clôture algébrique de $\mathbb{R}$; c'est le Théorème de d'Alembert [3] :

Théorème 5.2 (de d'Alembert)**.** *Tout polynôme de $\mathbb{C}[X]$ est produit de polynômes de degré 1.* □

Le résultat suivant est particulièrement important :

Théorème 5.3 (de Wedderburn [4])**.** *Tout corps fini est commutatif et son groupe multiplicatif est cyclique.*

Démonstration. Soit $\mathbb{K}$ un corps fini et $\mathbb{K}^*$ son groupe multiplicatif, dont l'ordre n se décompose en produit de puissances de nombres premiers :

$$n = p_1^{n_1} \dots p_k^{n_k}.$$

Le neutre est l'unique élément d'ordre 1, et à chaque indice i ($1 \leq i \leq k$) on peut associer un élément d'ordre p_i ; ainsi l'ensemble :

$$E_i = \{j \in \mathbb{N} \,|\, \exists x \in \mathbb{K} : |x| = p_i^j\}$$

est une partie non vide de $\mathbb{N}$ majorée par n_i, l'ordre du groupe engendré par x devant diviser n ; E_i possède un plus grand élément m_i, et il existe un élément a_i de $\mathbb{K}^*$ d'ordre $p_i^{m_i}$; a_i engendre le groupe des racines du polynôme :

$$P_i = X^{p_i^{m_i}} - 1,$$

groupe contenant tous les éléments ayant pour ordre une puissance de p_i.

Soit un élément quelconque z de $\mathbb{K}^*$, d'ordre $|z| = p_1^{z_1} \dots p_k^{z_k}$; élevé à la puissance $q_i = |z|/p_i^{z_i}$ il donne un élément dont l'ordre est une puissance de p_i, donc un élément de E_i. Les q_i sont premiers entre eux dans leur ensemble, n'étant pas divisibles par p_i, et il existe, d'après l'identité de Bézout (page 65), des entiers relatifs s_i tels que :

$$q_1 s_1 + \ldots + q_k s_k = 1 \ ;$$

2. Ernst Steinitz (1871-1928), mathématicien allemand. Voir par exemple Bourbaki, XI, Eléments de Mathématiques, Algèbre, Chapitre 5, §4.

3. Les démonstrations algébriques sont plus ou moins compliquées ; les fonctions holomorphes en donnent une très simple.

4. Joseph Wedderburn (1882-1948), mathématicien écossais.

on en déduit que :

$$z = z^{q_1 s_1 + \ldots + q_k s_k} = (x^{q_1})^{s_1} \ldots (x^{q_k})^{s_k} = a_1^{t_1} \ldots a_k^{t_k},$$

indépendamment de l'ordre des facteurs $a_i^{t_i}$.

Ceci montre que $\mathbb{K}^*$ a au plus $p_1^{m_1} \ldots p_r^{m_r}$ éléments ; or il en a $p_1^{n_1} \ldots p_k^{n_k}$, et donc $m_i = n_i$, et la décomposition de z en puissance de a_i est unique, à l'ordre près. On en déduit la commutativité de $\mathbb{K}$.

Considérons les puissances de l'élément $a_1 \ldots a_k$:

$$a^v = a_1^v \ldots a_k^v.$$

Pour obtenir le neutre, il faut que v soit multiple des ordres des a_i ; son ordre est donc n, et il engendre $\mathbb{K}^*$, qui est donc cyclique. □

Une **valeur absolue** sur un corps $\mathbb{K}$ est une application $N : \mathbb{K} \to \mathbb{R}_+$ telle que, quels que soient x et y :

$$\begin{array}{rcl} N(x) & = & 0 \iff x = 0, \\ N(x\,y) & = & N(x)\,N(y), \\ N(x+y) & \leq & N(x) + N(y). \end{array}$$

Elle est en général notée $|x|$.

5.4 Idéal d'un anneau

Un **idéal** $\mathfrak{I}$ d'un anneau commutatif A est un sous-groupe additif (donc $\mathfrak{I}$ n'est pas vide) stable par multiplication par les éléments de A :

$$\forall x \in \mathfrak{I},\ \forall a \in A,\ ax \in \mathfrak{I}.$$

Les idéaux de $\mathbb{Z}$ sont ses sous-groupes $n\mathbb{Z}$; les idéaux de $\mathbb{R}[X]$ sont les multiples d'un polynôme (exercice 4) ; l'idéal engendré par un élément a est noté (a) ; ainsi, l'idéal de $\mathbb{R}[X]$ engendré par $X^2 + 1$ est-il :

$$(X^2 + 1) = \{(X^2 + 1)P(X) \,|\, P(X) \in \mathbb{R}[X]\}.$$

L'ensemble des polynômes de $\mathbb{K}[X]$ admettant l'élément t, algébrique sur $\mathbb{K}$, pour racine est un idéal de l'anneau factoriel $\mathbb{K}[X]$; il est donc engendré par un polynôme P, irréductible dans $\mathbb{K}[X]$ (sinon l'un de ses facteurs, s'annulant en t, appartiendrait à l'idéal et serait un multiple de P, ce qui est absurde), de degré n ; P est le **polynôme minimal** de t sur $\mathbb{K}$. L'extension algébrique $\mathbb{K}(t)$ de $\mathbb{K}$ est dite « de degré n » (exercice 25).

L'anneau lui-même est un idéal ; l'ensemble réduit au neutre de l'addition est un idéal, dit « trivial » , ou « nul » . On appelle **idéal propre** un idéal différent de l'anneau. Un idéal contenant 1 est égal à l'anneau. Si l'anneau n'est

pas commutatif, on peut définir les notions d'idéal à gauche, à droite, bilatère.

L'**anneau quotient** $A/\mathfrak{I}$ d'un anneau commutatif A par un de ses idéaux, $\mathfrak{I}$, est l'ensemble des classes d'équivalence modulo $\mathfrak{I}$ (deux éléments sont équivalents si leur différence est dans $\mathfrak{I}$; exercice 6).

Un idéal est **monogène**, ou **principal**, s'il est engendré par un élément, comme dans les exemples précédents.

Un **anneau principal** est un anneau intègre (donc commutatif) dont tous les idéaux sont monogènes. Les anneaux $\mathbb{Z}$, $\mathbb{Q}[X]$, $\mathbb{R}[X]$ et $\mathbb{C}[X]$ sont principaux. Le sous-anneau de $\mathbb{R}$ formé des éléments de la forme $x + y\sqrt{2}$, où x et y sont des entiers relatifs, n'est pas principal (exercice 5). On montre facilement qu'un anneau principal est factoriel.

Un idéal est **premier** s'il ne peut contenir un produit sans contenir l'un des facteurs au moins.

Le **radical** $r(\mathfrak{I})$ d'un idéal $\mathfrak{I}$ d'un anneau commutatif A est l'ensemble des éléments de A dont une puissance appartient à $\mathfrak{I}$. Montrons que c'est un idéal. Soient x et y dans $r(\mathfrak{I})$ et a dans A. Il existe des entiers $n > 0$ and $m > 0$ tels que x^n et y^m appartiennent à $r(\mathfrak{I})$. Alors $(ax)^n$ appartient à $\mathfrak{I}$ et ax est dans $r(\mathfrak{I})$. D'autre part, tous les monômes de $(x + y)^{m+n-1}$ sont dans $\mathfrak{I}$, donc aussi leur somme, et $x + y$ appartient à $r(\mathfrak{I})$, qui est ainsi un idéal de A.
Un idéal premier est égal à son radical.

Un idéal **maximal** est un idéal propre qui n'est pas contenu dans un idéal propre plus grand que lui. Tout idéal est contenu dans un idéal maximal (Théorème de Krull). On montrera (exercice 9) qu'un idéal de l'anneau A est maximal si et seulement si $A/\mathfrak{I}$ est un corps, dit **corps résiduel** de l'anneau.

Exemple 5.1. Montrons que les idéaux maximaux de $\mathbb{Z}$ sont de la forme $p\,\mathbb{Z}$, p étant un nombre premier. Soit p un nombre premier et un idéal $\mathfrak{I}$ contenant $p\,\mathbb{Z}$; supposons qu'il existe un élément q de $\mathfrak{I}$ n'appartenant pas à $p\,\mathbb{Z}$, donc non multiple de p ; p et q sont alors premiers entre eux et il existe des entiers u et v tels que $up + vq = 1$ (identité de Bézout, théorème suivant). L'idéal $\mathfrak{I}$, contenant p et q, contient aussi 1 ; par définition d'un idéal, il contient tout élément de $\mathbb{Z}$: il est égal à $\mathbb{Z}$, et $\mathfrak{I}$ est maximal.
Réciproquement, soit $\mathfrak{M}$ un idéal maximal de $\mathbb{Z}$; il est de la forme $a\,\mathbb{Z}$. Supposons a égal à bc : les idéaux $b\,\mathbb{Z}$ et $c\,\mathbb{Z}$ contiennent $a\,\mathbb{Z}$, ce qui est absurde, à moins que l'un des deux soit égal à $\mathfrak{M}$, si par exemple $a = b$, et l'autre à $\mathbb{Z}$, et alors $c = 1$ et a est premier. ▽

Exemple 5.2. Sur la différence entre idéal et sous-anneau. Soit A l'anneau obtenu en munissant $\mathbb{Q} \times \mathbb{Q}$ des opérations :

$$\begin{array}{rcl}(a,b)+(c,d) & = & (a+c, b+d),\\ (a,b).(c,d) & = & (a.c, b.d).\end{array}$$

Ce n'est pas un corps car il contient des diviseurs de zéro ; $\mathfrak{I} = \mathbb{Q} \times \{0\}$ est un idéal de A, mais pas un sous-anneau, bien que ce soit un anneau, car il ne contient pas le neutre $(1,1)$ de A, son propre neutre étant $(1,0)$; $B = \mathbb{Z} \times \mathbb{Z}$ est un sous-anneau de A, mais pas un idéal : il ne contient pas tous les produits de ses éléments par les éléments de A. ▽

Deux idéaux $\mathfrak{I}$ et $\mathfrak{K}$ sont **étrangers** si leur somme :

$$\mathfrak{I} + \mathfrak{K} = \{i + k \,|\, i \in \mathfrak{I},\ k \in \mathfrak{K}\}$$

est égale à l'anneau. Ainsi, d'après l'Exemple 1, il est équivalent de dire que les entiers p et q sont premiers entre eux ou que les idéaux $p\,\mathbb{Z}$ et $q\,\mathbb{Z}$ sont étrangers.

Le théorème suivant est extrêmement important.

Théorème 5.4 (Identité de Bézout)**.** *Des éléments $x_1, \ldots, x_n$ d'un anneau principal A sont premiers entre eux dans leur ensemble, c'est- à-dire que leurs seuls diviseurs communs sont les éléments inversibles de A, si et seulement s'il existe des éléments $y_1, \ldots, y_n$ de A tels que $\sum x_i y_i = 1$.*

Démonstration. Si $d \in A$ divise chaque x_i, il divise $\sum x_i y_i$, quels que soient les y_i. Réciproquement, l'ensemble des $x_i y_i$, quand les y_i sont des éléments quelconques de A, est un idéal, engendré par un élément d de A, l'anneau étant principal ; en prenant les y_i nuls sauf y_k égal à 1, on voit que x_k appartient à l'idéal : il est donc multiple de d, et si les x_i sont premiers entre eux, d doit être inversible. □

Théorème 5.5 (Gauss)**.** *Dans un anneau de polynômes $A = \mathbb{K}[X_1, \ldots, X_n]$ si a divise un produit bc et n'a pas de diviseurs communs avec b, il divise c.*

Démonstration. Le pgcd de a et b est égal à 1 et celui de ac et bc à c. Comme a divise ac et bc, il divise c, leur pgcd. □

Un **anneau local** est un anneau contenant un unique idéal maximal.

Si $\mathfrak{P}$ est un idéal premier d'un anneau intègre, on définit le **localisé** $A_{\mathfrak{P}}$ de A en $\mathfrak{P}$:

$$A_{\mathfrak{P}} = \{ab^{-1} \,|\, a, b \in A,\ b \notin \mathfrak{P}\}.$$

On montrera (exercice 22) que $A_{\mathfrak{P}}$ est un anneau local.

On dit qu'un sous-anneau A d'un corps $\mathbb{K}$ ($A \neq \mathbb{K}$) est un **anneau valué** de $\mathbb{K}$ si pour tout élément x non nul de $\mathbb{K}$ on a $x \in A$ ou $x^{-1} \in A$. Le corps $\mathbb{K}$

est alors un **corps valué**.

Un élément non nul a d'un anneau A est :

$$\begin{array}{ll} \textbf{nilpotent} & \iff \quad \exists n \in \mathbb{N}^* : a^n = 0 \neq a^{n-1}, \\ \textbf{idempotent} & \iff \quad a^2 = a. \end{array}$$

Notons que si a est nilpotent, $1 - a$ est inversible :

$$(1-a)^{-1} = 1 + a + a^2 + \cdots + a^{n-1},$$

et que, s'il est idempotent et inversible $a = 1$.

Si a et b sont des éléments de l'anneau principal $\mathbb{Z}$, les idéaux $a\,\mathbb{Z} + b\,\mathbb{Z}$ et $(a\,\mathbb{Z})(b\,\mathbb{Z})$ sont respectivement égaux à $d\,\mathbb{Z}$ et $m\,\mathbb{Z}$: d est appelé le **pgcd** des deux nombres (leur plus grand commun diviseur), et m leur **ppcm** (leur plus petit commun multiple).

5.5 Relations symétriques et sommes de Newton

Soient $x_1, \ldots, x_n$ des éléments de $\overline{\mathbb{F}}_2$ et $\mathfrak{S}_n$ le groupe des permutations sur n éléments. Une **relation symétrique** f entre les x_i est une fonction polynôme telle que :

$$\forall s \in \mathfrak{S}_n,\ f(x_{s(1)}, \ldots, x_{s(n)}) = f(x_1, \ldots, x_n).$$

En développant le polynôme :

$$\begin{array}{rcl} P & = & (X + x_1) \ldots (X + x_n) \\ & = & X^n + a_1 X^{n-1} + a_2 X^{n-2} + \cdots + a_n, \end{array}$$

on vérifie que a_1 est la somme des x_i, que a_2 est la somme des $x_i x_j$ pour tous les couples (i, j) tels que $i \neq j$, que a_k est la somme de tous les produits de $x_{i_1} \ldots x_{i_k}$, les indices i_h étant deux à deux distincts, et que a_n est le produit de tous les x_i.

On peut alors montrer que toute relation symétrique est une expression algébrique en les a_i, à coefficients entiers. Exemples :

$$\begin{array}{rcl} x_1^3 + x_2^3 + x_3^3 & = & a_1^3 + a_1\, a_2 + a_3\ ; \\ \dfrac{1}{x_1} + \dfrac{1}{x_2} + \dfrac{1}{x_3} & = & \dfrac{a_2}{a_3}. \end{array}$$

Nous allons le montrer pour les **sommes de Newton** :

$$s_k = x_1^k + x_2^k + \cdots + x_n^k$$

pour k compris entre 1 et $n - 1$. Notons $\dot{n}$ l'image de n dans $\mathbb{K}$ (0 si n est pair, 1 sinon).

Théorème 5.6. *Les sommes de Newton et les coefficients de P sont liés par les relations de Newton :*

$$\begin{aligned} 0 &= s_1 + a_1, \\ 0 &= s_2 + a_1\, s_1, \\ &\vdots \\ 0 &= s_n + a_1\, s_{n-1} + \cdots + a_{n-1}\, s_1 + \dot{n}\, a_n. \end{aligned}$$

Démonstration. On a :

$$DP(X) = \sum_{n-k\ impair} a_k\, X^{n-k-1} = \sum_j \prod_{i \neq j} (X + x_i)$$

et :

$$\frac{DP(X)}{P(X)} = \sum_i \frac{1}{X + x_i}.$$

En faisant la somme des :

$$\frac{1}{X + x_i} = \frac{1}{X}\,(1 + \frac{x_i}{X} + (\frac{x_i}{X})^2 + \cdots)$$

on obtient :

$$\frac{DP(X)}{P(X)} = \frac{1}{X}\,(\dot{n} + \frac{s_1}{X} + (\frac{s_2}{X}) + \cdots)$$

puis :

$$DP(X) = (X^n + a_1\, X^{n-1} + \cdots + a_n)\,(\frac{\dot{n}}{X} + \frac{s_1}{X^2} + \frac{s_2}{X^3} + \cdots)$$

Identifions, pour $1 \leq k \leq n-1$, les coefficients de X^k dans cette dernière équation et dans la première expression de $DP(X)$:

$$\begin{aligned} a_{n-1} &= s_{n-1} + a_1\, s_{n-2} + \cdots + \dot{n}\, a_{n-1}, \\ 0 &= s_{n-2} + a_1\, s_{n-3} + \cdots + \dot{n}\, a_{n-2}, \\ a_{\dot{n}-3} &= s_{n-3} + a_1\, s_{n-4} + \cdots + \dot{n}\, a_{n-3}, \\ &\vdots \\ (\dot{n}+1)\, a_3 &= s_3 + a_1\, s_2 + a_2\, s_1 + \dot{n}\, a_3, \\ \dot{n}\, a_2 &= s_2 + a_1\, s_1 + \dot{n}\, a_2. \\ (\dot{n}+1)\, a_1 &= s_1 + \dot{n}\, a_1, \end{aligned}$$

d'où $s_1 = a_1$, $s_2 = a_1^2$, $s_3 = a_3 + a_1\, s_2 + a_2\, s_1 = a_3 + a_1^3 + a_1\, a_2$, etc... □

5.6 Fractions rationnelles

Soit $\mathbb{K}$ un corps algébriquement clos, $\mathbb{K}[X]$ l'anneau des polynômes à une indéterminée à coefficients dans $\mathbb{K}$ et $\mathbb{K}(X)$ le corps des fractions de $\mathbb{K}[X]$, dont les éléments sont appelés « fractions rationnelles » .

Les fractions rationnelles de la forme $(X + a)^{-k}$, $a \in \mathbb{K}$, $k \in \mathbb{N}^*$, sont dites « éléments simples » .

Théorème 5.7. *Toute fraction rationnelle est somme d'un polynôme (sa partie entière) et d'une combinaison linéaire à coefficients dans $\mathbb{K}$ d'éléments simples (sa partie polaire).*

Démonstration. Soit $F = E + P\,Q^{-1}$ une fraction rationnelle : la partie entière E est obtenue par division euclidienne, P et Q sont premiers entre eux et $\deg(P) < \deg(Q)$. Si Q est le produit de deux polynômes, Q_1 et Q_2, premiers entre eux, il existe des polynômes P_1 et P_2 tels que :

$$F = \frac{P_1}{Q_1} + \frac{P_2}{Q_2}.$$

Il existe en effet, d'après l'identité de Bézout (page 64), des polynômes U_1 et U_2 tels que $U_1Q_1 + U_2Q_2 = 1$, et $P_1 = U_2P$, $P_2 = U_1P$. On en déduit par récurrence que si $Q = Q_1 \dots Q_k$, il existe des polynômes P_1,..., P_k tels que :

$$F = \frac{P_1}{Q_1} + \cdots + \frac{P_k}{Q_k}.$$

En factorisant les Q_i :

$$Q_i = \Pi_j (X + a_{ij})^{p_{ij}},$$

on obtient :

$$F = \sum_{1 \le i \le n} \frac{N_{ij}}{(X + a_{ij})^{p_{ij}}},\ \deg(N_{ij}) < p_{ij}.$$

Il n'y a plus qu'à décomposer chaque N_{ij} dans la base formée des puissances de $X + a_{ij}$ ($N_{ij} = \sum_{0 \le k \le p_{ij}-1} \lambda_{ijk}(X + a_{ij})^k$) et à simplifier pour obtenir une expression ayant la forme annoncée :

$$F = \sum_{i,j,k} \frac{\alpha_{ijk}}{(X + a_{ij})^k}.$$ □

5.7 Exercices

(1) Montrer qu'un idéal propre ne peut contenir d'éléments inversibles.

(2) Un anneau est un corps si et seulement s'il n'a pas d'idéal propre non nul.

(3) Construire tous les anneaux à quatre éléments et préciser leurs idéaux propres non nuls et leurs polynômes annulateurs.

(4) Montrer que l'anneau $\mathbb{K}[X]$ ($\mathbb{K}$, corps commutatif) est principal.

(5) Montrer que l'ensemble des éléments de $\mathbb{R}$ de la forme $x + y\sqrt{2}$ où x et y sont dans $\mathbb{Z}$ est un sous-anneau de $\mathbb{R}$ non principal (montrer que les éléments de la forme $2x + y\sqrt{2}$ constituent un idéal non monogène).

(6) Vérifier que $A/\mathfrak{I}$ est un anneau, $\mathfrak{I}$ étant un idéal de l'anneau A.

(7) Montrer que l'image réciproque d'un idéal par un morphisme d'anneaux est un idéal. A quelle condition l'image directe d'un idéal est-elle un idéal ?

(8) Montrer que l'anneau quotient d'un anneau principal par un idéal premier est principal.

(9) Montrer qu'un idéal $\mathfrak{M}$ d'un anneau est maximal si et seulement si $A/\mathfrak{M}$ est un corps.

(10) Monter que, $\mathfrak{I}$ et $\mathfrak{K}$ étant des idéaux de l'anneau commutatif A, $\mathfrak{I}+\mathfrak{K}$, $\mathfrak{I}\mathfrak{K}$, $\mathfrak{I}\cap\mathfrak{K}$, sont des idéaux de A. Que peut-on dire de $\mathfrak{I}\cup\mathfrak{K}$? Comparer $\mathfrak{I}\mathfrak{K}$ et $\mathfrak{I}\cap\mathfrak{K}$ lorsque $\mathfrak{I}$ et $\mathfrak{K}$ sont étrangers. Vérifier que si $\mathfrak{I}$ est maximal et ne contient pas $\mathfrak{K}$, $\mathfrak{I}$ et $\mathfrak{K}$ sont étrangers. Préciser les idéaux étrangers de $\mathbb{Z}$.

Les Exercices 11 à 17 sont liés.

(11) Soit $\mathbb{Z}_p$ l'ensemble des rationnels dont le dénominateur n'est pas divisible par le nombre premier p. Montrer que $\mathbb{Z}_p$ est un anneau valué. Traiter le cas $p=3$.

(12) Caractériser les éléments inversibles, dits unités, de $\mathbb{Z}_p$. On note U leur ensemble ; montrer que U est un groupe et que la relation dans $\mathbb{Q}$:

$$x\,\Re\,y \iff [\exists u\in U : y=ux]$$

est une équivalence, que l'on notera $x\sim y$.

(13) Montrer que pour tout élément x de $\mathbb{Q}$ il existe un entier relatif n tel que $x\sim p^n$. On pose $v_p(x)=n$, ce qui définit la valuation de x. On convient que $v_p(0)=+\infty$.

(14) Montrer que :

$$\begin{aligned} v_p(xy) &= v_p(x)+v_p(y),\\ v_p(x+y) &\geq \min(v_p(x),v_p(y)). \end{aligned}$$

(15) Montrer que les éléments d'un idéal propre non nul $\mathfrak{I}$ de $\mathbb{Z}_p$ sont multiples d'une certaine puissance p^n de p, $n\in\mathbb{N}^*$, et qu'on a donc $\mathfrak{I}=p^n\mathbb{Z}_p$, ce qui caractérise complètement les idéaux de $\mathbb{Z}_p$.

(16) Soit A un anneau de valuation d'un corps commutatif $\mathbb{K}$. Montrer que A est un anneau local, dont l'unique idéal maximal, $\mathfrak{M}$, est constitué des éléments non inversibles de A.

(17) Soit $\mathbb{K}$ un corps commutatif. On suppose l'existence d'une surjection v de $\mathbb{K}$ sur $\mathbb{Z} \cup \{+\infty\}$ telle que : $v(0) = +\infty$, $v(xy) = x(x) + v(y)$, $v(x+y) \geq \min(v(x), v(y))$, x et y étant des éléments quelconques de $\mathbb{K}$.

Vérifier que $v(1) = 0$ et que $v(x^{-1}) = -v(x)$. Montrer que l'anneau :

$$A = \{x \in K \,|\, v(x) \geq 0\}$$

est un anneau valué dont l'idéal maximal est :

$$\mathfrak{M} = \{x \in A \,|\, v(x) > 0\}$$

et dont l'ensemble des unités est :

$$U = \{x \in A \,|\, v(x) = 0\}.$$

Soit p un élément de A tel que $v(p) = 1$; montrer que tout élément x de A est équivalent à $p^{v(x)}$. Caractériser les idéaux de A.

(18) Construire le corps des fractions d'un anneau intègre en s'aidant de la construction de $\mathbb{Q}$ à partir de $\mathbb{Z}$.

(19) Soit A l'anneau des séries entières convergentes dans un voisinage de zéro et $\mathbb{K}$ son corps des fractions. Vérifier que A est un anneau valué de $\mathbb{K}$. Caractériser son idéal maximal $\mathfrak{M}$ et tous ses idéaux.

(20) Montrer qu'un idéal $\mathfrak{P}$ d'un anneau A est premier si et seulement si $A/\mathfrak{P}$ est intègre. Comparer $\mathfrak{P}$ et sa racine $r(\mathfrak{P})$.

(21) Montrer qu'un idéal maximal est premier et donner un idéal premier non maximal.

(22) Vérifier que $A_{\mathfrak{P}}$ est un anneau local. Préciser ses éléments non inversibles.

(23) Soit $\mathfrak{I}$ et $\mathfrak{K}$ deux idéaux d'un anneau A. Montrer que $A/(\mathfrak{I} + \mathfrak{K})$ est isomorphe à $(A/\mathfrak{I})/s(\mathfrak{K})$, s désignant la surjection canonique de A sur $(A/\mathfrak{I})$.

(24) Montrer qu'un anneau intègre fini est un corps.

(25) Considérons les deux structures d'anneau commutatif sur $\mathbb{Z}^2$, pour l'addition $(a,b) + (c,d) = (a+c, b+d)$ et pour le produit :

$$\begin{array}{rcl} (a,b).(c,d) & = & (ac, bd), \\ (a,b) \star (c,d) & = & (ac - bd, ad + bc). \end{array}$$

Notons A la première et B la seconde.

Quels sont les éléments idempotents de A et de B ?

Existe-t-il des morphismes entre ces deux anneaux ?

(26) Soit t un élément algébrique sur un corps $\mathbb{K}$ et P son polynôme minimal, de degré n. Montrer que $\mathbb{K}(t) = \mathbb{K}[t]$ et que $\mathbb{K}(t)$ est un espace vectoriel de dimension n sur $\mathbb{K}$. Réciproquement, montrer que si une extension $\mathbb{L}$ de $\mathbb{K}$ est un espace vectoriel de dimension finie sur $\mathbb{K}$, c'est une extension algébrique.

(27) Montrer qu'une extension algebrique $\mathbb{M}$ d'une extension algébrique $\mathbb{L}$ d'un corps $\mathbb{K}$ est une extension algebrique de $\mathbb{K}$.

5.8 Correction des exercices.

(1) Si un idéal contient un élément inversible x, il contient $x^{-1}x = 1$, et donc tous les éléments de l'anneau.

(2) Si A est un corps, son seul élément non inversible est 0 et son unique idéal propre est donc $\{0\}$. Si A n'est pas un corps, il possède au moins un élément non inversible $a \neq 0$, et l'ensemble des multiples de a, aA, est un idéal qui ne contient pas 1 ; c'est donc un idéal propre non nul.

(3) En caractéristique 4 on a l'anneau $\mathbb{Z}/4\mathbb{Z}$ dont l'unique idéal propre non nul est $\{0, 2\}$, maximal. Son polynôme annulateur est $X^4 + 2X^3 + 3X^2 + 2X$.

En caractéristique 2, partons des éléments de l'anneau : 0, 1, a, b ; chaque élément est son propre opposé, et $a+b$ ne peut être égal qu'à 1, $a+1$ à b, $b+1$ à a, donc $1+a+b=0$; a^2 est égal à l'un des quatre éléments ; on a évidemment :

$$a^2 + b^2 = (a+b)^2 = 1.$$

Si $a^2 = 0$, on a $b^2 = 1$ et :

$$ab = (b+1)b = b^2 + b = 1 + b = a.$$

L'unique idéal maximal de cet anneau non intègre ($a^2 = 0$) est $\{0, a\}$, et son polynôme annulateur est $X^4 + bX^2 + aX$.

Si $a^2 = 1$, les rôles de a et b sont échangés, et on retrouve l'anneau précédent.

Si $a^2 = a$, $b^2 = b$ et $ab = a(a+1) = a^2 + a = 0$; on obtient un anneau, non intègre ($ab = 0$), ayant deux idéaux maximaux : $\{0, a\}$ et $\{0, b\}$, et dont le polynôme annulateur est $X^4 + (a+b)X$.

Si $a^2 = b$, $b^2 = a$, on obtient le corps $\mathbb{F}_4$ dont on parlera dans le chapitre suivant.

(4) Soit $\mathfrak{I}$ un idéal propre non nul de $\mathbb{K}[X]$. les polynômes constants non nuls étant inversibles, $\mathfrak{I}$ ne peut en contenir aucun et l'ensemble des degrés de ses éléments non nuls est une partie de $\mathbb{N}^*$ qui possède à ce titre un plus petit élément, $d \geq 1$. Soit F un polynôme de degré d appartenant à $\mathfrak{I}$ et G un

élément quelconque de $\mathfrak{I}$; par division euclidienne, on obtient :

$$G = QF + R,\ \deg(R) < \deg(F).$$

Par définition d'un idéal, $R = G - QF$ appartient à $\mathfrak{I}$, or son degré est inférieur au minimum : R est donc nul, $G = QF$, et F est un générateur de $\mathfrak{I}$. Tout autre générateur sera un multiple de F de même degré, donc de la forme λF, $\lambda \in \mathbb{K}^*$, et si on impose à F d'avoir un coefficient dominant (celui du terme de plus haut degré) égal à 1, on obtient l'unicité.

(5) Supposons l'idéal $\mathfrak{I}$ engendré par l'un de ses éléments : $i = 2a + b\sqrt{2}$. Cette hypothèse signifie que pour un élément quelconque de $\mathfrak{I}$, $z = 2x + y\sqrt{2}$, il existe un élément de l'anneau $a = u + v\sqrt{2}$ tel que $z = ai$. Ceci donne :

$$u = \frac{ax - by}{2a^2 - b^2},\ v = \frac{-bx + 2ay}{2(2a^2 - b^2)},$$

ces nombres devant être entiers. En donnant à x et y les valeurs 1 et 0, on voit que a doit être divisible par $2a^2 - b^2$ et b par $2(2a^2 - b^2)$. En reportant dans $2a^2 - b^2$ on trouve que cette expression doit être multiple de 2 ; supposons-la multiple de 2^n : a et b le sont aussi et $2(2a^2 - b^2)$ est multiple de 2^{2n}... ces nombres tendent vers l'infini, ce qui est absurde.

(6) Un idéal $\mathfrak{I}$ étant un sous-groupe du groupe additif A, commutatif, le groupe quotient $A/\mathfrak{I}$ est bien défini ; il reste à voir ce qui se passe pour la multiplication.

Définissons le produit de deux classes, $x\mathfrak{I}$ et $y\mathfrak{I}$, comme étant la classe $xy\mathfrak{I}$ et vérifions que le résultat est indépendant du choix des éléments x et y représentant les classes. Si $x' = x + i$ et $y' = y + j$ remplacent respectivement x et y, i et j appartenant à $\mathfrak{I}$, la différence $x'y' - xy = (x + j)i + xj$ appartient à $\mathfrak{I}$ et $x'y'$ est dans la même classe que xy.

Il reste à voir la compatibilité des deux lois, c'est- à-dire la distributivité : elle est une conséquence immédiate de la distributivité dans A.

L'anneau $A/\mathfrak{I}$ est appelé **anneau quotient** de A par $\mathfrak{I}$.

(7) Soit $\psi : A \to B$ un morphisme d'anneaux, $\mathfrak{I}$ un idéal de B et :

$$\mathfrak{K} = \overset{-1}{\psi}(\mathfrak{I}) = \{a \in A \,|\, \psi(a) \in \mathfrak{I}\}.$$

Montrons que $\mathfrak{K}$ est un idéal de A. C'est évidemment un sous-groupe de A et il reste à montrer que si $a \in A$ et $k \in \mathfrak{K}$, alors $ak \in \mathfrak{K}$; or $\psi(ak)$, égal à $\psi(a)\psi(k)$, appartient à $\mathfrak{I}$, ce qui est la condition pour que ak appartienne à $\mathfrak{K}$.

Soit $\mathfrak{R}$ un idéal de A et $\psi(\mathfrak{R})$ son image par ψ. Si $\dot{x}, \dot{y} \in \psi(\mathfrak{R})$, ces éléments sont images d'éléments x et y de $\mathfrak{R}$, et :

$$\dot{x} + \dot{y} = \psi(x) + \psi(y) = \psi(x + y) \in \psi(\mathfrak{R})\ ;$$

$\psi(\mathfrak{R})$ est donc un groupe, visiblement commutatif. Pour que ce soit un idéal, il reste à voir s'il est stable pour la multiplication par les éléments de B :

$$\dot{x} \in \psi(\mathfrak{R}),\ b \in B \Rightarrow b\dot{x} \in \psi(\mathfrak{R})\ ?$$

Il faut pour cela que $b\dot{x}$ soit l'image par ψ d'un élément de A ; condition remplie si ψ est surjectif.

(8) Soit A un anneau principal, $\mathfrak{I}$ un de ses idéaux, et π la surjection canonique (le passage aux classes d'équivalence) de A sur $B = A/\mathfrak{I}$ (exercice 6). L'anneau B est évidemment commutatif et intègre : si $\pi(a)\pi(b) = 0$, $\pi(ab) = 0$, et ab est dans $\mathfrak{I}$; l'un des deux éléments, par exemple a, est dans $\mathfrak{I}$ (l'idéal étant principal), et $\pi(a) = 0$.

L'image réciproque d'un idéal quelconque $\mathfrak{S}$ de $A/\mathfrak{I}$ est un idéal $\mathfrak{R}$ de A (exercice précédent) et $\pi(\mathfrak{R}) = \mathfrak{S}$. Par hypothèse, $\mathfrak{R}$ est de la forme Ar, pour un certain $r \in A$. On a alors :

$$\mathfrak{S} = \pi(Ar) = \pi(A)\pi(r) = B\pi(r)$$

et l'idéal $\mathfrak{S}$ est engendré par $\pi(r)$, donc monogène, et B est principal. Si $\pi(r) = 0$, r appartient à $\mathfrak{I}$ et $\mathfrak{S}$ est nul, et réciproquement. Si $\pi(r)$ est inversible, $\mathfrak{S}$ est égal à B et $\mathfrak{R}$ à A, et réciproquement.

(9) La surjection canonique $\psi : A \to A/\mathfrak{M}$ (le passage aux classes) est évidemment un morphisme d'anneaux. Si $\mathfrak{I}$ est un idéal propre de $A/\mathfrak{M}$, son image réciproque par ψ est un idéal de A contenant $\mathfrak{M}$ (puisque $\psi(\mathfrak{M}) = 0$), ce qui est absurde, $\mathfrak{M}$ étant maximal ; l'anneau $A/\mathfrak{M}$ n'ayant pas d'idéal propre non nul est un corps (exercice 2).

Réciproquement, si $A/\mathfrak{M}$ est un corps, soit $\mathfrak{I}$ un idéal de A contenant $\mathfrak{M}$, et supposons qu'il existe $x \in \mathfrak{I}$, $x \notin \mathfrak{M}$; alors $\psi(x)$, non nul, est inversible et il existe $y \in A$ tel que $\psi(x)\psi(y) = 1$; de $\psi(xy) = 1$ on déduit que $xy = 1 + m$, $m \in \mathfrak{M}$, et que $1 = xy - m$ appartient à $\mathfrak{I}$ (puisque $xy \in \mathfrak{I}$), qui est donc égal à A : $\mathfrak{M}$ est maximal.

(10) On note $\mathfrak{I} + \mathfrak{K}$ l'ensemble $\{x + y \in A \,|\, x \in \mathfrak{I},\, y \in \mathfrak{K}\}$ et $\mathfrak{I}\mathfrak{K}$ l'ensemble des éléments de A pouvant s'écrire comme somme finie de produits xy, $x \in \mathfrak{I}$, $y \in \mathfrak{K}$; les vérifications sont sans la moindre difficulté, comme pour l'intersection. La réunion n'est pas un idéal en général ; ainsi, dans l'anneau $\mathbb{Z}$, 4 appartient à l'idéal $4\mathbb{Z}$, 6 à l'idéal $6\mathbb{Z}$ mais leur somme 10 n'appartient pas à $4\mathbb{Z} \cup 6\mathbb{Z}$; le plus petit idéal contenant $4\mathbb{Z} \cup 6\mathbb{Z}$ est $2\mathbb{Z}$ car 2 est le pgcd de 4 et de 6.

Comme $\mathfrak{I}\mathfrak{K}$ est inclus dans $\mathfrak{I}$ et dans $\mathfrak{K}$, il est toujours inclus dans l'intersection.

La réciproque est vraie lorsque $\mathfrak{I}$ et $\mathfrak{K}$ sont étrangers ; choisissons un élément quelconque $x \in \mathfrak{I} \cap \mathfrak{K}$ et utilisons l'hypothèse pour écrire 1 sous la forme $a + b$; nous pouvons alors écrire : $x = (a + b)x = ax + bx$, avec ax et bx dans $\mathfrak{I}\mathfrak{K}$, et donc aussi x.

Si $\mathfrak{I}$ est maximal et ne contient pas $\mathfrak{K}$, $\mathfrak{I} + \mathfrak{K}$ est un idéal plus grand que $\mathfrak{I}$: c'est donc A.

Si deux idéaux de $\mathbb{Z}$, donc de la forme $p\,\mathbb{Z}$ et $q\,\mathbb{Z}$, sont étrangers, on peut écrire $1 = ap + bq$ et, d'après l'identité de Bézout (page 65), p et q sont premiers entre eux.

(11) Un rationnel x s'écrit sous la forme irréductible $s^{-1}r$; si $s \notin p\,\mathbb{Z}$, $x \in \mathbb{Z}_p$; si $s \in p\,\mathbb{Z}$, $r \notin p\,\mathbb{Z}$, $x^{-1} = r^{-1}s \in \mathbb{Z}_p$; $\mathbb{Z}_p$ est donc valué.

Si $p = 3$, on a :

$$\mathbb{Z}_3 = \Big\{ \frac{p}{q} \,|\, p, q \in \mathbb{Z}, q \notin 3\mathbb{Z} \Big\},$$

son corps des fractions est $\mathbb{Q}$, son unique idéal maximal est :

$$3\mathbb{Z}_3 = \Big\{ \frac{p}{q} \,|\, p \in 3\mathbb{Z}, q \notin 3\mathbb{Z} \Big\},$$

son corps résiduel $\mathbb{Z}_3/3\mathbb{Z}_3$, étant un corps à trois éléments, est isomorphe à $\mathbb{F}_3$. La classe de 0 contient les fractions de numérateur multiple de 3, la classe de 1 contient les fractions de la forme :

$$\frac{3m+1}{3n+1} \quad \text{ou} \quad \frac{3m+2}{3n+2},$$

la classe de 2 contient les fractions de la forme :

$$\frac{3m+2}{3n+1} \quad \text{ou} \quad \frac{3m+1}{3n+2}.$$

(12) Un élément $x = s^{-1}r$ de $\mathbb{Z}_p$ est inversible si ni r ni s ne sont divisibles par p ; U est évidemment un groupe ; on a $x\,\Re\,x$ car $1 \in U$, et $x\,\Re\,y \Rightarrow y\,\Re\,x$ car $u \in U \Rightarrow u^{-1} \in U$; la transitivité enfin découle du fait que si u et v sont dans U, uv y est aussi.

(13) Si le rationnel $x = s^{-1}r$ appartient à $\mathbb{Z}_p$, $s \notin p\,\mathbb{Z}$, $r = p^n t$, $n \geq 0$, $x = s^{-1}tp^n$ et $x \sim p^n$ car $s^{-1}t \in U$; si $x^{-1} = r^{-1}s$ appartient à $\mathbb{Z}_p$, on aura de même $x^{-1} \sim p^n$ et $x \sim p^{-n}$; $n = 0$ pour les éléments de U.

(14) Si, avec les notations précédentes, $x = up^n$, $y = vp^m$, $xy = uvp^{n+m}$, et $v_p(xy) = n + m$, ce qui prouve la première égalité.

Si $n > m$, $x + y = p^m(v + up^{n-m})$ et $v_p(x + y) = m$.

Si $n = m$, $x + y = p^n(u + v)$ et $v_p(xy) = n + v_p(u + v) \geq n$; si $y = -x$, $v_p(x + y) = +\infty$.

(15) L'ensemble des $v_p(x)$ lorsque x parcourt $\mathfrak{I}$ est une partie non vide de $\mathbb{N}^*$ (l'idéal ne pouvant contenir d'unités) et possède une borne inférieure $n \geq 1$. Soit $x \in \mathfrak{I}$ tel que $v_p(x) = n$; x s'écrit donc $x = p^n u$, $u \in U$; on en déduit, en multipliant par u^{-1}, que $p^n \in \mathfrak{I}$ et que $p^n\mathbb{Z}_p \subset \mathfrak{I}$; y étant un élément quelconque de $\mathfrak{I}$, $v_p(y) = n + d$, $d \geq 0$, et $y = p^{n+d}v$, $v \in U$; y appartient donc à $p^n\mathbb{Z}_p$ et $\mathfrak{I} \subset p^n\mathbb{Z}_p$, d'ou $\mathfrak{I} = p^n\mathbb{Z}_p$.

(16) Appelons U l'ensemble des éléments inversibles (unités) de A ; c'est un groupe multiplicatif. Il faut montrer que $\mathfrak{M} = A \setminus U$ est un idéal ; il sera alors maximal et unique. Montrons d'abord que si $a \in A$ et $x \in \mathfrak{M}$, alors $ax \in \mathfrak{M}$.

Supposons ax dans U : $ax = u \in U$, $u^{-1}ax = 1$, x est inversible, ce qui est absurde.

Pour deux éléments quelconques a et b de A^*, $b^{-1}a$ et $a^{-1}b$ existent dans $\mathbb{K}^*$ et l'un des deux est dans A^* par définition d'un anneau valué. Si x et y sont dans $\mathfrak{M}$ et si par exemple $x^{-1}y = a \in A^*$, $y = ax$ et la somme $x + y = x(1 + a)$ appartient à $\mathfrak{M}$ d'après ce qui précède. Enfin si $x \in \mathfrak{M}$, $-x \in \mathfrak{M}$ et $\mathfrak{M}$ est un idéal de A.

(17) De :

$$v(x) = v(1.x) = v(1) + v(x)$$

on tire que $v(1) = 0$; de :

$$0 = v(1) = v(x) + v(x^{-1})$$

on tire que $v(x^{-1}) = -v(x)$. On en déduit immédiatement que :

$$v(x) = 0 \Rightarrow v(x^{-1}) = 0$$

et que $x^{-1} \in A$; $v = 0$ est donc l'équation de U.

Soit $x \in \mathbb{K}$; si $v(x) \geq 0$, x est dans A ; si $v(x) < 0$, $v(x^{-1}) > 0$ et x est dans A ; A est donc un anneau valué.

L'élément -1 étant inversible, $v(x) = v(-x)$, et si $x \in \mathfrak{M}$, -x est aussi dans $\mathfrak{M}$; si $x \in \mathfrak{M}$ et $y \in \mathfrak{M}$, $v(x + y) \geq \min(v(x), v(y)) > 0$ et $x + y$ est dans $\mathfrak{M}$; $(\mathfrak{M}, +)$ est donc un groupe.

Si $a \in A$ et $x \in \mathfrak{M}$, alors $v(ax) = v(a) + v(x) \geq v(x) > 0$ et ax appartient à $\mathfrak{M}$, ce qui achève de prouver que $\mathfrak{M}$ est un idéal ; il est maximal car les autres éléments de A, étant inversibles car vérifiant $v = 0$, ne peuvent appartenir à un idéal propre.

Soit $x \in A$; si $v(x) = 0$, x est dans U et $x \sim 1 = x^{v(x)}$; si $v(x) = n > 0$, $v(xp^{-n}) = 0$, xp^{-n} est dans U, $x = p^n u$, avec $u \in U$, et $x \sim p^n = p^{v(x)}$.

Soit $\mathfrak{I}$ un idéal de A et n la valeur minimale que prend v sur $\mathfrak{I}$; soit $x \in \mathfrak{I}$ tel que $v(x) = n$; il existe donc $u \in U$ tel que $x = up^n$ et $p^n = xu^{-1}$ appartient à $\mathfrak{I}$; l'ensemble $p^n A$ des multiples de p^n est un idéal contenu dans $\mathfrak{I}$ et son équation est $v \geq n$.

Réciproquement, si $y \in \mathfrak{I}$, $v(y) = n' \geq n$, $v(yp^{-n}) \geq 0$, $yp^{-n} = a \in A$, et $y = ap^n \in Ap^n$. On a donc l'égalité $\mathfrak{I} = Ap^n$, ce qui donne la forme de tous les idéaux de A.

(18) Soit A un anneau intègre, $E = A \times A^*$ l'ensemble des couples muni de la relation d'équivalence :

$$(a, b) \sim (a', b') \iff ab' = ba'.$$

Notons $(a, b)^*$ la classe de (a, b) et F l'ensemble des classes. Munissons F d'une addition :

$$(a, b)^* + (c, d)^* = (ad + bc, bd)^*$$

en remarquant d'abord que bd ne peut être nul, l'anneau étant intègre, ensuite que le résultat ne change pas si l'on remplace, par exemple, (a, b) par un couple équivalent (a', b') ; on vérifie en effet sans peine que $(ad+bc, bd)$ est équivalent à $(a'd+b'c, b'd)$; le neutre est $(0, 1)^*$ et l'opposé de $(a, b)^*$ est $(-a, b)^*$. Munissons enfin F d'une multiplication :

$$(a, b)^*(c, d)^* = (ac, bd)^*$$

pour laquelle le neutre est $(1, 1)^*$ et l'inverse de $(a, b)^*$, si $a \neq 0$, est $(b, a)^*$; on vérifie sans peine que le résultat est indépendant du choix des représentants dans les classes et que les axiomes de corps sont respectés.

(19) Rappelons un exemple : la série entière $\sum_{n\geq 0} x^n$, lorsqu'elle converge, a pour somme $(1-x)^{-1}$; elle a donc pour inverse $1-x$.

Plus généralement, l'inverse de la série $1+\sum_{n\geq 1} a_n x^n$ est, si elle converge, la série $1+\sum_{n\geq 1} b_n x^n$, les b_i s'exprimant en fonction des a_i.

Un élément de A s'écrit $a_0 x^n(1+a_0^{-1}a_1 x+\cdots)$ avec $n \geq 0$ et $a_0 \neq 0$, et sa valuation est n ; son inverse est de la forme $a_0^{-1}x^{-n}(1+b_1 x+\cdots)$, de valuation $-n$ et il n'appartient à l'anneau que si son rayon de convergence n'est pas nul, c'est- à-dire si $n = 0$. Les éléments inversibles sont donc ceux de valuation nulle.

Soit $\mathfrak{I}$ un idéal propre non nul de A, n la valuation minimale de ses éléments et σ un élément de $\mathfrak{I}$ de valuation n :

$$\sigma = a_0 x^n + a_1 x^{n+1} + \cdots,\ a_0 \neq 0\ ;$$

n est supérieur ou égal à 1 car σ ne peut être inversible ; tout élément ξ de A de valuation m supérieure ou égale à n :

$$\xi = b_0 x^m + a_1 x^{m+1} + \cdots,\ b_0 \neq 0\ ;$$

appartient à $\mathfrak{I}$ car il est le produit de σ par un élément a de A, de valuation $m-n$:

$$a = x^{-n}(x^{-n}\sigma)^{-1}\xi = b_0 a_0^{-1} x^{m-n}(1+c_1 x+\cdots)\ ;$$

$\mathfrak{I}$ est donc l'ensemble des éléments de A de valuation supérieure ou égale à n. La réunion de tous les idéaux, ensemble des éléments de valuation supérieure ou égale à 1 est donc l'unique idéal maximal de A.

(20) Si $A/\mathfrak{P}$ n'est pas intègre il existe deux éléments non nuls $\dot{x}$ ($x \notin \mathfrak{P}$) et $\dot{y}$ ($y \notin \mathfrak{P}$) dont le produit $\dot{x}\dot{y}$ est nul : $xy \in \mathfrak{P}$, et $\mathfrak{P}$ n'est donc pas premier.

Supposons $A/\mathfrak{P}$ intègre et soient deux éléments x et y de A dont le produit est dans $\mathfrak{P}$: le produit de leurs classes est donc nul, et par intégrité l'une des classes est nulle, par exemple $\dot{x}$, et x appartient à $\mathfrak{P}$ qui est donc premier.

Si $x \in r(\mathfrak{P})$, il existe $n \in \mathbb{N}^*$ tel que $x^n \in \mathfrak{P}$; comme $x^n = x^{n-1}x$, ou bien $x \in \mathfrak{P}$ ou bien $x^{n-1} \in \mathfrak{P}$; on arrive toujours, par itération, à $x \in \mathfrak{P}$, ce qui montre que $r(\mathfrak{P}) = \mathfrak{P}$.

La réciproque est fausse : l'idéal $6\mathbb{Z}$ de $\mathbb{Z}$ est égal à sa racine sans être premier.

(21) Si $\mathfrak{M}$ est un idéal maximal de l'anneau A, $A/\mathfrak{P}$ est intègre car c'est un corps.

Soit A un anneau intègre qui n'est pas un corps ; $B = A \times A$ muni des lois :

$$(a, b) + (c, d) = (a + c, b + d),$$

$$(a, b) * (c, d) = (ac, bd),$$

est un anneau (qui ne peut être intègre car $(1, 0) * (0, 1) = (0, 0)$) dont $\{0\} \times A$ est un idéal premier, le quotient étant isomorphe à A, mais non maximal, A n'étant pas un corps ; les idéaux maximaux de B sont de la forme $A \times \mathfrak{M}$ et $\mathfrak{M} \times A$, $\mathfrak{M}$ étant un idéal maximal de A.

(22) Les éléments non inversibles de $A_{\mathfrak{P}}$ s'écrivent ab^{-1} avec $a \in \mathfrak{P}$; leur ensemble $\mathfrak{P}A_{\mathfrak{P}}$ forme un idéal maximal, donc unique, et $A_{\mathfrak{P}}$ est un anneau local.

(23) Notons d'abord que $s(\mathfrak{K})$ est un idéal de $A/\mathfrak{I}$ car s est une surjection (exercice 7) ; $(A/\mathfrak{I}) \,/\, s(\mathfrak{K})$ est donc un anneau-quotient ; soit :

$$\sigma : A/\mathfrak{I} \to (A/\mathfrak{I}) \,/\, s(\mathfrak{K})$$

la surjection canonique. Le morphisme :

$$p = \sigma \circ s : A \to (A/\mathfrak{I}) \,/\, s(\mathfrak{K})$$

est évidemment surjectif ; on déduit des équivalences :

$$a \in \mathrm{Ker}(p) \iff \sigma(s(a)) = 0 \iff s(a) \in s(\mathfrak{K}) \iff a \in (\mathfrak{I} + \mathfrak{K})$$

que $(A/\mathfrak{I}) \,/\, s(\mathfrak{K})$, isomorphe à $A/\mathrm{Ker}(p)$, est isomorphe à $A \,/\, (\mathfrak{I}+\mathfrak{K})$. L'image réciproque de $s(\mathfrak{K})$ est en effet égale à $\{\, a \in A \mid s(a) \in s(\mathfrak{K}) \,\}$, donc à $\mathfrak{K}+\mathrm{Ker}(s) = \mathfrak{I} + \mathfrak{K}$.

(24) L'application $\alpha : x \mapsto ax$, avec $a \in A^*$, est un morphisme de l'anneau A, dont le noyau est nul par hypothèse (A est intègre) ; A et $\mathrm{Im}(\alpha)$ ont donc même cardinal : α est bijective, et $\alpha^{-1}(1)$ est l'inverse de a ; tout élément non nul étant inversible, A est un corps.

(25) Les idempotents de A sont $(1, 0)$, $(0, 1)$ et les neutres $(0, 0)$ et $(1, 1)$. Ceux de B sont les neutres $(0, 0)$ et $(1, 0)$ (le carré de $(0, 1)$ est $(-1, 0)$).

Si $\phi : A \to B$ est un morphisme d'anneaux, on doit avoir $\phi((1, 1)) = (1, 0)$ (les neutres) et $\phi((1, 0)) = (1, 0)$ ou $(0, 0)$. Si $\phi((1, 0)) = (1, 0)$, on doit avoir :

$$\phi((0, 1)) = \phi((1, 1)) - \phi((1, 0)) = 0,$$

et si $\phi((1, 0)) = (0, 0)$, $\phi((0, 1)) = (-1, 0)$, ce qui est impossible, $(-1, 0)$ n'étant pas idempotent. On a finalement $\phi((a, b)) = (a, 0)$.

Si $\psi : B \to A$ est un morphisme d'anneaux, on doit avoir $\psi((1, 0)) = (1, 1)$ (les neutres). Si $\psi((0, 1)) = (a, b)$, le carré de $(0, 1)$ étant $(-1, 0)$, on doit avoir

$\psi(-1,0) = (-1,-1) = (a^2, b^2)$, or -1 n'est pas un carré dans $\mathbb{Z}$. Il n'y a donc pas de morphisme de B vers A.

(26) On désigne par $\mathbb{K}[t]$ l'ensemble de combinaisons linéaires de puissances de t à coefficients dans $\mathbb{K}$, et par $\mathbb{K}(t)$ le corps des fractions de $\mathbb{K}[t]$; or $\mathbb{K}[t]$ est isomorphe à $\mathbb{K}[X]/(P)$: c'est donc un corps, (P) étant un idéal maximal. Il est donc égal à son corps des fractions.

Le monôme t^n, étant combinaison linéaire des t^i, $0 \leq i \leq n-1$, appartient à $\mathrm{vect}(1, t, \ldots, t^{n-1})$; une récurrence simple montre qu'il en est de même pour les puissances supérieures ; les t^i, $0 \leq i \leq n-1$, sont libres, car une relation de dépendance linéaire entre eux donnerait un polynôme ayant pour racine t et de degré inférieur à celui du polynôme minimal. Ceci prouve que $\mathbb{K}(t)$ est un espace vectoriel de dimension n sur $\mathbb{K}$.

Soit $\mathbb{L}$ une extension de degré fini, m, de $\mathbb{K}$, et $t \in \mathbb{L}$, $t \notin \mathbb{K}$; les monômes t^k sont liés, sinon l'espace vectoriel $\mathbb{L}$, de dimension finie, aurait un sous-espace, engendré par les t^k, de dimension infinie. Cet élément t est donc algébrique sur $\mathbb{K}$, et $\mathbb{L}$ est une extension algébrique. Il n'y a pas de réciproque : la clôture algébrique de $\mathbb{F}_2$, $\overline{\mathbb{F}}_2$, nous le verrons plus loin, est une extension algébrique de degré infini de $\mathbb{F}_2$; $\overline{\mathbb{F}}_2$ est la réunion de toutes les extensions algébriques de degré fini de $\mathbb{F}_2$.

(27) Soit $t \in \mathbb{M} \setminus \mathbb{L}$, verifiant la relation :

$$t^n + a_{n-1}t^{n-1} + \cdots + a_0 = 0,\ a_i \in \mathbb{L},\ a_0 \neq 0,$$

donc algébrique sur $\mathbb{K}[a_0, \ldots, a_{n-1}]$, qui est une extension de degré fini (donc algébrique, exercice 25) sur $\mathbb{K}$. En effet, si a_i est de degré n_i sur $\mathbb{K}$, les produits $a_0^{k_1} \ldots a_{n-1}^{k_{n-1}}$, $0 \leq k_i \leq n_i$, en nombre fini, forment une base de $\mathbb{K}[a_0, \ldots, a_{n-1}]$ sur $\mathbb{K}$. Alors, les produits $a_0^{k_1} \ldots a_{n-1}^{k_{n-1}} t^k$, $0 \leq k < n$, forment une base (finie) de $\mathbb{K}[a_0, \ldots, a_{n-1}][t]$ sur $\mathbb{K}$. Ce corps est donc une extension algébrique de $\mathbb{K}$, et t est algébrique sur $\mathbb{K}$. Chaque élément de $\mathbb{M}$ étant algébrique sur $\mathbb{K}$, $\mathbb{M}$ est une extension algébrique de $\mathbb{K}$.

6 Corps de caractéristique finie

Un corps de caractéristique finie peut être infini, comme la clôture algébrique de $\mathbb{F}_2$ que nous construirons plus loin (5.5), mais rappelons que tout corps fini est commutatif et que son groupe multiplicatif est cyclique (théorème 4.3 de Wedderburn).

Soit $\mathbb{K}$ un corps : il est muni de deux opérations, l'une notée additivement, l'autre multiplicativement, par une croix, ou un point, ou si cela n'introduit pas de confusion, sans aucun symbole, pour alléger l'écriture. Les éléments neutres de ces opérations sont notés respectivement 0_K et 1_K, ou 0 et 1 s'il n'y a pas de confusion possible, et $\mathbb{K}^*$ désigne l'ensemble des éléments non nuls, donc inversibles, de $\mathbb{K}$.

Notons $(\mathbb{K}, +)$ l'ensemble des éléments de $\mathbb{K}$ muni de la seule addition : c'est par définition un groupe commutatif ; $\mathbb{K}^*$ est un groupe pour la multiplication, cyclique, donc commutatif, si $\mathbb{K}$ est fini.

Le groupe $(\mathbb{Z}, +)$ opère naturellement sur $\mathbb{K}$: $1.z = z$, $(a + b).z = a.z + b.z$. Si $n.1_K \neq 0_K$ pour tout $n \in \mathbb{Z}$, $\mathbb{K}$ contient un sous-anneau isomorphe à $\mathbb{Z}$, et il est de caractéristique 0, et infini.

Si l'ensemble des $n \in \mathbb{Z}$ tels que $n.1_K = 0_K$ n'est pas vide, c'est évidemment un sous-groupe de $\mathbb{Z}$. Il est donc de la forme $p\mathbb{Z}$, et $\mathbb{K}$ contient un sous-anneau isomorphe à $\mathbb{Z}/p\mathbb{Z}$, dont les éléments non nuls doivent être inversibles, ce qui impose que p soit premier ; $\mathbb{K}$ contient donc un sous-corps que l'on identifie, à isomorphisme près, à $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Si $\mathbb{K}$ est fini, donc commutatif, il existe par conséquent un nombre premier p tel que $p.1_K = 0_K$, ce qui implique que, $\forall z \in \mathbb{K}$, $p.z = p.(1.z) = 0_K$. Le corps est de caractéristique p.

Les corps $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont de caractéristique nulle ; $\mathbb{Z}/4\mathbb{Z}$ est un anneau de caractéristique 4 ; $\mathbb{Z}/5\mathbb{Z}$ est un corps de caractéristique 5 .

Proposition 6.1. *Si $\mathbb{K}$ est un corps fini, de caractéristique p, c'est un espace vectoriel sur son sous-corps $\mathbb{F}_p$, et il a donc p^m éléments, $m \geq 1$.*

Démonstration. Le produit $\mathbb{F}_p \times \mathbb{K} \to \mathbb{K}$ est bien défini, puisque $\mathbb{F}_p \subset \mathbb{K}$. Si $\mathbb{K}$ est de dimension m sur $\mathbb{F}_p$, il a p^m éléments. □

Proposition 6.2. *Deux corps à p^m éléments sont isomorphes.*

Démonstration. Soient $\mathbb{K}_1$ et $\mathbb{K}_2$ deux corps ayant p^m éléments. Les groupes $\mathbb{K}_1^*$ et $\mathbb{K}_2^*$ sont respectivement engendrés par α_1 et α_2. L'application $\phi(\alpha_1) = \alpha_2$ compatible avec les structures de corps est un isomorphisme de corps. □

Un corps à p^m éléments est noté $\mathbb{F}_{p^m}$, à isomorphisme près.

Théorème 6.1. *Les éléments de $\mathbb{F}_{p^m}$ sont les racines du polynôme $X^{p^m} - X$, et ses éléments non nuls sont les racines du polynôme $X^{p^m-1} - 1$.*

Démonstration. Les éléments non nuls de $\mathbb{F}_n$, $n = p^m$, sont les puissances d'un certain élément α tel que $\alpha^{n-1} = 1$. Quel que soit l'entier r, on a $(\alpha^r)^{n-1} = (\alpha^{n-1})^r = 1$. Les $n-1$ éléments de $\mathbb{F}_n^*$ sont donc les $n-1$ racines de $X^{n-1} - 1$, et, en ajoutant le 0, on obtient les racines de $X^n - X$. □

Théorème 6.2. *Dans une algèbre commutative A sur un corps commutatif $\mathbb{K}$, de caractéristique p, on a la formule du binôme :*

$$(x+y)^{p^n} = x^{p^n} + y^{p^n}$$

quels que soient les éléments x et y de A (ou de $\mathbb{K}$ qui est une algèbre sur lui-même) et l'entier naturel n.

Démonstration. Les coefficients du binôme :

$$\binom{p}{k} = \frac{p\,!}{k!\,(p-k)} = p\,\frac{(p-1)!}{k!\,(p-k)!}$$

étant congrus à 0 modulo p pour $1 \leq k \leq p-1$, il ne reste, dans la formule du binôme classique, que :

$$(x+y)^p = x^p + y^p$$

ce qui donne le résultat pour $n = 1$. Une récurrence sur n permet de conclure, car :

$$(x+y)^{p^n} = [(x+y)^{p^{n-1}}]^p$$

Si p n'est pas premier (cas d'un anneau) la propriété n'est pas conservée ; ainsi dans $\mathbb{Z}/4\mathbb{Z}$ on a :

$$(x+y)^4 = x^4 + 2x^2\,y^2 + y^4.$$ □

Si $\mathbb{K}$ est un corps de caractéristique p, il contient comme nous venons de le voir un sous-corps isomorphe au corps $\mathbb{F}_p = \mathbb{Z}/p\,\mathbb{Z}$. Par abus de langage, nous dirons que $\mathbb{F}_p$ est un sous-corps de $\mathbb{K}$, ou que $\mathbb{K}$ est une extension de $\mathbb{F}_p$. Le corps $\mathbb{K}$ est un espace vectoriel sur $\mathbb{F}_p$, de dimension m s'il est fini ; le nombre de ses éléments, son cardinal, est alors égal à p^m.

Nous verrons un peu plus loin que tous les corps à p^m éléments sont isomorphes, ce qui permet de les noter tous $\mathbb{F}_{p^m}$, à isomorphisme près.

Si $\mathbb{K} = \mathbb{F}_{p^m}$ et si $n = 2^m - 1$, nous savons qu'il existe, le groupe $\mathbb{K}^*$ étant cyclique, $\alpha \in \mathbb{K}^*$ tel que :

$$\mathbb{K}^* = \{\alpha,\ \alpha^2, \ldots,\ \alpha^{n-1},\ \alpha^n = 1\}\,,$$

Comme $\alpha^n = 1$, quel que soit r, $1 \leq r \leq n$, $(\alpha^r)^n = (\alpha^n)^r = 1$, et les éléments de $\mathbb{K}^*$ sont les racines du polynôme $X^n - 1$ et ceux de $\mathbb{K}$, les racines de $X^{n+1} - X$. Ces deux polynômes sont dans $\mathbb{F}_p[X]$, c'est- à-dire à coefficients dans $\mathbb{F}_p$. Une racine qui engendre toutes les autres, telle α ci-dessus, est dite **racine primitive**, ou **élément primitif**. La somme des racines de $X^n - 1$ étant nulle

(comme coefficient de X^{n-1}, d'après les relations entre les coefficients et les racines d'un polynôme) on a :

$$1 + \alpha + \alpha^2 + \cdots + \alpha^{n-1} = 0\,.$$

On peut aussi remarquer que :

$$X^n - 1 = (X-1)\,(1 + X + X^2 + \cdots + X^{n-1})\,.$$

Si r est un entier premier avec n, $\beta = \alpha^r$ est aussi racine primitive ; il existe en effet des entiers u et v tels que $un + vr = 1$ (identité de Bézout, page 65), ce qui donne :

$$\alpha = \alpha^{un+vr} = (\alpha^n)^u\,(\alpha^r)^v = \beta^v,$$

et le groupe engendré par β contient α ; comme le groupe engendré par α contient β, ces deux groupes sont bien confondus.

6.1 Automorphisme de Frobenius

Soit $\mathbb{K}$ un corps fini de caractéristique p. L'application :

$$\begin{array}{rccc} \phi : & \mathbb{K} & \to & \mathbb{K} \\ & x & \mapsto & x^p \end{array}$$

est injective, et donc surjective à cause de la finitude. Elle vérifie, pour tous éléments x et y, les conditions :

$$\begin{cases} \phi(xy) & = \phi(x)\,\phi(y), \\ \phi(x+y) & = \phi(x) + \phi(y), \end{cases}$$

la dernière découlant du théorème 5.2. Cette application est donc un automorphisme de corps pour $\mathbb{K}$, appelé **automorphisme de Frobenius**, très utile et dont il sera fait grand usage.

Un élément x de $\mathbb{K}$ est **invariant** par un morphisme u si $u(x) = x$.

Théorème 6.3. *Les éléments invariants par l'Automorphisme de Frobenius ϕ de $\mathbb{F}_{p^m}$ sont les éléments de son sous-corps $\mathbb{F}_p$.*

Démonstration. Les éléments de $\mathbb{F}_{p^m}$ invariants par ϕ sont les racines du plynôme $X^p - X$ dans $\mathbb{F}_{p^m}$, c'est- à-dire les éléments de son sous-corps $\mathbb{F}_p$. Plus précisément, si α est élément primitif de $\mathbb{F}_{p^m}$, posons :

$$\beta = \alpha^{1+p+p^2+\cdots+p^{m-1}}\,.$$

On a alors :

$$\beta^p = \alpha^{p+p^2+\cdots+p^m} = \beta$$

car $\alpha^{p^m} = \alpha$. Les puissances de β de 1 à $p-1$ ainsi que 0 sont les solutions du problème. □

6.2 Construction des corps de caractéristique 2

Les corps de caractéristique 2 sont les plus utilisés, ne serait-ce que pour des raisons informatiques évidentes, les ordinateurs calculant en mode binaire. Ils sont utilisés dans toutes les techniques de codage. Nous ne considérerons qu'eux dans la suite, et allons étudier leur construction sur quelques exemples.

Un corps est de caractéristique 2 si pour tout élément x on a $x + x = 0$, ou encore $x = -x$. Les signes $+$ et $-$ ont la même signification. Nous utiliseront donc le signe $+$.

Si ce corps est fini, il possède 2^m éléments, dont $n = 2^m - 1$ sont différents de 0, et sont les puissances d'un même élément primitif α.

Remarquons que si α est un élément primitif, il en va de même pour ses itérés par l'Automorphisme de Frobenius, car 2 est premier avec n.

Construction de $\mathbb{F}_2$. Le corps de départ ($m = 1$) est $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$, le corps trivial réduit à ses éléments neutres 0 et 1, racines du polynôme $X^2 + X$.

Construction de $\mathbb{F}_4$. Considérons dans $\mathbb{F}_2[X]$ le polynôme :

$$X^3 + 1 = (X + 1)(X^2 + X + 1).$$

Le second facteur n'a pas de racine dans $\mathbb{F}_2$ (comme -1 dans $\mathbb{R}$), ce qui mène à considérer une extension de $\mathbb{F}_2$, $\mathbb{F}_2(\alpha)$, α étant une racine de X^2+X+1, vérifiant donc $\alpha^2 = \alpha + 1$, $\alpha^3 = 1$, $\alpha^4 = \alpha$ ... L'inverse de α est α^2, noté aussi $\overline{\alpha}$. Le corps $\mathbb{F}_2(\alpha)$ possède quatre éléments : 0, 1, α et $\overline{\alpha}$, et on le note $\mathbb{F}_4$.

On dit que $X^2 + X + 1$ est le **polynôme minimal** de α : tout polynôme de $\mathbb{K}[X]$, $\mathbb{K}$ étant une extension finie de $\mathbb{F}_2$, admettant α pour racine est multiple de ce polynôme ; α est algébrique sur $\mathbb{F}_2$, et $\mathbb{F}_4$ est le **corps de décomposition** de $X^2 + X + 1$, c'est- à-dire le plus petit corps dans lequel ce polynôme se factorise complètement (se scinde) :

$$X^2 + X + 1 = (X + \alpha)(X + \overline{\alpha}),$$

les deux racines étant primitives. Les tables d'addition et de multiplication sont obtenues sans calcul. Le corps $\mathbb{F}_4$ est une extension algébrique de $\mathbb{F}_2$.

C'est aussi un espace vectoriel de dimension 2 sur $\mathbb{F}_2$. On peut ainsi noter $0 = (0, 0)$, $1 = (1, 0)$, $\alpha = (0, 1)$, ces deux derniers éléments formant une base, et $\alpha^2 = (1, 1)$.

Les éléments de $\mathbb{F}_4$ sont les quatre racines du polynôme $X^4 + X$ de $\mathbb{F}_2[X]$.

Généralisation. Partons du polynôme de $\mathbb{F}_2[X]$:

$$X^n + 1 = (X + 1)(X^{n-1} + \cdots + X + 1)$$

où $n = 2^m - 1$, et posons $\mathbb{F}_{2^m} = \mathbb{F}_2(\alpha)$, α étant une racine $n^{\text{ième}}$ de l'unité ($\alpha^n = 1$) primitiuve (c'est- à-dire dont les puissances 2, 3,..., $n - 1$ sont toutes

les autres racines $n^{\text{ièmes}}$ de l'unité). Les éléments de $\mathbb{F}_{2^m}$ sont donc 0, 1, α, α^2,..., α^{n-1} ; $\mathbb{F}_{2^m}^*$ est le groupe cyclique d'ordre n engendré par α.

La table de multiplication est évidente. Celle d'addition est calculée à partir d'une relation liant certaines puissances de α, que l'on détermine pour chaque valeur de m en factorisant le polynôme $X^n + 1$ dans $\mathbb{F}_2$, chaque facteur étant appelé **polynôme cyclotomique**.

Comment construit-on ces polynômes cyclotomiques ? On commence par partitionner l'ensemble des éléments de $\mathbb{F}_{2^m}^*$ en sous-ensembles cyclotomiques globalement invariants par l'automorphisme de Frobenius, E_i. On associe à chaque E_i le polynôme P_i dont les racines sont les éléments de E_i en utilisant les relations entre les coefficients et les racines. Ces coefficients, fonctions symétriques des racines, sont évidemment invariants par ϕ, et appartiennent donc à $\mathbb{F}_2$. Les P_i sont les polynômes cyclotomiques.

Construction de $\mathbb{F}_8$. Pour $m = 3$, $\mathbb{F}_8 = \{0,\ 1,\ \alpha, \ldots,\ \alpha^6\}$, α désignant un élément primitif ($\alpha^7 = 1$). Formons les sous-ensembles invariants par ϕ, l'automorphisme de Frobenius, d'éléments non nuls :

$$\begin{array}{rcl} E_0 & = & \{1\}, \\ E_1 & = & \{\alpha,\ \alpha^2,\ \alpha^4\}, \\ E_2 & = & \{\alpha^3,\ \alpha^6,\ \alpha^{12} = \alpha^5\}, \end{array}$$

d'où $P_0 = X + 1$, puis :

$$\begin{array}{rcl} P_1 & = & (X + \alpha)\,(X + \alpha^2)\,(X + \alpha^4) \\ & = & X^3 + sX^2 + tX + p, \end{array}$$

avec :

$$\begin{array}{rcl} s & = & \alpha + \alpha^2 + \alpha^4, \\ t & = & \alpha^3 + \alpha^5 + \alpha^6, \\ p & = & 1. \end{array}$$

Utilisons l'automorphisme de Frobenius :

$$s = (I + \phi + \phi^2)(\alpha),$$

puis :

$$(I + \phi)(s) = (I + \phi^3)(\alpha)\ ;$$

comme $\phi^3 = I$, s est dans le noyau de $(I + \phi)$, c'est- à-dire dans $\mathbb{F}_2$. Choisissons d'abord $s = 0$. De même :

$$t = (I + \phi + \phi^2)(\alpha^3),$$

et il faut prendre $t = 1$ car $s + t + 1 = 0$. D'où :

$$P_1 = X^3 + X + 1.$$

On trouve avec la même méthode :

$$P_2 = X^3 + X^2 + 1,$$

qui correspond au choix $s = 1$, $t = 0$, d'où la factorisation :

$$\begin{aligned} X^7 + 1 &= P_0\, P_1\, P_2 \\ &= (X+1)\,(X^3 + X + 1)\,(X^3 + X^2 + 1). \end{aligned}$$

Prenant pour élément primitif α une racine de P_1, on a : $\alpha^3 = \alpha + 1$. La table de multiplication est évidente, et celle d'addition est obtenue à partir de la relation précédente ; $\mathbb{F}_8$ étant un espace vectoriel de dimension 3 sur $\mathbb{F}_2$, on écrit :

$$1 = (1,0,0)\,,\ \alpha = (0,1,0)\,,\ \alpha^2 = (0,0,1)$$

d'où :

$$\begin{array}{rcrl} \alpha^3 &=& 1+\alpha & = (1,1,0)\,, \\ \alpha^4 &=& \alpha+\alpha^2 & = (0,1,1)\,, \\ \alpha^5 &=& \alpha^2+\alpha^3 & = (1\ 1\ 1)\,, \\ \alpha^6 &=& \alpha^3+\alpha^4 & = (1,0,1)\,, \end{array}$$

et $\alpha^7 = 1$, ce qui permet toutes les additions, le résultat pouvant être mis sous forme d'une puissance de α. Ainsi :

$$\alpha^3 + \alpha^5 = (1,1,0) + (1,1,1) = (0,0,1) = \alpha^2.$$

Si nous choisissons le troisième facteur, P_2, l'élément primitif β vérifie la relation $\beta^3 = \beta^2 + 1$, et nous obtenons la même structure, avec $\beta = \alpha^3$. Remarquons en effet que 7 étant premier, les puissances de α, à l'exception de 1, sont racines primitives, et la racine primitive α^3 est racine de P_2 :

$$P_2(\alpha^3) = \alpha^9 + \alpha^6 + 1 = \alpha^2 + \alpha^6 + 1 = (\alpha^3 + \alpha + 1)^2 = 0$$

ce qui permet de choisir β au lieu de α.

Le corps $\mathbb{F}_2(X)$ des fractions rationnelles à une indéterminée et à coefficients dans $\mathbb{F}_2$ est un exemple de corps infini de caractéristique 2. C'est une extension transcendante de $\mathbb{F}_2$, dans laquelle le « Frobenius » est un morphisme injectif, mais non surjectif (x n'a pas d'antécédent). Ce n'est plus un automorphisme.

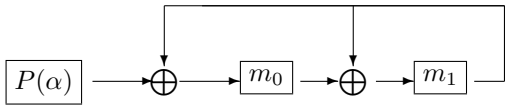
6.3 Calcul automatisé dans $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$

On utilise des registres à décalage simple :

ou circulaire :

et les opérateurs à deux entrées (et une sortie) $\bigoplus$ et $\bigotimes$. Le premier sort 0 pour $(0,0)$ ou $(1,1)$ et 1 pour $(1,0)$ ou $(0,1)$. Le second sort 0 pour $(0,0)$, $(1,0)$ ou $(0,1)$, 1 pour $(1,1)$. Voici quelques exemples.

Calcul de $P(\alpha)$ dans la base $(1,\alpha)$:



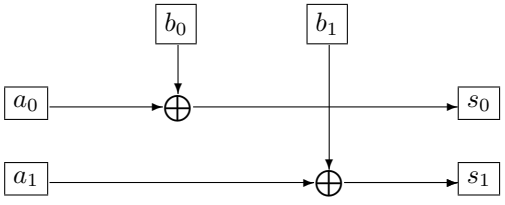
On entre $P(\alpha)$ selon les puissances décroissantes de α. Après la dernière entrée, le résultat est $m_0 + m_1\,\alpha$.

Appliquons à $P(\alpha) = \alpha^4 + 1$. Après deux entrées, les mémoires sont à $(0,1)$ (1, coefficient de α^4, 0, coefficient de α^3).

On entre le coefficient de α^2, 0 : m_0 passe à 0 plus la valeur précédente de m_1, 1, m_1 est égal à la valeur précédente de m_0 plus celle de m_1, soit 1. Les mémoires sont à $(1,1)$.

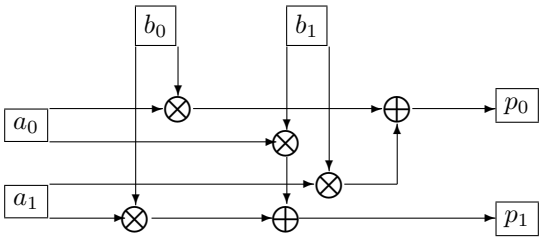
L'entrée du coefficient de α, 0, les fait passer à $(1,0)$, puis celle du terme constant, 1, à $(1,1)$: le résultat est $1 + \alpha$.

Calcul de la somme de deux nombres :



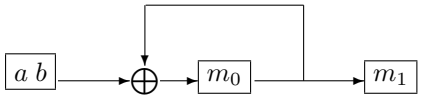
$$(a_0 + a_1\alpha) + (b_0 + b_1\alpha) = s_0 + s_1\alpha.$$

et de leur produit :



$$(a_0 + a_1\alpha) * (b_0 + b_1\alpha + b_2\overline{\alpha}) = p_0 + p_1\alpha.$$

Calcul de l'inverse de $a + b\,\alpha \neq 0$:



$$(a + b\,\alpha)^{-1} = m_0 + m_1\,\alpha$$

Les mémoires m_0 et m_1, initialisées à $(0, 0)$, contiennent successivement $(a, 0)$ et $(a + b, b)$, qui est le résultat $(a + b + a\,\alpha)$.

Pour diviser, on multiplie par l'inverse.

6.4 Ordre filtrant

Le corps $\mathbb{K} = \mathbb{F}_{2^h}$ est un sous-corps de $\mathbb{L} = \mathbb{F}_{2^k}$ si et seulement si 2^k est une puissance de 2^h, c'est- à-dire si h divise k ($k = nh$).

La plus petite extension commune à $\mathbb{F}_4$ et $\mathbb{F}_8$, le plus petit corps les contenant, est $\mathbb{F}_{64}$. Si α est élément primitif de $\mathbb{F}_{64}$, $\mathbb{F}_4$ peut être identifié au sous-corps $\{0, 1, \alpha^{21}, \alpha^{42}\}$ et $\mathbb{F}_8$ au sous-corps d'élément primitif α^9.

Un $\mathbb{K}$-**automorphisme** de $\mathbb{L}$ est un automorphisme de $\mathbb{L}$ dont la restriction à son sous-corps $\mathbb{K}$ est l'identité.

Si d et m sont respectivement le pgcd et le ppcm des entiers naturels a et b, on peut définir les opérations d'intersection :

$$\mathbb{F}_{2^a} \wedge \mathbb{F}_{2^b} = \mathbb{F}_{2^d}$$

et d'union :

$$\mathbb{F}_{2^a} \vee \mathbb{F}_{2^b} = \mathbb{F}_{2^m}$$

et la relation d'ordre :

$$\mathbb{F}_{2^a} \geq \mathbb{F}_{2^b} \iff b|a\,,$$

$b|a$ signifiant que b divise a. Cette dernière relation définit un **ordre filtrant** croissant : l'union $\mathbb{F}_{2^a} \vee \mathbb{F}_{2^b}$ est plus grande que chacun des deux corps $\mathbb{F}_{2^a}$ et $\mathbb{F}_{2^b}$, et un ordre filtrant décroissant : l'intersection $\mathbb{F}_{2^a} \wedge \mathbb{F}_{2^b}$ est plus petite que chacun des deux. Aucun des deux n'est un ordre total puisque, par exemple, $\mathbb{F}_4$ et $\mathbb{F}_8$ ne sont pas comparables, mais sont tous les deux plus grands que $\mathbb{F}_2$ et plus petits que $\mathbb{F}_{64}$.

6.5 La clôture algébrique $\overline{\mathbb{F}}_2$

Un corps $\mathbb{K}$ est algébriquement clos si tout polynôme de $\mathbb{K}[X]$ possède une racine dans $\mathbb{K}$; il est alors décomposable en produit de polynômes de degré 1. Tout corps est sous-corps d'un corps algébriquement clos, appelé sa clôture algébrique (théorème de Steinitz).

Un corps $\mathbb{F}_{2^m}$ n'est jamais algébriquement clos car, par exemple, le polynôme $X^{2^m+1}+1$ possède 2^m+1 racines simples (une racine multiple serait commune au polynôme et au polynôme dérivé X^{2^m}, ce qui est impossible) dans un corps algébriquement clos, plus nombreuses que les éléments de $\mathbb{F}_{2^m}$.

Soit $\overline{\mathbb{F}}_2$ la réunion de tous les corps $\mathbb{F}_{2^m}$.

Théorème 6.4. *L'ensemble $\overline{\mathbb{F}}_2$ est un corps commutatif, de caractéristique 2, infini et algébriquement clos : c'est la clôture algébrique commune de tous les $\mathbb{F}_{2^m}$.*

Démonstration. Soient deux éléments, x et y, de $\overline{\mathbb{F}}_2$. Si $x \in \mathbb{F}_{2^m}$ et $y \in \mathbb{F}_{2^n}$, on calcule leur somme et leur produit dans $\mathbb{F}_{2^m} \vee \mathbb{F}_{2^n}$; $\overline{\mathbb{F}}_2$ est un donc un corps commutatif, de caractéristique 2 et évidemment infini.

Soit $P \in \overline{\mathbb{F}}_2[X]$. En fait, $P \in \mathbb{F}_{2^h}[X]$ pour un certain h, et, si ses racines ne sont pas toutes dans $\mathbb{F}_{2^h}$, elles engendrent une extension algébrique, corps fini de caratéristique 2, donc de la forme $\mathbb{F}_{2^k}$. Les racines de P étant dans $\overline{\mathbb{F}}_2$, ce corps est algébriquement clos. □

6.6 Racines de l'unité

Soit n est un entier naturel impair et :

$$\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$$

le passage aux classes modulo n. Les puissances de 2 étant premières avec n, les $\pi(2^k)$ ne sont jamais nuls. L'espace d'arrivée étant de cardinal fini, n, il existe des couples (h, k) d'entiers naturels, $h < k$, tels que $\pi(2^h) = \pi(2^k)$. On a alors :

$$\pi(2^{k-h}) \equiv 1 \bmod n\,.$$

Soit m le plus petit entier naturel tel que l'on ait $2^m = 1 + sn$. Si α est un élément primitif de $\mathbb{F}_{2^m}$, l'élément $\beta = \alpha^s$ engendre un groupe cyclique d'ordre n, puisque :

$$\beta^n = \alpha^{ns} = \alpha^{2^m-1} = 1$$

et que les β^k pour $0 \leq k \leq n-1$ sont toutes distinctes. Chaque β^k est une **racine $n^{\text{ième}}$ de l'unité**, β engendre le groupe des racines $n^{\text{ième}}$ de l'unité, et $\mathbb{F}_{2^m}$ est le corps des racines $n^{\text{ième}}$ de l'unité, et le corps de décomposition du polynôme $X^n + 1$.

Appliquons ceci au cas $n = 9$. La suite des restes modulo 9 des puissances de 2 est : 2, 4, 8, 7, 5 et 1. Donc 2^6 est congru à 1 modulo 9. Si α est élément primitif de $\mathbb{F}_{64}$, les racines neuvièmes de l'unité sont les neuf premières puissances de α^7.

6.7 Extensions associées à un polynôme

Un corps $\mathbb{L}$ est **corps de rupture** d'un polynôme irréductible P à coefficients dans un corps $\mathbb{K}$ si P a une racine dans $\mathbb{L}$. Le plus petit corps contenant toutes les racines de P est son **corps de décomposition**, ou son **corps des racines**.

Soit $P = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ un polynôme irréductible à coefficients dans $\mathbb{F}_{2^m}$, dont toutes les racines, x_1,..., x_n (dans $\overline{\mathbb{F}}_2$), sont simples (P n'a pas de racine commune avec son polynôme dérivé, P').

L'idéal (P) étant maximal (P est irréductible), l'anneau-quotient $\mathbb{F}_{2^m}[X]/(P)$ est un corps, noté $\mathbb{M}$. Soit $\mathbb{L}$ le corps engendré par une racine, $\mathbb{L}{=}\mathbb{F}_{2^m}(x_i)$, corps de rupture de P, et $\mathbb{S}$ son corps de décomposition.

Proposition 6.3. *Les classes modulo P de 1, X,..., X^{n-1}, c'est- à-dire 1, x,..., x^{n-1}, forment une base sur $\mathbb{F}_{2^m}$ de l'espace vectoriel $\mathbb{M}$, qui est donc de dimension n.*

Démonstration. Ces classes sont libres, car une relation de dépendance donnerait un polynôme annulateur de x de degré inférieur à celui de P, or P est minimal. Si Q est un polynôme de degré supérieur ou égal à n, la division euclidienne par P :

$$Q = D\,P + R\,,\ \deg(R) \leq n-1$$

montre que sa classe dans $\mathbb{M}$ est celle de R ; elle est donc combinaison linéaire des classes des x_i^k pour $0 \leq k \leq n-1$. Cette famille est donc génératrice et

libre : c'est une base. Comment s'écrit par exemple dans cette base la classe de l'inverse de Q ? L'identité de Bézout (page 65) pour les polynômes assure l'existence de polynômes A et B de $\mathbb{K}[X]$ tels que :

$$P\,A + Q\,B = 1\,,$$

ce qui montre que, modulo P, les classes de Q et de B sont inverses l'une de l'autre, et la classe de Q^{-1} est égale à celle de B, qui est elle-même une combinaison linéaire des classes des x_1^k pour $0 \leq k \leq n-1$. □

Proposition 6.4. *Les puissances x_i^k de x_i pour $0 \leq k \leq n-1$ forment une base sur $\mathbb{F}_{2^m}$ de l'espace vectoriel $\mathbb{L}$, qui est donc de dimension n.*

Démonstration. Elle est identique à la précédente. □

La dimension vectorielle d'une extension $\mathbb{H}$ d'un corps $\mathbb{K}$, lorsqu'elle est finie, est son **degré**, noté $[\mathbb{H} : \mathbb{K}]$.

Proposition 6.5. *Une extension de degré 1 d'un corps $\mathbb{K}$ est égale à $\mathbb{K}$. Une extension $\mathbb{M}$ de degré n d'une extension $\mathbb{L}$ de degré m de $\mathbb{K}$ est une extension de degré mn de $\mathbb{K}$.*

Démonstration. La base d'une extension de degré 1 est réduite à 1 : elle est confondue avec $\mathbb{K}$. Si $y_1, \ldots, y_n$ est une base de $\mathbb{M}$ sur $\mathbb{L}$ et si $x_1, \ldots, x_m$ est une base de $\mathbb{L}$ sur $\mathbb{K}$, les mn produits $x_i\,y_j$ forment une base de $\mathbb{M}$ sur $\mathbb{K}$. □

Les automorphismes de $\mathbb{F}_{2^m}$ forment un groupe cyclique d'ordre m engendré par l'automorphisme de Frobenius, ϕ. La puissance m de ϕ, $\psi = \phi^m$, est égale à l'identité sur $\mathbb{F}_{2^m}$, et ψ laisse donc invariant les coefficients de P. Les images par ψ, ψ^2, etc..., de x_1 sont donc les autres racines de P (ψ^n est l'identité sur le corps des racines). Ces racines sont donc des puissances de x_i et appartiennent à $\mathbb{F}_{2^m}(x_i)$, ce qui prouve l'égalité de $\mathbb{L}$ et de $\mathbb{S}$.

Les extensions $\mathbb{M}$ et $\mathbb{L}$ de $\mathbb{F}_{2^m}$ sont de même degré n. Comme la classe de X est une racine de P ($P(x) = 0$), on peut l'identifier à x_i, faisant de $\mathbb{L}$ une extension de degré 1 de $\mathbb{M}$. Ces deux extensions sont donc égales.

On a ainsi identifié les corps $\mathbb{F}_{2^m}[X]/(P)$, $\mathbb{F}_{2^m}(x_1)$, et $\mathbb{F}_{2^m}(x_1, \ldots, x_n)$.

Donnons un exemple. Le polynôme $P = X^4 + X^3 + X^2 + X + 1$ se factorise dans $\mathbb{F}_{16}$ d'élément primitif α :

$$P = (X + \alpha^3)\,(X + \alpha^6)\,(X + \alpha^9)\,(X + \alpha^{12})\,.$$

Le corps $\mathbb{F}_2[X]/(P)$ contient une racine, par exemple α^9, et ses puissances : α^3, α^6, α^{12}. C'est donc le corps des racines. Comme $\alpha = \alpha^3 + \alpha^9$, il contient α : il est égal à $\mathbb{F}_{16}$.

Remarquons que la situation est différente si $\mathbb{K}$ (de caractéristique 2) est infini. Ainsi, soit $x(t)$ une racine du polynôme $P = X^3 + 1 + t$, à coefficients dans l'extension transcendante $\mathbb{F}_2(t)$. Les autres racines sont $\alpha x(t)$ et $\alpha^2 x(t)$, α étant

un élément primitif de $\mathbb{F}_4$. Elles n'appartiennent ni à $\mathbb{F}_2(t)(x)$ ni à $\mathbb{F}_2(t)[X]/(P)$, mais à $\mathbb{F}_4(t)(x)$, qui est égal au corps des racines $\mathbb{F}_4(t)(x, \alpha x, \alpha^2 x)$. Il y a donc inclusion stricte. Si enfin $x(t)$ est racine du polynôme X^2+t, elle est racine double.

Ceci mène aux définitions suivantes : une extension $\mathbb{L}$ de $\mathbb{K}$ est est une **extension normale** si tout polynôme de $\mathbb{K}[X]$ ayant une racine dans $\mathbb{L}$ a toutes ses racines dans $\mathbb{L}$. Un élément de $\mathbb{L}$ est séparable sur $\mathbb{K}$ s'il est racine simple de son polynôme minimal, et $\mathbb{L}$ est une **extension séparable** de $\mathbb{K}$ si tous ses éléments sont séparables sur $\mathbb{K}$. Enfin, une extension est **galoisienne** si elle est normale et séparable.

Proposition 6.6. *Soit $\mathbb{L}$ une extension algébrique d'un corps $\mathbb{K}$ de caractéristique 2. Un élément x de $\mathbb{L}$ de polynôme minimal P est séparable sur $\mathbb{K}$ si et seulement si $P \notin \mathbb{K}[X^2]$.*

Démonstration. L'élément x est séparable si et seulement si $P'(x) \neq 0$, or $P'(x) = 0$ équivaut à dire que P' est multiple de P, polynôme minimal de x, donc identiquement nul puisque $\deg(P') < \deg(P)$. Comme P peut se mettre sous la forme $P_1(X^2) + X\,P_2(X^2)$ et que les dérivées de $P_1(X^2)$ et de $P_2(X^2)$ sont nulles, on a $P'(X) = P_2(X^2)$; $P' = 0$ équivaut ainsi à $P = P_1(X^2)$, et $P'(x) \neq 0$ à $P \notin \mathbb{K}[X^2]$. □

6.8 Inverses binaires

Si q est un entier relatif impair, il est premier avec 2^n, et il existe, d'après l'identité de Bézout (page 65), des entiers r et s tels que :

$$q\,r + 2^n\,s = 1\ ;$$

r est déterminé modulo 2^n (si on ajoute $2^n k$ à r, il faut remplacer s par $s + kq$), et on peut donc le choisir strictement compris entre 0 et 2^n, ce qui permet de définir l'inverse binaire d'ordre n de q comme étant l'unique entier naturel $(q)_n^{-1}$ défini par la relation :

$$q\,(q)_n^{-1} \equiv 1 \bmod 2^n\,,\ 1 \leq (q)_n^{-1} \leq 2^n - 1\,,\ n \geq 1\,.$$

Ainsi, la suite des inverses binaires de 11 est :

$$((11)_n^{-1}) = (1, 3, 3, 3, 3, 35, 35, 163, 419, 931, 931, 2979, \ldots)\,,$$

et celle de -11 :

$$((-11)_n^{-1}) = (1, 1, 5, 13, 29, 29, 93, 93, 93, 93, 1117, \ldots)\,.$$

La suite des inverses binaires des nombres $2^k - 1$ a une forme particulière (exercice 13) ; écrivons celle de 3 :

$$((3)_n^{-1}) = (1, 3, 3, 11, 11, 43, 43, \ldots)\,,$$

et celle de 7 :

$$((7)_n^{-1}) = (1, 3, 7, 7, 23, 55, 55, 183, 439, 439, \ldots)\,.$$

6.9 Exercices

(1) (Construction de $\mathbb{F}_{16}$)

Vérifier que $\phi^4 = I$, ϕ étant l'automorphisme de Frobenius. Former les classes invariantes par ϕ. Factoriser le polynôme $X^{15} + 1$. Choisir une racine primitive α. Exprimer α^4,..., α^{14} comme combinaisons linéaires de 1, α, α^2, α^3 à coefficients dans $\mathbb{F}_2$. Caractériser les racines primitives.

(2) Montrer l'unicité de la structure de corps à 2^m éléments (considérer deux corps à 2^m éléments, chacun muni d'un élément primitif).

(3) Existe-t-il des puissances de α, élément primitif de $\mathbb{F}_{16}$, annulant P_2 ? P_4 ? Qu'en conclut-on ?

(4) Le corps $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$, de caractéristique 3, est formé des classes modulo 3, restes dans la division des entiers par 3, c'est- à-dire de la classe de 0, représentant les multiples de 3 ($3\mathbb{Z}$), de celle de 1, représentant les multiples de 3 plus 1 ($3\mathbb{Z}+1$) et celle de 2 (ou de -1) représentant les multiples de 3 plus 2 ($3\mathbb{Z}-1$). Les tables d'addition et de multiplication sont évidentes. L'automorphisme de Frobenius est ici l'élévation à la puissance 3. Construire les extensions $\mathbb{F}_9$ et $\mathbb{F}_{27}$.

(5) Montrer que l'ensemble des quatre matrices à coefficients dans $\mathbb{F}_2$:

$$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix},$$

muni de l'addition et du produit matriciel est un anneau de caractéristique 2.

(6) Même question avec les matrices :

$$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

(7) Soit $\mathrm{M}_2(\mathbb{F}_2)$ l'ensemble des matrices à deux lignes et deux colonnes à coefficients dans $\mathbb{F}_2$. Montrer que $\mathrm{M}_2(\mathbb{F}_2)$ muni de l'addition et de la multiplication matricielles est un anneau de caractéristique 2, à 16 éléments. Est-il commutatif ?

Montrer que $\mathrm{M}_2(\mathbb{F}_2)$ est naturellement muni d'une structure d'espace vectoriel sur $\mathbb{F}_2$; en donner une base.

Montrer que l'ensemble des éléments de déterminant égal à 1 est un groupe multiplicatif d'ordre 6, et que l'ensemble des éléments de trace nulle (la trace est la somme des termes diagonaux) est un groupe additif d'ordre 8.

(8) (Détermination de tous les automorphismes de $\mathbb{K} = \mathbb{F}_{2^m}$ et des $\mathbb{K}$-automorphismes de $\mathbb{L} = \mathbb{F}_{2^{mn}}$.

Soit ψ un automorphisme, α un élément primitif de $\mathbb{F}_{2^m}$ et $k \in N^*$ tel que $\psi(\alpha) = \alpha^k$. Evaluer $(x + y)^k$, x et y dans $\mathbb{F}_{2^m}$, à partir de l'écriture binaire de

k. En déduire que $\mathrm{Aut}(\mathbb{F}_{2^m})$ est un groupe cyclique engendré par ϕ, l'automorphisme de Frobenius.

(9) Donner la matrice B, traduction dans $\mathbb{F}_2$ de la matrice :

$$\begin{bmatrix} 1 & \alpha \\ 0 & \alpha^2 \end{bmatrix} \in \mathrm{M}_2(\mathbb{F}_2)\,.$$

(10) Soit P un polynôme irréductible de $\mathbb{F}_2[X]$. Montrer que P :
- n'a pas de racine multiple,
- divise $X^n + 1$ pour certaines valeurs de n,
- engendre une extension de $\mathbb{F}_2$.

Etudier les cas particuliers de $P_r = X^r + X + 1$ pour $2 \leq r \leq 8$.

(11) Soit P un polynôme irréductible de $\mathbb{F}_2[X]$. Montrer qu'un corps de rupture de P contient son corps de décomposition. Montrer, à partir du polynôme $X^3 - 2$, qu'il n'en va pas de même dans $\mathbb{Q}[X]$.

(12) Montrer que tout polynôme irréductible de $\mathbb{F}_{2^m}[X]$ divise un polynôme de la forme $X^n + 1$.

(13) On pose $q = 2^v - 1$. Vérifier qu'il existe un entier naturel d tel que $(q)_d^{-1} = q$. Montrer que $(q)_{n+v}^{-1} = 2^v\,(q)_n^{-1} - 1$; en déduire que la suite (a_k) est périodique. Que se passe-t-il pour $q = (2^v - 1)\,p^{-1}$, $1 \leq p \leq 2^v - 2$? Réciproque ? Calculer les inverses binaires de $p/7$ et de $p/15$.

(14) (Critère d'Eisenstein) Soit $P \in \mathbb{Z}[X]$:

$$P(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0.$$

S'il existe un nombre premier p tel que les a_i, à l'exception de a_n, soient divisibles par p, et que a_0 ne soit pas divisible par p^2, montrer que P est irréductible.

Etendre le domaine d'application du critère en utilisant des translations.

(15) Pour un entier naturel impair q et ses inverses binaires $(q)_n^{-1}$, évaluer la différence $(q)_{n+1}^{-1} + (q)_n^{-1}$; en déduire que $(q)_n^{-1}$ est une somme de puissances de 2 :

$$(q)_n^{-1} = \sum_{k=0}^{n} a_k\, 2^k\,,\ a_k \in \mathbb{F}_2\,.$$

6.10 Correction des exercices

(1) Etablissons la factorisation de $X^{15} + 1$. Soit α une racine primitive 15-ième de l'unité (α^k est aussi une racine primitive de l'unité si le plus grand commun diviseur de k et de 15 vaut 1, c'est- à-dire si k est premier avec 15). Les relations entre les coefficients et les racines d'un polynôme indiquent que la somme des racines vaut 0 et leur produit 1.

Remarquons que l'automorphisme de Frobenius vérifie dans le cas de $\mathbb{F}_{16}$, au sens de la composition, $\phi^4 = I$, de sorte que si on pose :

$$\theta = I + \phi + \phi^2 + \phi^3,$$

on a :

$$(\phi + I) \circ \theta = \phi^4 + I = 0\,,$$

ce qui signifie que :

$$\mathrm{Im}(\theta) \subset \mathrm{Ker}(\phi + I) = \mathbb{F}_2\,.$$

Faisons une partition des éléments de $\mathbb{F}_{16}^*$ en classes globalement invariantes par ϕ :

$$\begin{array}{rcl} E_0 & = & \{1\}\,, \\ E_1 & = & \{\alpha, \alpha^2, \alpha^4, \alpha^8\}\,, \\ E_2 & = & \{\alpha^3, \alpha^6, \alpha^{12}, \alpha^{24} = \alpha^9\}\,, \\ E_3 & = & \{\alpha^5, \alpha^{10}\}\,, \\ E_4 & = & \{\alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11}\}\,, \end{array}$$

et considérons les polynômes cyclotomiques P_k dont les racines sont les éléments de E_k. Nous avons immédiatement $P_0 = X+1$ et $P_3 = X^2+X+1$. Les éléments de E_2 sont les racines de $X^5 + 1$ à l'exception de 1, et donc :

$$P_2 = X^4 + X^3 + X^2 + X + 1\,.$$

Soient σ_k et π_k respectivement la somme et le produit des éléments de E_k, avec évidemment $\pi_k = 1$. Nous avons vu que la somme des σ_k est égale à 0. On vérifie facilement que $\sigma_2 = \sigma_3 = 1$ (progressions géométriques), de sorte que $\sigma_1 + \sigma_4 = 1$. Comme $\sigma_1 = \theta(\alpha^3)$ est dans $\mathbb{F}_2$, choisissons par exemple $\sigma_1 = 0$ (l'autre choix correspondrait à une autre racine primitive, dans E_4), et posons :

$$P_1 = X^4 + s_1\,X^3 + s_2\,X^2 + s_3\,X + s_4\,.$$

Nous savons que $s_1 = \sigma_1 = 0$. La somme des produits des racines deux à deux vaut :

$$s_2 = \alpha^3 + \alpha^5 + \alpha^9 + \alpha^6 + \alpha^{10} + \alpha^{12} = \sigma_2 + \sigma_3 = 0\,,$$

la somme des produits des racines trois à trois :

$$s_3 = \alpha^{14} + \alpha^{13} + \alpha^{11} + \alpha^7 = \sigma_4 = 0\,,$$

et comme $s_4 = \alpha^{15} = 1$ (produit des racines), nous obtenons :

$$P_1 = X^4 + X + 1\,.$$

Les racines de P_4 étant les inverses de celles de P_1, nous avons :

$$P_4 = X^4\,P_1(X^{-1}) = X^4 + X^3 + 1\,,$$

d'où finalement :

$$X^{15}+1 = \Pi\, P_k\,.$$

La racine choisie α étant racine de P_1, elle vérifie la relation $\alpha^4 = \alpha + 1$; on a ensuite :

$$\begin{array}{lcl}
\alpha^5 & = & \alpha^2+\alpha\,,\\
\alpha^6 & = & \alpha^3+\alpha^2\,,\\
\alpha^7 & = & \alpha^3+\alpha+1\,,\\
\alpha^8 & = & \alpha^2+1\,,\\
\alpha^9 & = & \alpha^3+\alpha\,,\\
\alpha^{10} & = & \alpha^2+\alpha+1\,,\\
\alpha^{11} & = & \alpha^3+\alpha^2+\alpha\,,\\
\alpha^{12} & = & \alpha^3+\alpha^2+\alpha+1\,,\\
\alpha^{13} & = & \alpha^3+\alpha^2+1\,,\\
\alpha^{14} & = & \alpha^3+1\,,\\
\alpha^{15} & = & 1\,,
\end{array}$$

et les α^k sont combinaisons linéaires de 1, α, α^2, α^3 à coefficients dans $\mathbb{F}_2$ ($\mathbb{F}_{16}$ est un espace vectoriel de dimension 4 sur $\mathbb{F}_2$, mais aussi un espace vectoriel de dimension 2 sur $\mathbb{F}_4$). Les racines primitives sont les α^k pour k premier avec 15, donc multiple ni de 3 ni de 5.

(2) Considérons deux corps, $\mathbb{K}_1$ et $\mathbb{K}_2$ de caractéristique 2, ayant 2^m éléments. Nous allons montrer qu'ils sont isomorphes, de sorte que la structure de corps à 2^m éléments est unique : nous noterons $\mathbb{F}_{2^m}$ tous les corps à 2^m éléments, que nous identifierons donc, à isomorphisme près. Les groupes multiplicatifs $\mathbb{K}_1^*$ et $\mathbb{K}_2^*$ sont évidemment isomorphes en tant que groupes cycliques de même ordre, mais il faut trouver un isomorphisme respectant les structures additives. Soit α un élément primitif de $\mathbb{K}_1$, racine du polynôme cyclotomique P, et β un élément primitif de $\mathbb{K}_2$; les puissances de β sont 2^m-1 racines du polynôme $X^{2^m-1}+1$, c'est- à-dire le groupe cyclique $\mathbb{K}_2^*$; P divisant ce polynôme, une puissance de β est racine de P : appelons-la α_* ; les autres racines de P sont les itérées de α_* par l'automorphisme de Frobenius. Considérons l'isomorphisme de groupes multiplicatifs :

$$\chi : \mathbb{K}_1^* \to \mathbb{K}_2^*\,,\ \chi(\alpha) = \alpha_*\,.$$

Les deux corps étant des espaces vectoriels de dimension m sur $\mathbb{F}_2$, les monômes 1, X,..., X^{m-1} sont libres et P est de degré m.

Si $P = X^m + \sum_{i=0}^{m-1} \lambda_i\, X^i$, nous obtenons les deux relations :

$$\alpha^m = \sum_{i=0}^{m-1} \lambda_i\, \alpha^i\,,\ \alpha_*^m = \sum_{i=0}^{m-1} \lambda_i\, \alpha_*^i\,.$$

Les combinaisons linéaires ont les mêmes coefficients. Pour obtenir à partir de χ un isomorphisme de corps, il nous faut d'abord le prolonger en 0 en posant $\chi(0) = 0$, puis montrer que, pour des éléments quelconques, on a $\chi(x+y) =$

$\chi(x)+\chi(y)$; or ces éléments sont des puissances de α, respectivement $x=\alpha^r$ et $y=\alpha^s$; soit α^t leur somme :

$$\begin{aligned}\chi(x+y) &= \chi(\alpha^t)\\ &= \alpha_*^t\\ &= \alpha_*^r+\alpha_*^s\\ &= \chi(x)+\chi(y)\,.\end{aligned}$$

La bijectivité de χ découle de sa construction même. Le résultat demeure en caractéristique quelconque, avec la même démonstration.

(3) Par construction, si $P_2(\alpha^k)=0$, k est multiple de 3, donc non premier avec 15, et α^k n'est pas primitive. Si $P_4(\alpha^k)=0$, k est multiple de 7 modulo 15. On trouve les valeurs 7, 14, 13 et 11. Les α^k sont primitives. En choisissant une racine de P_4 on obtient un corps isomorphe, donc encore $\mathbb{F}_{16}$.

(4) Factorisons X^8-1 dans $\mathbb{F}_3$; remarquons que -1 ne peut être égal qu'à α^4 ; les ensembles cyclotomiques sont :

$$\begin{aligned}E_0 &= \{1,-1\}\,,\\ E_1 &= \{\alpha,\alpha^3\}\,,\\ E_2 &= \{\alpha^2,\alpha^6\}\,,\\ E_3 &= \{\alpha^5,\alpha^7\}\;;\end{aligned}$$

et les polynômes cyclotomiques, excepté $P_0=(X-1)\,(X+1)$:

$$\begin{aligned}P_1 &= X^2-(\alpha+\alpha^3)X-1,\\ P_2 &= X^2-(\alpha^2+\alpha^6)X+1,\\ P_3 &= X^2-(\alpha^5+\alpha^7)X-1\,.\end{aligned}$$

Le terme $\alpha^2+\alpha^6=\alpha^2(1+\alpha^4)$ est nul. Etant invariant par ϕ et non nul, $\alpha+\alpha^3$ peut être égal à 1 ou à -1 ; choisissons 1.

Comme $\alpha^5+\alpha^7=\alpha^4(\alpha+\alpha^3)=-1$, on a finalement :

$$\begin{aligned}P_1 &= X^2-X-1\,,\\ P_2 &= X^2+1\,,\\ P_3 &= X^2+X-1\,.\end{aligned}$$

On déduit de P_1 pour l'élément primitif les deux relations :

$$\alpha^2=\alpha+1=\alpha^6\,,$$

$$\alpha^3=\alpha^2+\alpha=2\alpha+1=-\alpha^7\,.$$

Pour construire $\mathbb{F}_{27}$ il faut d'abord factoriser $X^{26}-1$ dans $\mathbb{F}_3$ par la méthode

habituelle. La partition est :

$$\begin{aligned}
E_0 &= \{1, \alpha^{13}, -1\}, \\
E_1 &= \{\alpha, \alpha^3, \alpha^9\}, \\
E_2 &= \{\alpha^2, \alpha^6, \alpha^{18}\}, \\
E_3 &= \{\alpha^4, \alpha^{12}, \alpha^{10}\}, \\
E_4 &= \{\alpha^5, \alpha^{15}, \alpha^{19}\}, \\
E_5 &= \{\alpha^7, \alpha^{21}, \alpha^{19}\}, \\
E_6 &= \{\alpha^8, \alpha^{24}, \alpha^{20}\}, \\
E_7 &= \{\alpha^{14}, \alpha^{16}, \alpha^{22}\}, \\
E_8 &= \{\alpha^{17}, \alpha^{25}, \alpha^{23}\}.
\end{aligned}$$

Soit s_i la somme des éléments de E_i. Les polynômes cyclotomiques, excepté $P_0 = (X+1)(X-1)$, sont :

$$\begin{aligned}
P_1 &= X^3 - s_1 X^2 + s_3 X + 1, \\
P_2 &= X^3 - s_2 X^2 - s_6 X - 1, \\
P_3 &= X^3 - s_3 X^2 + s_7 X - 1, \\
P_4 &= X^3 - s_4 X^2 + s_6 X + 1, \\
P_5 &= X^3 - s_5 X^2 + s_2 X + 1, \\
P_6 &= X^3 - s_6 X^2 + s_2 X - 1, \\
P_7 &= X^3 - s_7 X^2 + s_3 X - 1, \\
P_8 &= X^3 - s_8 X^2 + s_7 X + 1.
\end{aligned}$$

De $\alpha^{13} = -1$ on déduit les relations $s_7 = -s_1$, $s_4 = -s_2$, $s_8 = -s_3$, $s_6 = -s_5$. Choisissons $s_1 = 0$, $s_2 = -1$, puis remarquons que les éléments de E_2 sont les carrés de ceux de E_1, de même pour E_6 et E_3. On obtient les relations : $s_2 = s_1^2 + s_3 = s_3$ (d'où $s_3 = -1$), $s_6 = s_3^2 + s_7$ (d'où $s_6 = 1$ et $s_5 = -1$). De $0 = s_7 s_8 = s_4 + s_5$ on tire $s_4 = 1$. Finalement on obtient :

$$\begin{aligned}
P_1 &= X^3 - X + 1, \\
P_2 &= X^3 + X^2 + X - 1, \\
P_3 &= X^3 + X^2 - 1, \\
P_4 &= X^3 - X^2 + X + 1, \\
P_5 &= X^3 + X^2 - X + 1, \\
P_6 &= X^3 - X^2 - X - 1, \\
P_7 &= X^3 - X - 1, \\
P_8 &= X^3 - X^2 + 1.
\end{aligned}$$

A partir de $P_1(\alpha) = 0$ on a $\alpha^3 = \alpha + 1$, $\alpha^4 = \alpha^2 + \alpha$, etc... Les racines primitives étant les α^k pour k impair et différent de 13, on obtient un corps isomorphe, donc la même structure, en partant de P_1, de P_4, de P_5 ou de P_8. De même en faisant un choix différent pour s_1 et s_2.

(5) Les neutres sont O et I ; $P + Q = I$; $P + P = Q + Q = I + I = O$; $P^3 = P$; $Q^3 = Q$; $PQ = 0$. L'ensemble est stable pour les deux lois. L'anneau est commutatif, non intègre, de caractéristique 2.

(6) Les neutres sont O et I ; $A + A = B + B = I + I = O$ (caractéristique 2) ; la somme de deux éléments non nuls donne le troisième, et l'ensemble est stable pour l'addition ; $A^2 = O$, $B^2 = I$, $AB = BA = A$, et l'ensemble est stable pour la multiplication. L'anneau est commutatif et non intègre ; A est nilpotent, ses puissances étant nulles à partir de 2 ; B est idempotent : $B^{2k} = I$, $B^{2k+1} = B$.

(7) On sait que $\mathrm{M}_n(\mathbb{K})$, $\mathbb{K}$ étant un corps quelconque et n un entier supérieur à 1, est un anneau, non intègre et non commutatif en général ; M possède $2^4 = 16$ éléments ; il est non commutatif :

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$

et :

$$\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}.$$

L'élément générique s'écrit :

$$\begin{bmatrix} a & c \\ b & d \end{bmatrix} = a \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + b \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} + c \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} + d \begin{bmatrix} 0 & c \\ 0 & 1 \end{bmatrix}$$

$$= a\, e_1 + b\, e_2 + c\, e_3 + d\, e_4 \,,$$

avec a, b, c, d dans $\mathbb{F}_2$; les e_i sont libres et forment une base de M, espace vectoriel de dimension 4 sur $\mathbb{F}_2$. Le déterminant de l'élément générique étant égal à $ad + bc$, il est égal à 1 si $ad + bc = 1$; résolvons donc cette équation dans $\mathbb{F}_2$:

$$ad = 1\,,\ bc = 0 \Rightarrow \{(1,0,0,1),(1,0,1,1),(1,1,0,1)\}\,,$$

$$ad = 0\,,\ bc = 1 \Rightarrow \{(0,1,1,0),(1,1,1,0),(0,1,1,1)\}\,,$$

ce qui donne six éléments.

L'ensemble est stable pour le produit matriciel, le déterminant d'un produit étant égal au produit des déterminants, donc à 1. C'est un groupe d'ordre 6 non commutatif car :

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$$

et :

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}.$$

Les éléments de trace nulle vérifient l'équation $a + d = 0$; ce sont :

$$a = d = 0 \Rightarrow \{(0,0,0,0),(0,0,1,0),(0,1,0,0),(0,1,1,0)\}\,,$$

$$a = d = 1 \Rightarrow \{(1,0,0,1),(1,0,1,1),(1,1,0,1),(1,1,1,1)\}\,.$$

La trace d'une somme étant la somme des traces, l'ensemble est stable pour l'addition : c'est un groupe d'ordre 8, commutatif.

(8) Si l'écriture binaire de k, $\sum_i a_i 2^i$, contient n coefficients a_i non nuls (égaux à 1), une récurrence immédiate montre que $(x+y)^k$ possède 2^n monômes ; or on doit avoir $(x+y)^k = x^k + y^k$ pour que ψ soit un automorphisme de $\mathbb{K}$, ce qui impose que $n = 1$ et que $k = 2^r$; on a donc $\psi = \phi^r$. Les automorphismes de $\mathbb{K}$ sont donc les puissances ϕ^r de ϕ, de $r = 1$ à $r = m$, cette dernière donnant l'identité.

Les automorphismes de $\mathbb{L}$ sont les puissances de ϕ, de 1 à mn, et ses $\mathbb{K}$-automorphismes sont donc les puissances de ϕ^m de 1 à n.

(9) La matrice B est associée à un endomorphisme de $\mathbb{F}_2^4$. Traduisons les éléments de $\mathbb{F}_4$, dans $\mathbb{F}_2$:

$$O = \begin{bmatrix} 0 \\ 0 \end{bmatrix},\ 1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix},\ \alpha = \begin{bmatrix} 0 \\ 1 \end{bmatrix},\ \alpha^2 = 1 + \alpha = \begin{bmatrix} 1 \\ 1 \end{bmatrix},$$

puis les multiplications, représentées par des matrices de $\mathrm{M}_2(\mathbb{F}_2)$. La multiplication par 1 est l'identité. La multiplication par α est représentée par la matrice dont la première colonne est l'image de 1, soit α, la deuxième colonne, l'image de α, soit α^2 ; on obtient :

$$M(\alpha) = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$$

et enfin la multiplication par α^2 :

$$M(\alpha^2) = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}.$$

Reportons ces résultats dans A pour obtenir la matrice :

$$B = \begin{bmatrix} M(1) & M(\alpha) \\ M(0) & M(\alpha^2) \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

(10) Les racines x_1, x_2,..., x_d de P appartiennent à $\overline{\mathbb{F}}_2$, et sont donc dans une certaine extension $\mathbb{F}_{2^m}$ de $\mathbb{F}_2$. L'ensemble des racines étant globalement invariant sous l'action de l'automorphisme de Frobenius, ϕ, on peut supposer, quitte à changer les indices, que $x_{i+1} = \phi(x_i)$, avec $x_{d+1} = x_1$. Si P s'écrit :

$$P = \prod_k (X + x_k)^{p_k},$$

il s'écrit aussi, étant invariant par ϕ :

$$P = \prod_k (X + x_{k+1})^{p_k},$$

d'où l'on conclut que les p_k sont égaux entre eux, $p_k = p$, et que :

$$P = \Big(\prod_k (X + x_k) \Big)^p = Q^p \,.$$

Le polynôme Q, étant invariant par ϕ, appartient à $\mathbb{F}_2[X]$; ceci contredit l'hypothèse d'irréductibilité de P. On a évidemment $\phi^d = I$, et donc $m = d$. Les x_k appartiennent à $\mathbb{F}_{2^d}$ et sont racines du polynôme $X^{2^d-1} + 1$, qui est donc divisible par P, comme d'ailleurs tous les polynômes $X^n + 1$ associés aux extensions successives de $\mathbb{F}_{2^d}$. L'équation $P_r = 0$ donne, pour les racines de P_r, $x^r = x + 1$, d'où $x^{r+1} = x^2 + x$,..., jusqu'à obtenir $x^n = 1$. Appliquons ceci pour les valeurs croissantes de r :

$$\begin{array}{lllllll}
x^2 + x + 1 = 0 & \Rightarrow & x^3 = x^2 + x = 1 & \Rightarrow & \mathbb{F}_4 \,, & & \\
x^3 + x + 1 = 0 & \Rightarrow & x^6 = x^2 + 1 & \Rightarrow & x^7 = 1 & \Rightarrow & \mathbb{F}_8 \,, \\
x^4 + x + 1 = 0 & \Rightarrow & x^8 = x^2 + 1 & \Rightarrow & x^{16} = x^4 + 1 = x & \Rightarrow & \mathbb{F}_{16} \,, \\
x^5 + x + 1 = 0 & \Rightarrow & x^{20} = x^4 + 1 & \Rightarrow & x^{21} = x^5 + x = 1 & \Rightarrow & x^{63} = 1 \,,
\end{array}$$

la dernière ligne donnant $\mathbb{F}_{64}$, alors qu'on attendait plutôt $\mathbb{F}_{32}$. Factorisons P_5 dans $\mathbb{F}_{64}$, d'élément primitif ω :

$$P_5 = (X + \omega^{21})\,(X + \omega^{42})\,(X + \omega^{27})\,(X + \omega^{54})\,(X + \omega^{45}) \,.$$

Les deux premières racines forment un ensemble globalement invariant par ϕ, de même que les trois dernières, et les éléments de ces deux ensembles sont donc les racines de deux polynômes de $\mathbb{F}_2[X]$:

$$(X + \omega^{21})\,(X + \omega^{42}) = X^2 + X + 1 \,,$$

et :

$$(X + \omega^{27})\,(X + \omega^{54})\,(X + \omega^{45}) = X^3 + X^2 + 1 \,.$$

On voit que P_5 n'est pas irréductible dans $\mathbb{F}_2$; $X^2 + X + 1$ se scinde dans $\mathbb{F}_4$, $X^3 + X^2 + 1$ dans $\mathbb{F}_8$, donc P_5 dans leur extension commune $\mathbb{F}_{64}$. Poursuivons :

$$\begin{array}{lllllll}
x^6 + x + 1 = 0 & \Rightarrow & \ldots & \Rightarrow & X^{63} = 1 & \Rightarrow & \mathbb{F}_{64} \,, \\
x^7 + x + 1 = 0 & \Rightarrow & \ldots & \Rightarrow & x^{127} = 1 & \Rightarrow & \mathbb{F}_{128} \,, \\
x^8 + x + 1 = 0 & \Rightarrow & \ldots & \Rightarrow & x^{63} = 1 & \Rightarrow & \mathbb{F}_{64} \,;
\end{array}$$

P_8 n'est donc pas irréductible :

$$P_8 = (X^2 + X + 1)\,(X^6 + X^5 + X^3 + X^2 + 1) \,.$$

(11) Ceci revient à montrer que si $\mathbb{F}_{2^m}$ contient une racine α de P, il les contient toutes. Les itérées de α par l'automorphisme de Frobenius sont racines de P, et le polynôme :

$$R = (X + \alpha)\,(X + \phi(\alpha)) \ldots (X + \phi^{m-1}(\alpha))$$

divise P, supposé irréductible ; R et P sont donc égaux.

L'hypothèse d'irréductibilité est nécessaire : le polynôme P_5 de l'exercice précédent admet $\mathbb{F}_4$ comme corps de rupture et $\mathbb{F}_{64}$ comme corps de décomposition.

Le polynôme X^3-2, irréductible dans $\mathbb{Q}$, a une racine réelle, $\alpha = 2^{1/3}$; $\mathbb{Q}[\alpha]$ est un corps de rupture, dans lequel :

$$X^3 - 2 = (X-\alpha)\,(X^2+\alpha X+\alpha^2)\,.$$

Le corps de décomposition est $\mathbb{Q}[\alpha, j]$, avec $j = (-1+i\sqrt{3}\,)/2$, les autres racines étant $j\alpha$ et $j^2\alpha$.

(12) Le corps $\mathbb{F}_{2^m}$ a pour clôture algébrique $\overline{\mathbb{F}}_2$, et tout polynôme irréductible $P \in \mathbb{F}_{2^m}[X]$ se décompose en produit de facteurs du premier degré dans $\overline{\mathbb{F}}_2$; ce dernier étant la réunion de tous les $\mathbb{F}_{2^q}$, les racines de P sont dans l'un de ces corps (et dans ses extensions), par exemple dans $\mathbb{F}_{2^n}$; elles sont donc racines du polynôme $X^{2^n-1}+1$, que divise donc P. Le quotient appartient à $\mathbb{F}_{2^m}[X]$ car on vérifie sans peine que les relations symétriques entre ses racines, qui donnent ses coefficients, sont dans $\mathbb{F}_{2^m}$. Une extension algébrique d'une extension algébrique de $\mathbb{F}_2$ est donc une extension algébrique de $\mathbb{F}_2$.

(13) Comme $q^2 = 2^{v+1}(2^{v-1}+1)+1$, q est l'un de ses inverses binaires. Partons de la définition :

$$(2^k-1)\,(q)_n^{-1} = 2^n h + 1\,,$$

et posons $r = 2^v (q)_n^{-1} - 1$; la condition $(q)_n^{-1} < 2^n$ impose que $r < 2^{n+k}$; on a successivement :

$$\begin{aligned}(2^v-1)r &= (2^v-1)\left((2^v-1)\,(q)_n^{-1} + (q)_n^{-1} - 1\right),\\ &= (2^v-1)\,(2^n\,h + (q)_n^{-1})\,,\\ &= 2^{n+v}\,h + 1\,,\end{aligned}$$

ce qui montre que $r = (q)_{n+v}^{-1}$; pour montrer la périodicité, évaluons la différence :

$$(q)_{n+v}^{-1} - (q)_{n+v-1}^{-1} = 2^v\left((q)_n^{-1} - (q)_{n-1}^{-1}\right)$$

si $a_n = 0$, $(q)_n^{-1} = (q)_{n-1}^{-1}$, et $a_{n+v} = 0$; si $a_n = 1$:

$$(q)_n^{-1} = (q)_{n-1}^{-1} + 2^{n-1}\,,$$

$$(q)_{n+v}^{-1} = (q)_{n+v-1}^{-1} + 2^{n+v-1}\,,$$

et $a_{n+v} = 1$; on a donc $a_{n+v} = a_n$.

Passons au cas $q = (2^v-1)p^{-1}$, avec $1 \le p \le 2^v-2$. La longueur de la période est conservée, et il y a 2^v-2 possibilités pour la valeur $(a_{v+1}, \ldots, a_{2v})$ de ses coefficients, si l'on exclut évidemment $(0,\ldots,0)$ et $(1,\ldots,1)$, qui correspondent à $q=1$. On fait démarrer la période à $v+1$ et non à 1 pour ne pas devoir traiter le cas « pair » . Ces 2^v-2 possibilités sont associées aux différentes valeurs de p ; $(0,1,\ldots,1)$ correspond à $p=1$, $(0,\ldots,0,1)$ à $p = 2^{v-1}-1$, la multiplication

par 2 décale d'une unité vers la droite, et les périodes de p et de $2^v - p - 1$ sont complémentaires ; donnons un exemple, avec $v = 3$:

$$\frac{1}{7} \mapsto (0,1,1)\,,\ \frac{2}{7} \mapsto (1,0,1)\,,\ \frac{4}{7} \mapsto (1,1,0)\,,$$
$$\frac{6}{7} \mapsto (1,0,0)\,,\ \frac{5}{7} \mapsto (0,1,0)\,,\ \frac{3}{7} \mapsto (0,0,1)\,.$$

Réciproquement, la longueur de la période donne $2^v - 1$ et sa valeur, somme des $a_k 2^k$, donne p. Ainsi, par exemple, la période $(1,1,1,0)$ est associée à $8/15$ car sa complémentaire, $(0,0,0,1)$, correspond à $7/15$. On peut aussi remarquer qu'en décalant de trois unités la période $(0,0,0,1)$ de $1/15$, on obtient celle de $2^3/15$.

Pour avoir les périodes de $p/15$, il nous manque celles de $3/15$ et de $5/15$:

$$\frac{3}{15} \mapsto (0,0,1,1)\ ,\ \frac{5}{15} \mapsto (0,1,0,1)\,.$$

En effet :

$$\frac{1}{15} \mapsto (0,1,1,1) \Rightarrow \frac{2}{15} \mapsto (1,0,1,1)\ , \frac{4}{15} \mapsto (1,0,0,1)\ ,\ \frac{8}{15} \mapsto (1,1,1,0)\,,$$
$$\frac{14}{15} \mapsto (0,1,1,1) \Rightarrow \frac{13}{15} \mapsto (0,1,0,0)\ , \frac{11}{15} \mapsto (0,0,1,0)\ ,\ \frac{7}{15} \mapsto (0,0,0,1)\,,$$
$$\frac{3}{15} \mapsto (0,0,1,1) \Rightarrow \frac{6}{15} \mapsto (1,0,0,1)\ , \frac{12}{15} \mapsto (1,1,0,0)\ ,\ \frac{9}{15} \mapsto (0,1,1,0)\,,$$
$$\frac{5}{15} \mapsto (0,1,0,1) \Rightarrow \frac{10}{15} \mapsto (1,0,1,0)\,.$$

(14) En plongeant P dans $\mathbb{F}_p[X]$, on obtient le monôme $\bar{P}(X) = \bar{a}_n X^n$. Si P était égal au produit RS de deux polynômes de $\mathbb{Z}[X]$, on aurait dans $\mathbb{F}_p[X]$ $\bar{R}(X)\bar{S}(X) = \bar{a}_n X^n$. Or le produit de deux polynômes n'est un monôme que si chacun de ces polynômes est un monôme. En effet, comme $\bar{R}(0)\bar{S}(0) = 0$ grâce à la condition sur a_0, et l'une, au moins, des deux constantes est nulle. Si c'est $\bar{R}(0)$, on divise $\bar{R}$ par X, et on recommence, jusqu'à ce que l'un des deux polynôme soit une constante : c'était donc un monôme au départ, et l'autre est forcément un monôme. Enfin, $P = RS$ impliquerait que $a_0 = r_0 s_0$ serait divisible par p^2.

Si $a_0 = 0$, on divise P par X.

Si P est irréductible, $P(X + a)$, $\forall a \in \mathbb{Z}$, l'est aussi.

Le polynôme $P(X) = X^4 + X^3 + X^2 + X + 1$ n'obéit pas aux conditions du critère, mais $Q(X) = P(X + 1)$:

$$Q(X) = X^4 + 5X^3 + 10X^2 + 10X + 5$$

y obeit, pour $p = 5$, et n'est pas factorisable, de même que P.

(15) On a évidemment $(q)_1^{-1} = 1$ et $(q)_2^{-1} = 1$ ou 3 ; la différence vaut 0 ou 2. Plus généralement, la définition :

$$\begin{aligned} q\,(q)_n^{-1} &\equiv 1 \bmod 2^n\,, \\ q\,(q)_{n+1}^{-1} &\equiv 1 \bmod 2^{n+1}\,, \end{aligned}$$

implique que :

$$q\,(q)_{n+1}^{-1} - q(q)_n^{-1} = 2^n k\,.$$

Mais comme $q\,(q)_{n+1}^{-1}$ est inférieur à 2^{n+1}, k est nul ou égal à 1.
Si $q\,(q)_{n+1}^{-1} - q\,(q)_n^{-1}$ n'est pas nul, il vaut 2^n, d'où la conclusion.

7 Théorie de Galois

7.1 Quelques rappels historiques

Les notions de groupe et de corps mènent naturellement à la théorie de Galois, qui, historiquement, est à leur origine. Nous allons en dire quelques mots. Elle est traitée de façon complète, par exemple, dans le livre "Théorie de Galois" de Jean-Pierre Escofier, chez Masson, qui contient beaucoup d'exercices corrigés. Citons également le livre "Equations algébriques et théorie de Galois" de Claude Mutafian, chez Vuibert.

Un illustre mathématicien, contemporain de Galois, avait jugé cette théorie sans intérêt, les méthodes d'Analyse Numérique donnant les racines avec la précision souhaitée, mais, outre sa beauté, son principal mérite est d'avoir ouvert la voie à l'Algèbre moderne.

Avant la mise au point de l'écriture mathématique, la simple représentation d'un polynôme était peu maniable. Ainsi, au seizième siècle encore, $X^3 + \cdots$ va s'exprimer "*Le cube avec les choses...*".

Le zéro était connu des Mayas et des Hindous il y a près de deux mille ans, des Arabes au huitième siècle, des Européens au treizième siècle (ils utilisaient encore les chiffres romains).

Les nombres négatifs sont entrés dans les moeurs en Occident très tard et difficilement. Sans le zéro ni les nombres négatifs, comment écrire l'équation $X^3 + X + 1 = 0$? Mais cette équation n'était d'ailleurs même pas envisageable, les solutions devant être positives.

La notation des variables et des paramètres par des lettres date de la fin du seizième siècle.

La nécessité des nombres complexes était connue, mais le symbole i n'a été accepté, petit à petit, qu'avec réticence.

Enfin, Euler (1707-1783) vint... Pensons à tout ce qu'on lui doit.

Le symbolisme complet utilisé aujourd'hui, y compris les conventions d'Einstein, date du vingtième siècle.

Les Babyloniens savaient résoudre certaines équations de degré 2, il y a près de 4000 ans.

des formules et méthodes explicites pour les degrés 3 et 4 sont apparues au seizième siècle, mais on savait déjà résoudre certaines équations de degré 3.

Le degré 5 résistait à tous les assauts.

7.2 Extensions algébriques

7.2.1 Polynôme minimal, éléments conjugués

Un corps $\mathbb{L}$ sera une **extension algébrique** d'un corps $\mathbb{K}$ si $\mathbb{K}$ est un sous-corps de $\mathbb{L}$ et si tous les éléments de $\mathbb{L}$ n'appartenant pas à $\mathbb{K}$ sont algébriques sur $\mathbb{K}$, c'est-à-dire racine d'un polynôme $P \in \mathbb{K}[X]$.

L'ensemble des polynômes de $\mathbb{K}[X]$ annulant un élément $x \in \mathbb{L}$ est un idéal de $\mathbb{K}[X]$, donc monogène, et le polynôme unitaire engendrant cet idéal est le

polynôme minimal de x sur $\mathbb{K}$, P. Le degré de P est le **degré (algébrique)** de x (sur $\mathbb{K}$).

Deux éléments de $\mathbb{L}$ sont **conjugués** s'ils ont même polynôme minimal.

Nous considérons les corps $\mathbb{K}$ de caractéristique 0, donc infinis, contenant $\mathbb{Q}$ à partir de leur élément 1, et contenus dans $\mathbb{C}$ (algébriquement clos).

Le corps $\mathbb{K}$ sera donc $\mathbb{Q}$ ou une extensions de $\mathbb{Q}$, algébrique ou non.

Rappelons que $\mathbb{K}[a]$ est l'image de $\mathbb{K}[X]$ par le morphisme d'anneaux, de $\mathbb{K}[X]$ dans $\mathbb{K}$, défini par $X \mapsto a$, dont le noyau est l'idéal P engendré par le polynôme minimal P de a si a est algébrique. L'anneau $\mathbb{K}[a]$ est donc isomorphe à $\mathbb{K}[X]/(P)$; $\mathbb{K}(a)$ est son corps des fractions.

L'inverse de $a+b\sqrt{2}$, a et b rationnels non tous les deux nuls, est $-\frac{1}{a}+\frac{\sqrt{2}}{2b}$ si $a \neq 0$, $\frac{\sqrt{2}}{2b}$ si $a=0$ et $\frac{1}{a}$ si $b=0$, de sorte que $\mathbb{Q}[\sqrt{2}] = \mathbb{Q}(\sqrt{2})$. C'est une extension algébrique de $\mathbb{Q}$, définie par le polynôme minimal X^2-2, dont les deux racines sont dans $\mathbb{Q}[\sqrt{2}] = \mathrm{vect}_{\mathbb{Q}}(1,\sqrt{2})$. Sa dimension vectorielle est donc égale à 2.

L'anneau $\mathbb{Q}[\pi] = \{a\pi + b \,|\, a,b \in \mathbb{Q}\}$ n'est pas un corps, et il diffère de son corps des fractions $\mathbb{Q}(\pi)$.

Proposition 7.1. *Si a est algébrique sur $\mathbb{K}$, on a $\mathbb{K}(a) = \mathbb{K}[a]$.*

Démonstration. Si P est le polynôme minimal de a, il est évidemment irréductible, l'idéal (P) est maximal, $\mathbb{K}[X]$ est intègre, et $\mathbb{K}[X]/(P)$ est un corps ; $\mathbb{K}[a]$, isomorphe à $\mathbb{K}[X]/(P)$, est donc un corps, égal à son corps des fractions $\mathbb{K}(a)$. □

L'ensemble $\mathbb{Q}[\sqrt{2},\sqrt{3}]$ des éléments $a+b\sqrt{2}+c\sqrt{3}$, $a,b,c \in \mathbb{Q}$, est une extension algébrique de $\mathbb{Q}$. Il est égal à $\mathbb{Q}[a] = \mathbb{Q}(a)$ avec $a = \sqrt{2}+\sqrt{3}$, car en élevant $a-\sqrt{2}$ au carré on obtient :

$$\sqrt{2} = \frac{a^2-1}{2a},\ \sqrt{3} = \frac{a^2+1}{2a},$$

et le carré de a^2-5 donne $a^4-10a^2+1=0$; a est donc algébrique sur $\mathbb{Q}$ et engendre $\mathbb{Q}[\sqrt{2},\sqrt{3}]$. Nous verrons que c'est un *élément primitif*.

Ce corps est engendré vectoriellement par $1,\sqrt{2},\sqrt{3},\sqrt{6}$, et sa dimension vectorielle est égale à 4. Il est isomorphe à $\mathbb{Q}[\sqrt{2}]\,[\sqrt{3}]$ (ou $\mathbb{Q}[\sqrt{3}]\,[\sqrt{2}]$...).

Plus généralement, la somme et le produit de deux nombres algébriques a et b sont algébriques, $\mathbb{Q}(a,b)$ étant une extension algébrique de $\mathbb{Q}$. Le calcul de leurs polynômes minimaux peut être assez fastidieux.

L'extension $\mathbb{L}$ de $\mathbb{K}$ est un espace vectoriel sur $\mathbb{K}$. La dimension de cet espace vectoriel est le **degré** de l'extension, noté $[\mathbb{L} : \mathbb{K}]$. Ainsi, $\mathbb{C}$ est une extension algébrique de $\mathbb{R}$ de degré 2 ($\mathbb{C} = \mathbb{R}[i] = \mathrm{vect}_{\mathbb{R}}(1,i)$).

Nous ne considérerons que les extensions de degré fini.

Exemple 7.1. Les racines du polynôme $X^3+2 \in \mathbb{Q}[X]$ sont $-\sqrt[3]{2}$, $-j\sqrt[3]{2}$ et $-j^2\sqrt[3]{2}$. Leur somme est nulle ($1+j+j^2=0$, $-j^2 = 1+j$).

Le corps des racines de ce polynôme est engendré vectoriellement par 1, $\sqrt[3]{2}$, $j\sqrt[3]{2}$, j (quotient des deux précédents), $\sqrt[3]{4}$ et $j\sqrt[3]{4}$. On obtient en effet deux racines : $-\sqrt[3]{2}$, $-j\sqrt[3]{2}$, puis la troisième, la somme des trois étant nulle, et leurs carrés. C'est donc une extension de degré 6 de $\mathbb{Q}$. Elle est engendrée algébriquement par j et $\sqrt[3]{2}$, ou par $a = \sqrt[3]{2}+j$, *élément primitif*, car $(a-j)^3 = 2$ donne :

$$j = \frac{a^3 - 3a - 3}{3(a^2+a)}, \text{ d'où } \sqrt[3]{2} = \frac{2a^3 + 3a^2 + 3a + 3}{3(a^2+a)}.$$

Cet exemple est repris dans les exemples 7.2. et 7.4. ▽

Proposition 7.2. *Si $\mathbb{L}$ est une extension de degré fini p de $\mathbb{K}$ et si $\mathbb{M}$ est une extension de degré fini q de $\mathbb{L}$, $\mathbb{M}$ est une extension de degré fini pq de $\mathbb{K}$:*

$$[\mathbb{M} : \mathbb{K}] = [\mathbb{M} : \mathbb{L}]\,[\mathbb{L} : \mathbb{K}].$$

Démonstration. Si les $(l_1, \ldots, lp)$ forment une base de l'espace vectoriel $\mathbb{L}$ sur $\mathbb{K}$ et si les $(m_1, \ldots, m_q)$ forment une base de l'espace vectoriel $\mathbb{M}$ sur $\mathbb{L}$, les pq $L_i m_j$ forment une base de l'espace vectoriel $\mathbb{M}$ sur $\mathbb{K}$:

$$\begin{cases} x \in \mathbb{M} \Rightarrow x = \sum_j x_j m_j = \sum_j x_j \sum_i \lambda_{ij} l_i = \sum_{ij} x_j \lambda_{ij} l_i m_j, \\ \sum \mu_{ij} l_i m_j = 0 \Rightarrow \forall j \sum \mu_{ij} l_i = 0 \Rightarrow \forall (i,j), \mu_{ij} = 0. \end{cases}$$

□

Revenons au corps des racines, $\mathbb{L}$, de $X^3 + 2$, (Exemple 1.2.1). On peut le mettre sous la forme $\mathbb{L} = \mathbb{Q}[j]\,[\sqrt[3]{2}]$, d'où :

$$[\mathbb{L} : \mathbb{Q}] = [\mathbb{L} : \mathbb{Q}[j] \times [\mathbb{Q}[j] : \mathbb{Q}] = 3 \times 2 = 6.$$

car $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ est une base de $\mathbb{L}$ sur $\mathbb{Q}[j]$ et $\{1, j\}$ en est une de $\mathbb{Q}[j]$ sur $\mathbb{Q}$.

7.2.2 Extensions normales, séparables, galoisiennes

Rappelons quelques définitions.

Une extension (algébrique) est **normale** si toutes les racines d'un polynôme minimal d'un élément quelconque appartiennent à l'extension.

Contre-exemple : $\mathbb{Q}[\sqrt[3]{2}]$ n'est pas une extension normale de $\mathbb{Q}$ car elle ne contient que l'une des trois racines du polynôme minimal $X^3 - 2$, et non les deux autres, $\sqrt[3]{2}\exp(2i\pi/3)$ et $\sqrt[3]{2}\exp(4i\pi/3)$.

Une extension (algébrique) est **séparable** si tout élément est racine simple de son polynôme minimal. C'est le cas des extensions usuelles.

Contre-exemple : le corps des fractions de $\mathbb{F}_2[X]$ est une extension du corps des fractions de $\mathbb{F}_2[X^2]$, le polynôme minimal de X est $P(Z) = Z^2 - X^2$, qui n'a qu'une racine, $Z = \pm X$ (la caractéristique étant 2), d'ordre 2.

Si un polynôme P à coefficients dans un sous-corps de $\mathbb{C}$ a une racine multiple, on élimine cette multiplicité en divisant P par le pgcd de P et du polynôme

dérivé P'.

Enfin, une extension est **galoisienne** si elle est normale et séparable. Précisément, si les polynômes minimaux de ses éléments ont toutes leur racines dans l'extension, et si ces racines sont simples. Les deux contre-exemples précédents donnent donc des extensions non galoisiennes.

Notons que $\mathbb{R}$ est une extension (non algébrique) de $\mathbb{Q}$ de degré infini.

7.2.3 Groupe de Galois d'une extension

Un $\mathbb{K}$-**automorphismes** de $\mathbb{L} = \mathbb{K}(x_1, \ldots, x_n)$ est un automorphismes (de corps) de $\mathbb{L}$ dont la restriction à $\mathbb{K}$ est l'identité.

L'identité de $\mathbb{L}$ est un $\mathbb{K}$-automorphisme.

Si $(x_1, \ldots, x_k)$ sont les racines d'un polynôme minimal $P \in \mathbb{K}[X]$, donc invariant sous l'action d'un $\mathbb{K}$-automorphisme (qui conserve ses coefficients), celui-ci induit une permutation sur ces x_i, et, réciproquement, une permutation σ sur ces x_i se prolonge en un $\mathbb{K}$-automorphisme : si F est une fraction rationnelle, on pose $\sigma(F) = F(\sigma)$, ce qui respecte les relations symétriques entre les racines. Ainsi, par exemple, $\sigma(x_1/x_2) = \sigma(x_1)/\sigma(x_2)$. Or tout élément de l'extension est une fraction rationnelle en les (x_i).

Si les x_i sont les racines de plusieurs polynômes minimaux, un $\mathbb{K}$-automorphisme induit une permutation sur les racines de chaque polynôme, et réciproquement.

Deux automorphismes coïncidant sur les x_i sont égaux.

Il peut ne pas y avoir de $\mathbb{K}$-automorphisme σ tel que $\sigma(x_i) = x_j$, pour un couple donné. Si par exemple $\mathbb{L} = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, il n'existe pas de $\mathbb{Q}$-automorphisme σ tel que $\sigma(\sqrt{2}) = \sqrt{3}$, car $2 = \sigma(2) = \sigma((\sqrt{2})^2) = (\sigma(\sqrt{2}))^2 \neq 3$. Ces deux nombres ont des polynômes minimaux différents ($X^2 - 2$ et $X^2 - 3$).

L'étude des permutations est faite dans le chapitre *Déterminants* de *Systèmes et Matrices*, et dans le chapitre *Le groupe symétrique* $\mathfrak{S}_n$ de *Groupes,Anneaux, Corps*, de cette page web.

L'ensemble des $\mathbb{K}$-automorphismes d'une extension $\mathbb{L}$ de $\mathbb{K}$ est un groupe, le **groupe de Galois** de l'extension, noté $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$, dont la loi est évidemment la composition.

Le groupe de Galois $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ d'une extension galoisienne n'est réduit à l'identité que si $\mathbb{L} = \mathbb{K}$, car, sinon, il existe $x \in \mathbb{L}$, $x \notin \mathbb{K}$, de polynôme minimal P (irréductible, $\deg(P) \geq 2$), ayant une racine $y \neq x$ permettant de construire un $\mathbb{K}$-automorphisme σ tel que $\sigma(x) = y$.

La symétrie est un $\mathbb{Q}$-automorphisme de $\mathbb{Q}(\sqrt{2})$ car :

$$(X - \sqrt{2})(X + \sqrt{2}) = X^2 - 2 \in \mathbb{Q}[X]$$

et $X^2 - 2$ est le polynôme minimal de $\sqrt{2}$, mais elle (la symétrie) n'en est pas un de $\mathbb{Q}(\sqrt[3]{2})$ car $-\sqrt[3]{2}$ n'est pas une racine de $X^3 - 2$, polynôme minimal de $\sqrt[3]{2}$.

7.2.4 Element primitif

Un **élément primitif** d'une extension algébrique $\mathbb{L}$ de degré fini d'un corps $\mathbb{K}$ est un élément $a \in \mathbb{L}$ engendrant algébriquement $\mathbb{L}$ sur $\mathbb{K}$: $\mathbb{L} = \mathbb{K}(a)$.

Tout corps fini a trivialement un élément primitif.

Voici un critère de primitivité.

Proposition 7.3. *Soient $\mathbb{L}$ une extension de $\mathbb{K}$ de degré n et $\sigma_1, \ldots, \sigma_n$ ses K-automorphismes. Un élément $\alpha \in \mathbb{L}$ est primitif si et seulement si les $\sigma_i(\alpha)$ sont deux à deux distincts.*

Démonstration. Si les $\sigma_i(\alpha)$ sont deux à deux distincts, ce sont a et tous ses conjugués, et le produit P des $X - \sigma_i(\alpha)$ est le polynôme minimal de α, de degré n :

$$P = X^n + \lambda_1 X^{n-1} + \cdots + \lambda_n.$$

Les puissances α^i, $0 \leq i \leq n-1$ sont linéairement indépendantes car une relation de dépendance donnerait un polynôme de degré inférieur à n. Elles donnent donc une base de $\mathbb{L}$ sur $\mathbb{K}$, et α est un élément primitif.

Réciproquement, supposons α élément primitif et $\sigma_i(\alpha) = \sigma_j(\alpha)$; $\sigma_j^{-1} \circ \sigma_i$ est un $\mathbb{K}$-automorphisme, égal à l'identité sur α, donc sur $\mathbb{L}$, et $\sigma_j = \sigma_i$. □

Nous allons avoir besoin du lemme :

Lemme 7.1. *La réunion d'un nombre fini n de sous-espaces vectoriels est un espace vectoriel si et seulement si l'un d'entre eux contient tous les autres.*

Démonstration. La propriété est bien connue si $n = 2$: A et B sont deux sous-espaces vectoriels d'un espace vectoriel E, $A \neq B$. On suppose que leur réunion est un espace vectoriel S. Si aucun des espaces ne contient l'autre, il existe $a \in A$, $a \notin B$, et $b \in B$, $b \notin A$. Quels que soient les scalaires λ et μ tels que $\lambda + \mu = 1$, $D = \{\lambda a + \mu b\}$ est une droite affine contenue dans S, mais ni dans A ni dans B. Or $D \cap A = \{a\}$ et $D \cap B = \{b\}$ (si un espace vectoriel contient plus d'un point d'une droite, il la contient toute), de sorte que $D \cap S = \{a, b\}$, ce qui est absurde.

On suppose la propriété démontrée pour $n-1$ sous-espaces vectoriels A_i, $1 \leq i \leq n-1$ et on ajoute le sous-espace vectoriel A_n. On suppose que la réunion des A_i, $1 \leq i \leq n$, est un espace vectoriel S, et soit B le sous-espace vectoriel engendré par les A_i, $1 \leq i \leq n-1$. On sait que l'un des deux espaces, A_n ou B, contient l'autre. Si c'est A_n, on a gagné. Si c'est B, on applique l'hypothèse de récurrence : l'un des A_i, $1 \leq i \leq n-1$, A_j, contient les autres, et on est ramené au cas $n = 2$, avec A_j et A_n. □

Théorème 7.1 (de l'élément primitif)**.** *Toute extension algébrique $\mathbb{L}$ d'un corps $\mathbb{K}$ (de caractéristique 0), de degré fini n, admet un élément primitif.*

Démonstration. Considérons tous les couples de $\mathbb{K}$-automorphismes distincts (σ_i, σ_j), et les sous-espaces vectoriels :

$$L_{ij} = \{x \in \mathbb{L} \,|\, \sigma_i(x) = \sigma_j(x)\}.$$

La réunion des L_{ij} ne peut être égale à $\mathbb{L}$ (lemme 7.1), elle est d'ailleurs de mesure nulle et son complémentaire est partout dense. Nous pouvons donc choisir un élément $\alpha \in \mathbb{L}$ n'appartenant à aucun des L_{ij} dont les images $\sigma_i(\alpha)$ (deux à deux distinctes et conjuguées de α). Comme $\mathbb{L}$ a n $\mathbb{K}$-automorphismes, a est au moins de degré n, $[\mathbb{K}(a) : \mathbb{K}] \geq n$, $[\mathbb{L} : \mathbb{K}(a)] \leq 1$, et donc $\mathbb{K}(a) = \mathbb{L}$. □

Corollaire : $\mathbb{K}(a_1, \ldots, a_n) = \mathbb{K}[a_1, \ldots, a_n]$.

Démonstration. Soit α un élément primitif :

$$\mathbb{K}(a_1, \ldots, a_n) = \mathbb{K}(\alpha) = \mathbb{K}[\alpha] = \mathbb{K}[a_1, \ldots, a_n]. \qquad \square$$

Théorème 7.2. *Le nombre de $\mathbb{K}$-automorphismes d'une extension galoisienne $\mathbb{L}$ est égal à son degré.*

Démonstration. Soient α un élément primitif de $\mathbb{L}$, corps de décomposition d'un polynôme irréductible de $\mathbb{K}[X]$, et $P = \sum \lambda_i X^i$, $\deg(P) = n$, le polynôme minimal de α. Les α^i, $0 \leq i \leq n-1$ constituent une base de $\mathbb{L} = \mathbb{K}[a]$, car :
- d'une part, ils sont linéairement indépendants, une relation de dépendance donnerait un polynôme minimal de degré inférieur à celui de P,
- d'autre part ils engendrent $\mathbb{L}$ par définition de $\mathbb{K}[\alpha]$.

Si $\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})$, $\sigma(\alpha)$ et α sont conjugués :

$$P(\sigma(\alpha)) = \sum \lambda_i (\sigma(\alpha))^i = \sum \sigma(\lambda_i \alpha^i) = \sigma(\sum \lambda_i \alpha^i) = \sigma(P(\alpha)) = 0$$

puisque $\lambda_i = \sigma(\lambda_i)$. Comme deux $\mathbb{K}$-automorphismes de $\mathbb{K}[\alpha]$ qui coïncident sur α sont égaux, il y en a n $(\sigma_1, \ldots, \sigma_n)$, et $|\mathrm{Gal}(\mathbb{L}/\mathbb{K})| = n = [\mathbb{L} : \mathbb{K}]$.

Si $\mathbb{L}$ est le corps de décomposition d'un polynôme produit de deux polynômes irréductibles S et T, alors $\mathbb{L} = \mathbb{K}[S]\,[T]$.

D'une part, nous savons (proposition 7.2) que $[\mathbb{L} : \mathbb{K}] = [\mathbb{L} : \mathbb{K}[S]]\,[\mathbb{K}[S] : \mathbb{K}]$.

D'autre part, $\mathrm{Gal}(\mathbb{L}/\mathbb{K}) = \mathrm{Gal}(\mathbb{L}/\mathbb{K}[S]) \times \mathrm{Gal}(\mathbb{K}[S]/\mathbb{K})$, un $\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})$ étant le composé d'un $\sigma' \in \mathrm{Gal}(\mathbb{L}/\mathbb{K}[S])$ et d'un $\sigma'' \in |\mathrm{Gal}(\mathbb{K}[S]/\mathbb{K})$, d'où $|\mathrm{Gal}([\mathbb{L}/\mathbb{K})| = [\mathbb{L} : \mathbb{K}]$, et, par récurrence, le résultat pour le corps de décomposition d'un produit fini de polynômes irréductibles. □

Exemple 7.2. L'extension $\mathbb{Q}[\sqrt[3]{2}]$, non galoisienne, est de degré 2, une base étant $\{1, \sqrt[3]{2}\}$, et n'a qu'un seul $\mathbb{Q}$-automorphisme, l'identité.

Les $\mathbb{Q}$-automorphismes du corps de décomposition $\mathbb{L}$ du polynôme $X^3 + 2$ (Exemple 1.2.1), extension galoisienne de $\mathbb{Q}$, sont, si l'on note a, b et c les racines $(a + b + c = 0)$, outre l'identité σ_1 :

$$\begin{array}{ll} \sigma_2 : (a,b,c) \mapsto (b,a,c), & \sigma_3 : (a,b,c) \mapsto (c,b,a), \\ \sigma_4 : (a,b,c) \mapsto (a,c,b), & \sigma_5 : (a,b,c) \mapsto (b,c,a), \\ \sigma_6 : (a,b,c) \mapsto (c,a,b). & \end{array}$$

L'ordre de son groupe de Galois est égal à son degré (6).

Exemple 7.3. Le corps $\mathbb{L} = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ est une extension galoisienne de $\mathbb{Q}$. L'élément $\sqrt{6} = \sqrt{2}\sqrt{3}$ n'est pas engendré vectoriellement par 1, $\sqrt{2}$ et $\sqrt{3}$, qui ne forment donc pas une base, mais $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ en est une, et $[\mathbb{L} : \mathbb{Q}] = 4$.

L'élément $\alpha = \sqrt{2} + \sqrt{6}$ est primitif, car $\alpha^2 = 4(\sqrt{3} + 2)$ et :

$$\sqrt{3} = \frac{\alpha^2 - 8}{4}, \quad , \sqrt{2} = \frac{\alpha^2 - 4}{2\alpha}, \quad \sqrt{6} = \frac{\alpha^4 - 12\alpha^2 + 32}{8\alpha}.$$

Comme $\alpha^4 = 16\alpha^2 - 16$, son polynôme minimal est $P = X^4 - 16X^2 + 16$, dont les racines sont $\pm(\sqrt{2} \pm \sqrt{3})$. Il est irréductible sur $\mathbb{Q}$:

$$X^4 - 16X^2 + 16 = (X^2 - 8 + 4\sqrt{3})(X^2 - 8 - 4\sqrt{3}),$$

et $\mathbb{L} = \mathbb{Q}(\alpha) = \text{vect}(1, \alpha, \alpha^2, \alpha^3) = \mathbb{Q}[\alpha]$.

A partir de P et de la relation de Bézout, on peut trouver un polynôme $A \in \mathbb{Q}[X]$ tel que $\sqrt{2} = A(\alpha)$.

Soit N/D une fraction rationnelle. Si P et D sont premiers entre eux, il existe des polynômes U et V tels que $UD - PV = 1$.

C'est le cas avec $P = X^4 - 16X^2 + 16$ et $D = X$:

$$\frac{1}{64}((X^5 - 20X^3 + 80X)X - (X^2 - 4)(X^4 - 16X^2 + 16)) = 1,$$

d'où $UD \equiv 1 \mod P$. En $X = \alpha$, et modulo $P(\alpha)$, on arrive à :

$$\sqrt{2} = \frac{N}{D} = \frac{N}{D}UD = NU = \frac{1}{8}(\alpha^3 - 12\alpha), \ \sqrt{6} = \alpha - \sqrt{2} = \frac{1}{8}(-\alpha^3 + 20\alpha).$$

Les corps $\mathbb{Q}(\sqrt{2})$ et $\mathbb{Q}(\sqrt{3})$ sont des **corps de rupture** (d'ordre 2) du polynôme $Q = X^4 - 5X^2 + 6$, c'est-à-dire dans lequel Q a des racines, respectivement, $\pm\sqrt{2}$ et $\pm\sqrt{3}$, et $\mathbb{L}$ est son **corps de décomposition**, ou *corps des racines* (d'ordre 4), c'est-à-dire engendré sur $\mathbb{Q}$ par toutes ses racines. C'est une exension des deux précédents :

$$\mathbb{L} = [\mathbb{Q}(\sqrt{3})]\,[\sqrt{2}] = \mathbb{Q}[\sqrt{2}]\,[\sqrt{3}].$$

Ces trois extensions de $\mathbb{Q}$ sont galoisiennes.

Les $\mathbb{Q}$-automorphismes de $\mathbb{Q}[\sqrt{2}]$ sont l'identité et la symétrie ($\sqrt{2} \leftrightarrows -\sqrt{2}$), ceux de $\mathbb{Q}[\sqrt{3}]$ sont l'identité et la symétrie ($\sqrt{3} \leftrightarrows -\sqrt{3}$), et ceux de $\mathbb{L}$ sont définies par :

$$\begin{cases} a \ : \ a(\sqrt{2}) = -\sqrt{2}, \ a(\sqrt{3}) = \sqrt{3}, \\ b \ : \ b(\sqrt{2}) = \sqrt{2}, \ b(\sqrt{3}) = -\sqrt{3}, \\ c \ : \ c(\sqrt{2}) = -\sqrt{2}, \ c(\sqrt{3}) = -\sqrt{3}, \\ e \ \text{ est l'identité} \end{cases}$$

et le groupe de Galois $\text{Gal}(\mathbb{L}/\mathbb{Q})$, d'ordre 4, est le groupe de Klein, commutatif, donc résoluble.

Remarquons la bijection entre les sous-groupes de $\text{Gal}(\mathbb{L}/\mathbb{Q})$ et les corps intermédiaires, de $\mathbb{Q}$ à $\mathbb{L}$:

- $\mathbb{Q}(\sqrt{3})$ est le corps des invariants par a,
- $\mathbb{Q}(\sqrt{2})$ est le corps des invariants par b,
- $\mathbb{Q}$ est le corps des invariants par c,
- $\mathbb{L}$ est le corps des invariants par e. ▽

Exemple 7.4. Reprenons l'extension $\mathbb{L} = \mathbb{Q}[\sqrt[3]{2}]$, qui n'est pas normale, donc pas galoisienne, de degré 3 : $\mathbb{L} = \text{vect}_{\mathbb{Q}}(1, \sqrt[3]{2}, \sqrt[3]{4})$. L'unique $\mathbb{Q}$-automorphisme est l'identité. La symétrie n'en est pas un car $\sqrt[3]{2}$ n'a pas de conjugué ($-\sqrt[3]{2}$ appartient à $\mathbb{L}$, mais n'est pas conjugué de $\sqrt[3]{2}$).

Bien que n'étant pas dans $\mathbb{Q}$, $\sqrt[3]{2}$ est invariant par $\mathbb{Q}$-automorphisme. ▽

Proposition 7.4. *Une extension galoisienne d'une extension galoisienne est galoisienne.*

Démonstration. Soient $\mathbb{L}$ une extension galoisienne de $\mathbb{K}$ et $\mathbb{M}$ une extension galoisienne de $\mathbb{L}$. Le polynôme minimal sur $\mathbb{K}$ d'un élément quelconque x de $\mathbb{M}$, $P_{\mathbb{K}}$ de degré p, appartient à $\mathbb{L}[X]$, il est donc multiple du polynôme minimal $P_{\mathbb{L}}$ de x sur $\mathbb{L}$, de degré q, et il a $p+q$ racines, deux à deux distinctes : $\mathbb{M}$ est séparable sur $\mathbb{K}$. L'extension $\mathbb{M}$ de $\mathbb{K}$ est donc normale et séparable. □

Proposition 7.5. *Si $\mathbb{L}$ est une extension galoisienne de degré fini de $\mathbb{K}$, c'est une extension galoisienne de toute extension intermédiaire.*

Démonstration. Soient $\mathbb{H}$ une extension intermédiaire, α un élément primitif de $\mathbb{L}$, P le polynôme unitaire primitif de α, dont le corps de décomposition est $\mathbb{L}$. Comme $\mathbb{K} \subset \mathbb{H}$, P est dans $\mathbb{H}[X]$, et donc $\mathbb{L}$ est une extension galoisienne de $\mathbb{H}$. Certaines racines de P pouvant être dans $\mathbb{H}$, on a $[\mathbb{L} : \mathbb{H}] \leq [\mathbb{L} : \mathbb{K}]$. □

7.2.5 Groupe de Galois d'un polynôme

Soit P, un polynôme de $K[X]$, irréductible, de degré n, dont les racines (x_i) sont deux à deux distinctes. Son corps de décomposition, $\mathbb{L}$, est une extension galoisienne de $\mathbb{Q}$.

Exemple 7.5. Le polynôme $P = X^4 - 2 \in \mathbb{Q}[X]$ a quatre racines, $x_1 = \sqrt[4]{2}$, $x_2 = i\sqrt[4]{2}$, $x_3 = -\sqrt[4]{2}$ et $x_4 = -i\sqrt[4]{2}$, algébriques sur $\mathbb{Q}$, que nous plaçons dans $\mathbb{C}$, aux sommets d'un carré. Les x_i n'engendrent pas vectoriellement $\mathbb{L}$, car toute combinaison linéaire des x_i aura $\sqrt[4]{2}$ en facteur, et aucune ne pourra être égale à $i = x_2/x_1$. On a $\mathbb{L} = \mathbb{Q}[i, i\sqrt[4]{2}]$, d'où :

$$[\mathbb{L} : \mathbb{Q}] = [\mathbb{Q}[i\sqrt[4]{2}] : \mathbb{Q}[i]] \times [\mathbb{Q}[i] : \mathbb{Q}] = 4 \times 2 = 8.$$

et l'extension $\mathbb{L} = \mathbb{Q}(x_i)$, corps de décomposition de P, est galoisienne, de degré 8. Un $\mathbb{Q}$-automorphisme de $\mathbb{L}$ doit être une isométrie du carré ci-dessus. Nous obtenons donc les quatre rotations et les quatre symétries. Son groupe de Galois est est le groupe diédral D_4 d'ordre 8, sous-groupe du groupe des permutations des racines, $\mathfrak{S}_4$, résoluble.

L'élément $a = i + \sqrt[4]{2}$ est primitif, car, à partir de $(a-i)^4 = 2$, soit :

$$a^4 - 4ia^3 - 6a^2 + 4ia + 1 = 2$$

on déduit :

$$i = \frac{a^4 - 6a^2 - 1}{4(a^3 - a)}, \text{ et } \sqrt[4]{2} = a - i = \frac{3a^4 + 6a^2 - 4a + 1}{4(a^3 - a)}. \qquad \triangledown$$

Le lemme suivant sera utile pour l'étude de certains polynômes de degré 5.

Lemme 7.2. *Un sous-groupe S de $\mathfrak{S}_5$ ayant un élément d'ordre 5 et un élément d'ordre 2 est égal à $\mathfrak{S}_5$, donc non résoluble.*

Démonstration. Nommons τ le 2-cycle et σ le 5-cycle. Les $\sigma^p(i)$, $1 \leq p \leq 5$, sont deux à deux distincts. En effet, si $\sigma^p(i) = \sigma^q(i)$, $1 \leq p < q \leq 5$, on aurait $\sigma^{q-p}(i) = i$, et donc $\sigma^k(i) = i$, $1 \leq k \leq 5$, puisque σ^{q-p} engendre le groupe cyclique d'ordre 5 des σ^k. Mais alors σ serait une permutation de $\mathfrak{S}_4$. Quitte à changer la numérotation, on peut supposer que $\tau = (1, 2)$.

On pose $\alpha_k = \sigma^k \circ \tau \circ \sigma^{-k}$, et on vérifie immédiatement que les α_k sont des 2-cycle ($\alpha_k \circ \alpha_k$ est l'identité). Ces 2-cycles sont deux distincts, car, suivant les valeurs de k :

$$\begin{cases} \sigma^{-k}(1) = 1 \Rightarrow \alpha_k(1) = \sigma^k(2), \\ \sigma^{-k}(1) = 2 \Rightarrow \alpha_k(1) = \sigma^k(1), \\ \sigma^{-k}(1) = 3 \Rightarrow \alpha_k(1) = \sigma^k(3), \\ \sigma^{-k}(1) = 4 \Rightarrow \alpha_k(1) = \sigma^k(4), \\ \sigma^{-k}(1) = 5 \Rightarrow \alpha_k(1) = \sigma^k(5), \end{cases}$$

et ces 2-cycles sont de la forme $(1, j)$, $1 \leq j \leq 5$. Ils engendrent tous les 2-cycles car $(p, q) = (1, q) \circ (1, p)$, dont on sait qu'ils engendrent $\mathfrak{S}_5$. $\square$

Exemple 7.6. Considérons le polynôme $P = X^5 - 5X + 1 \in \mathbb{Q}[X]$. Son polynôme dérivé $P' = 5(X^2 + 1)(X^2 - 1)$ n'a pas de racine commune avec P ; P' a deux racines réelles, ± 1, il est positif à l'extérieur et négatif à l'intérieur, $P(-1) = 5$ est un maximum, $P(1) = -3$ est un minimum ; P a donc trois racines réelles $x_1 < -1$, $x_2 \in]0, 1[$ et $x_3 > 1$, et deux racines complexes conjuguées $x_4 = x + iy$ et $x_5 = x - iy$, $y \neq 0$.

Comme :

$$P(X - 1) = X^5 - 5X^4 + 10X^3 - 10X^2 + 5$$

P est irréductible sur $\mathbb{Q}[X]$ d'après le critère d'Eisenstein (voir l'exercice 14 dans *Corps de caractéristique finie*), les coefficients, sauf le premier, étant multiples de 5, et le dernier n'étant pas multiple de 5^2. Il est donc polynôme minimal des x_i, et $\mathbb{L}$ est une extension séparable et normale, donc galoisienne, de $\mathbb{Q}$. Le groupe des permutations sur ces racines est $\mathfrak{S}_5$, non résoluble. $\triangledown$

7.2.6 Extensions cycliques

Une extension galoisienne dont le groupe de Galois est cyclique est dite **cyclique**.

Soient $P = X^n - a$, $\mathbb{K} = \mathbb{Q}(i)$, $a \in \mathbb{Q}$, $b \in \mathbb{C}$ tel que $b^n = a$ et $\xi = \exp(2i\pi/n)$. Les $\xi^k b$, $0 \leq k \leq n-1$, dans $\mathbb{K}[b]$, extension algébrique de $\mathbb{K}$ de degré n (puisque $b^n = a$) sont les n racines de P. Le $\mathbb{K}$-automorphisme défini par $\sigma(x) = \xi x$ engendre le groupe de Galois de $\mathbb{K}[b]$ sur $\mathbb{K}$, qui est donc cyclique, isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Exemple 7.7. Ainsi, $P = X^4 - 6$, irréductible sur $\mathbb{K} = \mathbb{Q}[i]$, a pour corps de décomposition $\mathbb{L} = \mathbb{K}(\sqrt[4]{6})$, l'application $\sqrt[4]{6}) \mapsto i\sqrt[4]{6}$ se prolonge en un $\mathbb{K}$-automorphisme σ, et :

$$\mathrm{Gal}(\mathbb{L}/\mathbb{K}) = \{i_d, \sigma, \sigma^2, \sigma^3\} \cong \mathbb{Z}/4\mathbb{Z}.$$

Le corps $\mathbb{Q}(\sqrt[4]{6})$, qui ne contient que deux racines de P, est corps de rupture.

Bien que $P = X^4 - 9$ ne soit pas irréductible, son corps de décomposition $\mathbb{L} = \mathbb{Q}(i, \sqrt{3})$ est encore une extension cyclique de $\mathbb{Q}$, de degré 4.

Les $\mathbb{Q}$-automorphismes sont définis par $\sigma_k(\sqrt{3}) = i^k\sqrt{3}$, $0 \leq k \leq 3$, et $\{1, i, \sqrt{3}, i\sqrt{3}\}$ est une base sur $\mathbb{Q}$. ▽

7.2.7 Extensions radicales, tours radicales

Une **extension radicale** est une extension par une racine : $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[i\sqrt{2}$, sont des extensions radicales de $\mathbb{Q}$.

Une suite $\mathbb{K} = \mathbb{K}_0 \subset \mathbb{K}_1 \subset \ldots \subset \mathbb{K}_n$ dans laquelle chaque K_i est une extension radicale de $\mathbb{K}_{i-1}$, $1 \leq i \leq n$, est une **tour radicale**.

On peut associer une telle tour radicale à un polynôme dont les racines sont simples.

Exemple 7.8. Considérons le polynôme $X^7 - 2X^4 - 3X^3 + 6$ de $\mathbb{Q}[X]$, dont $\sqrt[3]{2}$ est une racine. L'extension $\mathbb{Q}_1 = \mathbb{Q}[j]$ est une extension radicale de $\mathbb{Q}$ ($j = \sqrt[3]{1}$), d'ordre 2. De même, $\mathbb{Q}_2 = \mathbb{Q}_1[i]$ est une extension radicale de $\mathbb{Q}_1$, d'ordre 2. $\mathbb{Q}_3 = \mathbb{Q}_2[\sqrt[3]{2}]$, qui contient les racines conjuguées de la première, est une extension radicale de $\mathbb{Q}_2$, d'ordre 3 (de base $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$).

Une autre racine étant $\sqrt[4]{3}$, l'extension $\mathbb{Q}_4 = \mathbb{Q}_3[\sqrt[4]{3}]$, extension radicale de $\mathbb{Q}_3$ d'ordre 4 (de base $\{1, \sqrt[4]{3}, \sqrt[4]{9}, \sqrt[4]{27}\}$), contient les quatre autres racines.

Ces extensions sont cycliques.Nous avons ainsi construit la *tour radicale* $(\mathbb{Q}, \mathbb{Q}_1, \mathbb{Q}_2, \mathbb{Q}_3, \mathbb{Q}_4)$. Nous avons $\mathbb{Q}_4 = \mathbb{Q}[\sqrt[3]{2}, \sqrt[4]{3}, \xi]$. $\xi = \exp(i\pi/6) = -ij$ remplaçant i et j, puisque $\xi^3 = i$ et $\xi^4 = j$. C'est une extension d'ordre 48 de $\mathbb{Q}$. ▽

Exemple 7.9. Considérons une suite $(a_1, \ldots, a_n)$ de nombres complexes et supposons qu'il existe une suite de rationnels (b_i) et une suite d'entiers (r_i), telles que $a_i^{r_i} = b_i$.

Soient r le ppcm des r_i, $r = d_i r_i$, $\xi = \exp(2i\pi/r)$ et $\mathbb{K} = \mathbb{Q}[\xi]$. Supposons de plus que a_i soit l'unique racine de $X^{r_i} - b_i$ dans la suite $(a_1, \ldots, a_n)$, les autres étant les $a_i(\xi^{d_i})^k$, $1 \leq k \leq r_i$.

Comme précédemment, construisons l'**extension radicale** $\mathbb{K}_1$ de $\mathbb{K}$ contenant les racines de $X^{r_1} - b_1$, puis $\mathbb{K}_2$, extension radicale de $\mathbb{K}_1$ contenant les racines de $X^{r_2} - b_1$...

On construit ainsi une suite $\mathbb{K}_i$ d'extensions radicales, $\mathbb{K}_i$ étant une extension radicale de $\mathbb{K}_{i-1}$, $1 \leq i \leq n$, $\mathbb{K}_0 = \mathbb{K}$, $\mathbb{K}_n = \mathbb{K}[a_1, \ldots, a_n]$. Ainsi, à partir d'une suite $(a_1, \ldots, a_n)$, on obtient une **tour radicale** $\mathbb{K}[a_1, \ldots, a_n]$. $\triangledown$

Un polynôme $P \in \mathbb{K}[X]$ est résoluble par radicaux si et seulement s'il existe une tour radicale $\mathbb{L}$ de $\mathbb{K}$ contenant son corps de décomposition (ses racines). Rappelons que $\mathbb{Q} \subset \mathbb{K} \subset \mathbb{L} \subset \mathbb{C}$.

Nous verrons un peu plus loin que P est résoluble par radicaux si et seulement si le groupe $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ est résoluble.

7.2.8 Correspondance et théorème de Galois

Le théorème d'Abel assure l'existence d'équations de degré supérieur ou égal à 5, à coefficients complexes, non résolubles par radicaux. C'est une conséquence du théorème de Galois, plus général, que nous allons démontrer.

Hypothèses : $\mathbb{L}$ est une extension galoisienne de degré fini de $\mathbb{K}$ (en général $\mathbb{Q}$ ou une extension), Λ est l'ensemble des extensions intermédiaires, notées $\mathbb{K}_i$, croissantes avec i :

$$\mathbb{K} = \mathbb{K}_0 \subset \mathbb{K}_1 \subset \mathbb{K}_2 \subset \ldots \subset \mathbb{K}_n \subset \mathbb{L},$$

Γ est l'ensemble des sous-groupes $G_i = \mathrm{Gal}(\mathbb{L}/\mathbb{K}_i)$ de $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$, décroissants avec i :

$$\mathrm{Gal}(\mathbb{L}/\mathbb{K}_0) \supset \mathrm{Gal}(\mathbb{L}/K_1) \supset \mathrm{Gal}(\mathbb{L}/\mathbb{K}_2) \ldots \supset \mathrm{Gal}(\mathbb{L}/\mathbb{L}) = \{i_d\}.$$

Remarquons que si H est un sous-groupe de G =$\mathrm{Gal}(\mathbb{L}/\mathbb{K})$, l'ensemble :

$$\mathbb{K}_H = \{x \in \mathbb{L} \,|\, \forall \sigma \in H \,:\, \sigma(x) = x\}$$

est un corps, donc un sous-corps de $\mathbb{L}$, contenant $\mathbb{K}$, c'est-à-dire l'un des $\mathbb{K}_i$, soit $\mathbb{K}_j$; H est son groupe de Galois sur $\mathbb{K}$, donc G_j.

Le sous-corps $\mathbb{K}_{G_i}$ de $\mathbb{L}$ est une extension de $\mathbb{K}$, décroissant avec i, dont G_i est le groupe de Galois.

Définissons les applications strictement décroissantes pour l'inclusion :

$$\begin{array}{rccc} u: & \Lambda & \to & \Gamma \\ & \mathbb{K}_i & \mapsto & \mathrm{Gal}(\mathbb{L}/\mathbb{K}_i). \end{array}$$

et :

$$\begin{array}{rccc} v: & \Gamma & \to & \Lambda \\ & G_i & \mapsto & \mathbb{K}_{G_i} \end{array}$$

$\mathbb{K}_{G_i}$ étant le corps des invariants de G_i.

Théorème 7.3 (Correspondance de Galois)**.** *Dans la situation ci-dessus, u et v sont des bijections réciproques.*

Démonstration. A chaque corps intermédiaire correspond un sous-groupe, et à chaque sous-groupe correspond un corps intermédiaire ; l'application $\mathbb{K}_i \mapsto G_i$ est bijective, et $\mathbb{K}_{G_i} = \mathbb{K}_i$. □

Si $\mathbb{L}$ et $\mathbb{H}$ sont des extensions galoisiennes de $\mathbb{K}$, $\mathbb{H} \subset \mathbb{L}$, tout $\mathbb{K}$-automorphisme σ de $\mathbb{H}$ peut être prolongé en un certain nombre de $\mathbb{K}$-automorphisme de $\mathbb{L}$, qui, par restriction à $\mathbb{H}$, redonnent σ. Cette restriction définit un morphisme surjectif de groupes :

$$\phi : \mathrm{Gal}(\mathbb{L}/\mathbb{K}) \to \mathrm{Gal}(\mathbb{H}/\mathbb{K}),$$

dont le noyau est un sous-groupe invariant (voir 2.11, exercice (2)).

Proposition 7.6. *Dans cette situation, Gal*$(\mathbb{L}/\mathbb{H})$ *est un sous-groupe invariant de Gal*$(\mathbb{L}/\mathbb{K})$*, et le groupe quotient Gal*$(\mathbb{L}/\mathbb{K})/$*Gal*$(\mathbb{L}/\mathbb{H})$ *est isomorphe à Gal*$(\mathbb{H}/\mathbb{K})$*.*

Démonstration. Montrons que $\mathrm{Ker}(\phi)$ est isomorphe à $\mathrm{Gal}(\mathbb{L}/\mathbb{H})$.

On a $\phi(\sigma) = \sigma'$ si et seulement si σ prolonge σ', et $\phi(\sigma) = i_d$ signifie que σ appartient à $\mathrm{Gal}(\mathbb{L}/\mathbb{H})$; réciproquement, si σ est un $\mathbb{H}$-automorphisme, $\phi(\sigma)$ est l'identité de $\mathbb{H}$; $\mathrm{Ker}\phi$ est donc isomorphe à $\mathrm{Gal}(\mathbb{L}/\mathbb{H})$.

Enfin, ϕ étant surjectif, $\mathrm{Im}(\phi) = \mathrm{Gal}(\mathbb{H}/\mathbb{K})$ est isomorphe à $\mathrm{Gal}(\mathbb{L}/\mathbb{K})/\mathrm{Ker}(\phi)$, donc à $\mathrm{Gal}(\mathbb{L}/\mathbb{K})/\mathrm{Gal}(\mathbb{L}/\mathbb{H})$. □

Proposition 7.7. *Si* $\mathbb{H}$ *et* $\mathbb{H}' \subset \mathbb{H}$ *sont des extensions intermédiaires, on a Gal*$(\mathbb{L}/\mathbb{K})/$*Gal*$(\mathbb{L}/\mathbb{H}) \cong$ *Gal*$(\mathbb{H}/\mathbb{H}')$*.*

Démonstration. Il suffit de remplacer $\mathbb{K}$ par $\mathbb{H}'$ dans la proposition précédente. □

Exemple 7.10. Soit $\mathbb{L} = \mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{5}]$ une extension galoisienne de $\mathbb{Q}$. Posons $\mathbb{Q}_1 = \mathbb{Q}[\sqrt{2}]$ et $\mathbb{Q}_2 = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$, I désignant le groupe trivial.

Les $\mathbb{K}$-automorphismes ($\mathbb{K} = \mathbb{Q}, Q_1, Q_2$) sont composés de symétries sur les radicaux, d'où les $\mathbb{Z}/2\mathbb{Z}$.

Les $\mathbb{Q}$-automorphismes fixent les éléments de $\mathbb{Q}$ et agissent sur $\sqrt{2}$, $\sqrt{3}$ et $\sqrt{5}$, d'où $\mathrm{Gal}(\mathbb{L}/\mathbb{Q}) = G \cong (\mathbb{Z}/2\mathbb{Z})^3$; leurs invariants sont donc les éléments de $\mathbb{Q}$, et $\mathbb{Q}_G = \mathbb{Q}$.

Les $\mathbb{Q}_1$-automorphismes fixent les éléments de $\mathbb{Q}_1$ et agissent sur $\sqrt{3}$ et $\sqrt{5}$, d'où $\mathrm{Gal}(\mathbb{L}/\mathbb{Q}_1) = G_1 \cong (\mathbb{Z}/2\mathbb{Z})^2$; leurs invariants sont donc les éléments de $\mathbb{Q}_1$, et $\mathbb{Q}_{G_1} = \mathbb{Q}_1$.

Les $\mathbb{Q}_2$-automorphismes fixent les éléments de $\mathbb{Q}_2$ et agissent sur $\sqrt{5}$, d'où $\mathrm{Gal}(\mathbb{L}/\mathbb{Q}_2) = G_2 \cong \mathbb{Z}/2\mathbb{Z}$; leurs invariants sont donc les éléments de $\mathbb{Q}_2$, et $\mathbb{Q}_{G_2} = \mathbb{Q}_2$.

Les éléments invariants par I sont ceux de $\mathbb{L}$.

D'où la correspondance :

$$\begin{array}{cccccccc} & \mathbb{Q} & \subset & \mathbb{Q}_1 & \subset & \mathbb{Q}_2 & \subset & \mathbb{L} \\ u \downarrow & & & & & & & \\ & G & \subset & G_1 & \subset & G_2 & \subset & I \\ v \downarrow & & & & & & & \\ & \mathbb{Q}_G = \mathbb{Q} & \subset & \mathbb{Q}_{G_1} = \mathbb{Q}_1 & \subset & \mathbb{Q}_{G_2} = \mathbb{Q}_2 & \subset & \mathbb{Q}_I = \mathbb{L}. \end{array}$$

Les groupes-quotients sont isomorphes à $\mathbb{Z}/2\mathbb{Z}$. Ils sont donc cycliques d'ordre premier. ▽

Théorème 7.4 (Galois)**.** *Soient $P \in \mathbb{K}[X]$ et $\mathbb{L}$ son corps de décomposition. Les assertions suivantes sont équivalentes :*

(a) P est résoluble par radicaux,

(b) le groupe Gal($\mathbb{L}/\mathbb{K}$) est résoluble.

Démonstration. (a) ⇒ (b). Nous avons une tour radicale ($\mathbb{K}_i$) et les groupes de Galois G_i =Gal($\mathbb{L}/\mathbb{K}_i$) et H_i =Gal($\mathbb{K}_{i+1}/\mathbb{K}_i$). La suite des $\mathbb{K}_i$ est croissante, celle des G_i décroissante, comme celle des H_i. Nous savons (proposition précédente) que $G_i/G_{i+1} \cong H_i$, et que les H_i sont cycliques, donc commutatifs, ce qui signifie que G est résoluble.

(b) ⇒ (a). Si Gal($\mathbb{L}/\mathbb{K}$) = G_0 est résoluble, il existe une suite finie de groupes :

$$G_0 \supset G_1 \supset \dots G_n = \{i_d\},$$

dans laquelle G_{i+1} est un sous-groupe invariant de G_i et les quotients G_i/G_{i+1} sont cycliques d'ordre premier (théorème 2.5, page 15).

Posons, comme précédemment, $\mathbb{K}_i = \mathbb{K}_{G_i}$. De :

$$\mathrm{Gal}(\mathbb{K}_{i+1}/\mathbb{K}_i) \cong \mathrm{Gal}(\mathbb{L}/\mathbb{K}_i)/\mathrm{Gal}(\mathbb{L}/\mathbb{K}_{i+1}) \cong G_i/G_{i+1}$$

on déduit que Gal($\mathbb{K}_{i+1}/\mathbb{K}_i$) est cyclique d'ordre premier, et qu'il existe un élément $a_i \in \mathbb{K}_{i+1}$ et un nombre premier p_i tels que $a_i^{p_i}$ appartient à $\mathbb{K}_i$, d'où $\mathbb{K}_{i+1} = \mathbb{K}_i[a_i]$ et $\mathbb{L} = \mathbb{K}[(a_i)]$ est résoluble par radicaux. □

7.3 Exercices

(1) Montrer que $S = \sqrt{a} + \sqrt{b}$ ($\sqrt{a} \notin \mathbb{Q}$, $\sqrt{b} \notin \mathbb{Q}$) est un élément primitif de $\mathbb{L} = \mathbb{Q}[\sqrt{a}, \sqrt{b}]$. On pourra utiliser le produit $P = \sqrt{a}\sqrt{b}$ et la différence $D = a - b$.

(2) Donner le degré et un élément primitif de l'extension $\mathbb{L} = \mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{5}]$.

(3) Etudier l'extension $\mathbb{L} = \mathbb{Q}[\sqrt{p}, \sqrt[3]{p}]$, p premier.

(4) Même question en remplaçant p par $-p$.

(5) Corps de décomposition, élément primitif, degré et groupe de Galois de :
(a) X^6+1,
(b) X^6-1,
(c) $X^5+X^4+X^3+X^2+X+1$,
(d) X^8-1,
(e) X^5+1,
(f) $X^3-\pi$.
(6) Irréductibilité ou non (sur $\mathbb{Q}$) de :
(a) $P=X^5\pm X+1$,
(b) $Q=\sum_{0\leq i\leq p-1}X^i$, p premier.

(7) Extension galoisienne engendrée par :
(a) $\sqrt{2}+i$.
(b) $\sqrt{2}+\sqrt[3]{2}$,

(8) Corps des racines $\mathbb{L}$ du polynôme réciproque :

$$P=X^6+X^5+2X^4+2X^3+2X^2+X+1.$$

Donner une base sur $\mathbb{Q}$ de $\mathbb{L}$, son groupe de Galois G, les sous-corps de $\mathbb{L}$, les sous-groues de G, et la correspondance.

Vérifier que $a=i+(\sqrt{5}+1+i\sqrt{10-2\sqrt{5}})/4$ est un élément primitif.

(9) Etude complète du corps des racines $\mathbb{L}$ du polynôme $X^5+2X^3+2X^2+4$.

7.4 Correction des exercices

(1) Les racines du polynôme X^2-SX+P, c'est-à-dire $\sqrt{a}$ et $\sqrt{b}$, sont égales à $S/2\pm\sqrt{\Delta}$, $\Delta=S^2-4P=(\sqrt{a}-\sqrt{b})^2$. De $(\sqrt{a}-\sqrt{b})(\sqrt{a}+\sqrt{b})=D$, on déduit que les racines sont $\dfrac{S}{2}\pm\dfrac{D}{2S}$.

Les éléments $1,S,S^2$ sont libres.

Une combinaison linéaire sur $\mathbb{Q}$ $S^3=\alpha+\beta S+\gamma S^2=SS^2$ équivaut à $\alpha+\beta S+(\gamma-S)S^2=0$. Ceci implique $\alpha=\beta=0$ et $\gamma=S$, ce qui est absurde, car $S\notin\mathbb{Q}$.

Comme $[\mathbb{L}:\mathbb{Q}]=4$, les éléments $1,S,S^2,S^3$, qui sont libres, sont générateurs, forment une base de $\mathbb{L}$, et S est primitif.

(2) On a la tour radicale :

$$\mathbb{K}_0=\mathbb{Q}\subset\mathbb{K}_1=\mathbb{K}_0[\sqrt{2}]\subset\mathbb{K}_2=\mathbb{K}_1[\sqrt{3}]\subset\mathbb{K}_3=\mathbb{K}_2[\sqrt{5}]=\mathbb{L},$$

d'où $[\mathbb{L}:\mathbb{Q}]=2^3=8$ (proposition 8.1).

Les éléments 1, $\sqrt{2}$, $\sqrt{3}$,$\sqrt{5}$,$\sqrt{6}$,$\sqrt{10}$,$\sqrt{15}$ et $\sqrt{30}$ constituent une base de $\mathbb{L}$ sur $\mathbb{Q}$.

Les huit $\mathbb{Q}$-automorphismes de $\mathbb{L}$, avec l'identité σ_0, sont définis par :

$$\begin{cases} \sigma_1 : (\sqrt{2},\sqrt{3},\sqrt{5}) \mapsto (-\sqrt{2},\sqrt{3},\sqrt{5}), \\ \sigma_2 : (\sqrt{2},\sqrt{3},\sqrt{5}) \mapsto (\sqrt{2},-\sqrt{3},\sqrt{5}), \\ \sigma_3 : (\sqrt{2},\sqrt{3},\sqrt{5}) \mapsto (\sqrt{2},\sqrt{3},-\sqrt{5}), \\ \sigma_4 = \sigma_1 \circ \sigma_2,\ \sigma_5 = \sigma_1 \circ \sigma_3,\ \sigma_6 = \sigma_2 \circ \sigma_3, \\ \sigma_7 = \sigma_1 \circ \sigma_2 \circ \sigma_3 = -i_d. \end{cases}$$

Les images de $a = \sqrt{2}+\sqrt{3}+\sqrt{5}$ par ces $\mathbb{Q}$-automorphismes sont :

$$\begin{cases} \sigma_0(a) = \sqrt{2}+\sqrt{3}+\sqrt{5}, \\ \sigma_1(a) = -\sqrt{2}+\sqrt{3}+\sqrt{5}, \\ \sigma_2(a) = \sqrt{2}-\sqrt{3}+\sqrt{5}, \\ \sigma_3(a) = \sqrt{2}+\sqrt{3}-\sqrt{5}, \\ \sigma_4(a) = -\sqrt{2}-\sqrt{3}+\sqrt{5}, \\ \sigma_5(a) = -\sqrt{2}+\sqrt{3}-\sqrt{5}, \\ \sigma_6(a) = \sqrt{2}-\sqrt{3}-\sqrt{5}, \\ \sigma_7(a) = -\sqrt{2}-\sqrt{3}-\sqrt{5}, \end{cases}$$

et on vérifie immédiatement, en regardant les signes, qu'elles sont deux à deux distinctes ; a est donc primitif (proposition 2.1).

(3) Comme $\mathbb{L} = \mathbb{Q}[\sqrt{p}\,][\sqrt[3]{p}])$, on a $[\mathbb{L}:\mathbb{Q}] = 2\times 3 = 6$, et :

$$\mathfrak{B} = \{1, \sqrt{p}, \sqrt[3]{p}, \sqrt[3]{p^2}, \sqrt{p}\sqrt[3]{p}, \sqrt{p}\sqrt[3]{p^2}\}$$

est une base de $\mathbb{L}$ sur $\mathbb{Q}$. Les six $\mathbb{Q}$-automorphismes sont obtenus en composant les deux de $\mathbb{Q}[\sqrt{p}]$ et les trois de $\mathbb{Q}[\sqrt[3]{p}]$. On vérifie comme précédemment que $a = \sqrt{p}+\sqrt[3]{p}$ est primitif. Notons que $\mathbb{L}$ n'est pas galoisienne car il lui manque les deux racines complexes de $X^3 - p$.

(4) On a $\mathbb{Q}[\sqrt{-p}] = \mathbb{Q}[i,\sqrt{p}]$, de degré 4, et $\mathbb{Q}[\sqrt[3]{-p}] = \mathbb{Q}[j,\sqrt[3]{p}]$, de degré 6. Le degré de l'extension est donc 24. Elle admet $a = \sqrt{p}+\sqrt[3]{p}+i\sqrt{p}+i\sqrt[3]{p}$ comme élément primitif.

(5) Les extensions sont galoisiennes.

(a) $X^6+1 = (X^2+1)(X^4-X^2+1)$. Son corps de décomposition est $\mathbb{L}$.

Les racines de X^4-X^2+1 sont $\pm\exp(\pm i\pi/6)$ et celles de X^2+1 sont $\pm i$. Le corps $\mathbb{K}$ des racines de X^4-X^2+1 a quatre $\mathbb{Q}$-automorphismes, une base $\{1,\sqrt{3},i,i\sqrt{3}\}$, et $\mathbb{K} = \mathbb{Q}[i,\sqrt{3}]$. Il a un élément primitif $a = i+\sqrt{3}$ car, à partir de $(a-i)^2$, on obtient $\sqrt{3} = (a^2+4)/2a$ et $i = (a^2-4)/2a$. Les racines de X^2+1 étant dans $\mathbb{K}$, l'extension par X^2+1 ne change rien : $\mathbb{L} = \mathbb{K}$.

(b) $X^6-1=(X+1)(X-1)(X^2+X+1)(X^2-X+1)$.

Les racines non rationnelles sont $\pm j$ et $\pm\bar{j}$, et son corps des racines, $\mathbb{Q}[j,\sqrt{3}]$, a quatre $\mathbb{Q}$-automorphismes, une base $\{1,\sqrt{3},i,i\sqrt{3}\}$ et pour élément primitif, par exemple, $a=i+\sqrt{3}$; en effet, $(a-i)^2=3$, d'où $i=(a^2-4)/2a$ et $\sqrt{3}=(a^2+4)/2a$.

(c) $X^5+X^4+X^3+x^2+x+1=\dfrac{X^6-1}{X-1}=(X+1)(X^2\pm X+1)$.

Les racines de (X^2+X+1) sont j et $\bar{j}$ et celles de X^2-X+1 sont $-j$ et $-\bar{j}$, d'où $\mathbb{L}=\mathbb{Q}[i,\sqrt{3}]$, de base $\{1,i,\sqrt{3},i\sqrt{3}\}$ et d'élément primitif $a=i+\sqrt{3}$. Finalement, $X+1$ ne donnant que l'identité, le groupe de Galois de $\mathbb{L}$ est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$.

(d) $X^8-1=(X^4+1)(X^2+1)(X-1)(X+1)$.

Soit $\mathbb{K}$ le corps des racines de X^4+1, $\mathbb{K}=\mathbb{Q}[i,\sqrt{2}]$, extension de degré 4, une base étant $\{1,i,\sqrt{2},i\sqrt{2}\}$, et $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})\cong\mathbb{Z}/4\mathbb{Z}$. Ensuite, $\mathbb{L}$ est le corps des racines de X^2+1 sur $\mathbb{K}$, or les racines de X^2+1 sont dans $\mathbb{K}$, et l'extension est de degré 1. On a donc $[\mathbb{L}:\mathbb{Q}]=4\times1=4$.

Les quatre $\mathbb{Q}$-automorphismes de $\mathbb{L}$ sont $\sqrt{2}(1+i)\mapsto\sqrt{2}(\pm1\pm i)$.

Un élément primitif est $a=i+\sqrt{2}$, car, en élevant $a-i$ au carré, on trouve $i=(a^2-3)/2a$ et $\sqrt{2}=(a^2+3)/2a$.

(e) Les racines autres que -1 sont celles de $P=X^4+X^3+X^2+X+1$.

Remarquant que ce polynôme cyclothomique est réciproque, on est ramené, en le divisant par X^2, au degré 2 en $Y=X+1/X$. Les racines de Y^2+Y-1 sont $(-1\pm\sqrt{5})/2$, d'où celles de P, égales à $\exp(\pm i\pi/5)$ et $\exp(\pm3i\pi/5)$:

$$\begin{cases}x_1=\frac{1}{4}(\sqrt{5}+1+i\sqrt{10-2\sqrt{5}})=\cos(\pi/5)+i\sin(\pi/5),\\ x_2=\frac{1}{4}(-\sqrt{5}+1+i\sqrt{10+2\sqrt{5}})=\cos(3\pi/5)+i\sin(3\pi/5)\end{cases}$$

et $x_3=\overline{x_2}$, $x_4=\overline{x_1}$. D'où quatre $\mathbb{Q}$-automorphismes : $\sigma_i(x_1)=x_i$, $1\le i\le4$. L'extension est de degré 4, et $\{1,\sqrt{5},i\sqrt{10-2\sqrt{5}},i\sqrt{10+2\sqrt{5}}\}$ en est une base.

On a $\mathbb{L}=\mathbb{Q}[i,\sqrt{5},\sqrt{10-2\sqrt{5}}\,]$, puisque :

$$\sqrt{10+2\sqrt{5}}=\frac{4\sqrt{5}}{\sqrt{10-2\sqrt{5}}}.$$

A partir de la définition des $\mathbb{Q}$-automorphismes, nous voyons que x_1 est un élément primitif , les $\sigma_i(x_1)$ étant distincts. On peut également remarquer que $x_2=x_1^3$, $x_3=x_1^7$ et $x_4=x_1^9$, modulo P, le polynôme minimal de x_1, soit $x_3=x_1^2$ et $x_4=-x_1^3-x_1^2-x_1-1$.

(f) Le corps des coefficients du polynôme $X^3-\pi$ est $\mathbb{K}=\mathbb{Q}(\pi)$, extension transcendante de $\mathbb{Q}$. Son corps de décomposition est $\mathbb{K}(j,\sqrt[3]{\pi})$, extension algébrique et galoisienne de $\mathbb{K}$ (mais pas de $\mathbb{Q}$), de base sur $\mathbb{K}$ $\{1,j,\sqrt[3]{\pi})$, de degré 3, les trois $\mathbb{K}$-automorphismes étant définis par les trois images possibles de $\sqrt[3]{\pi}$: $\sqrt[3]{\pi}$, $j\sqrt[3]{\pi}$ et $j^2\sqrt[3]{\pi}$, et dont $j+\sqrt[3]{\pi}$ est un élément primitif, car, de $\pi=(a-j)^3$ on déduit $j=(a^3*3a-1-\pi)/3(a+a^2)$ et $\sqrt[3]{\pi}=a-j$.

(6) (a) Cherchons une éventuelle racine $p/q \in \mathbb{Q}$, p et q premiers entre eux. On obtient, en multipliant par q^5 :

$$p^5 \pm pq^4 + q^5 = 0$$

et p^5 (respectivement q^5) est congru à 0 modulo q (respectivement modulo p), ce qui est absurde.

Il reste une factorisation éventuelle en deux polynômes, de degré 2 et 3.

La division de $P = X^5 + X + 1$ par $X^2 + aX + 1$ donne :

$$P = (X^2 + aX + 1)(X^3 - aX^2 + (a^2 - 1)X) + (2a - a^3)) + R.$$

Le reste, $R = (a^4 - 3a^2 + 2)X + (a^3 - 2a + 1)$, s'annule pour $a = 1$, et :

$$X^5 + X + 1 = (X^2 + X + 1)(X^3 - X^2 + 1).$$

Pour $X^5 - X + 1$, le reste, $(a^4 - 3a^2)X + (-a^3 - 2a + 1)$, ne peut s'annuler, les coefficients n'ayant pas de racine commune, et le polynôme est irréductible.

(b) Comme :

$$\begin{aligned} Q(X+1) &= \textstyle\sum_{k=0}^{p-1}(X+1)^k \\ &= \frac{(X+1)^p - 1}{X+1-1} \\ &= \frac{\sum_{k=0}^{p} C_p^k X^k - 1}{X} \\ &= X^{p-1} + \textstyle\sum_{k=2}^{p-1} C_p^k X^{k-1} + p, \end{aligned}$$

le critère d'Eisenstein s'applique, les C_p^k étant divisibles par p.

(7) (a) Soit $\mathbb{L}$ l'extension galoisienne engendrée par $a = \sqrt{2} + i$.

De $(a - i)^2 = 2$, on déduit que $i = (a^2 - 3)/2a$ et $\sqrt{2} = (a^2 + 3)/2a$ sont dans $\mathbb{L}$. Les polynômes minimaux de ces éléments étant $X^2 + 1$ et $X^2 - 3$, leurs conjugués sont $-i$ et $-\sqrt{3}$, et :

$$\mathbb{L} = \mathbb{Q}[i, \sqrt{3}] = \mathbb{Q}[\sqrt{3}]\,[i] = \mathbb{K}[i].$$

une base sur $\mathbb{Q}$ de $\mathbb{K}$ est $\{1, \sqrt{3}\}$, une base sur $\mathbb{L}$ de $\mathbb{K}$ est $\{1, i\}$, la dimension de $\mathbb{L}$ sur $\mathbb{Q}$ est donc 4, et $\mathbb{L}$ admet les quatre $\mathbb{Q}$-automorphismes :

$$\begin{cases} \text{l'identité} i_d, \\ (\sqrt{3}, i) \mapsto (-\sqrt{3}, i), \\ (\sqrt{3}, i) \mapsto (\sqrt{3}, -i), \\ (\sqrt{3}, i) \mapsto (-\sqrt{3}, -i). \end{cases}$$

Le groupe de Galois de $\mathbb{L}$ est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

(b) Soit $\mathbb{L}$ l'extension galoisienne engendrée par $a = \sqrt{2} + \sqrt[3]{2}$.

De $(a-\sqrt{2})^3 = 2$, on déduit :

$$\sqrt{2} = \frac{a^3 + 2a - 8}{2 - 3a^2}$$

et $\sqrt{2} \in \mathbb{L}$, puis $\sqrt[3]{2} = a - \sqrt{2} \in \mathbb{L}$. Le polynôme minimal de $\sqrt[3]{2}$ étant $X^3 - 2$, $\mathbb{L}$ doit contenir aussi les conjugués de $\sqrt[3]{2}$, soit $j\sqrt[3]{2}$ et $j^2\sqrt[3]{2}$. Elle contient également $j = j\sqrt[3]{2}/\sqrt[3]{2}$. D'où :

$$\mathbb{L} = \mathbb{Q}[\sqrt{2}, \sqrt[3]{2}, j\sqrt[3]{2}, j^2\sqrt[3]{2}] = \mathbb{Q}[\sqrt{2}]\,[\sqrt[3]{2}, j\sqrt[3]{2}, j^2\sqrt[3]{2}].$$

Si $\mathbb{K} = \mathbb{Q}[\sqrt{2}]$, on a $\mathbb{L} = \mathbb{K}[\sqrt[3]{2}, j\sqrt[3]{2}, j^2\sqrt[3]{2}]$. Le groupe $\mathrm{Gal}[\mathbb{L}/\mathbb{K}]$ contient l'identité et les multiplications par j et j^2 ; il est d'ordre 3, et la dimension de $\mathbb{L}$ sur $\mathbb{K}$ est égale à 3, d'où une base $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$.

Sur $\mathbb{Q}$, la dimension de $\mathbb{L}$ est égale à 6 (proposition 1.2), et les six $\mathbb{Q}$-automorphismes sont les composés des deux $\mathbb{Q}$-automorphismes de $\mathbb{K}$ et des trois de $\mathrm{Gal}[\mathbb{L}/\mathbb{K}]$.

(8) L'extension $\mathbb{L}$ est galoisienne, P n'ayant que des racines simples, toutes dans $\mathbb{L} \setminus \mathbb{Q}$. En divisant P par X^3 et en posant $Y = \dfrac{X+1}{X}$, on obtient le polynôme :

$$Q(Y) = Y(Y^2 + Y - 1)$$

dont les racines sont 0 et $(-1 \pm \sqrt{5})/2$.

$$\begin{cases} Y = 0 & \Rightarrow X = \pm i, \\ Y = (-1+\sqrt{5})/2 & \Rightarrow X = (-1+\sqrt{5} \pm i\sqrt{10+2\sqrt{5}})/4, \\ Y = (-1-\sqrt{5})/2 & \Rightarrow X = (-1-\sqrt{5} \pm i\sqrt{10-2\sqrt{5}})/4, \end{cases}$$

On peut remarquer, plus simplement, que $\dfrac{P}{X^2+1}$ est le polynôme cyclotomique de racines $\exp(2ik\pi/5)$, $1 \le k \le 4$. Les racines de P sont donc $\pm i$ et $e_k = \exp(2ki\pi/5)$, $1 \le k \le 4$ ($e_0 = e_5 = 1$ n'est pas racine).

On en déduit une base $\{e_1, \ldots, e_5, ie_1, \ldots, ie_5\}$, et $\dim_{\mathbb{Q}}(\mathbb{L}) = 10$.

Les dix $\mathbb{Q}$-automorphismes sont les cinq σ_n définis par $\sigma_n : e_k \mapsto e_{k+n}$, $1 \le n \le 5$ ($\sigma_5 = i_d$), et leurs cinq composés avec la conjugaison c, $c\,\sigma_n$.

Le groupe de Galois G, d'ordre 10, a un sous-groupe invariant d'ordre 5, donc cyclique d'ordre premier, constitué des σ_n, le groupe quotient étant isomorphe à $\mathbb{Z}/2\mathbb{Z}$. Le corps intermédiaire correspondant au sous-groupe d'ordre 5 est le corps des racines du polynôme cyclotomique, celui correspondant au groupe quotient est le corps des racines du polynôme $X^2 + 1$.

On peut aussi considérer le sous-groupe invariant d'ordre 2, $\{i_d, c\}$, le groupe quotient étant alors isomorphe à $\mathbb{Z}/5\mathbb{Z}$. Il y a interversion des corps intermédiaires.

La racine égale à $\exp(2i\pi/5)$ est celle qui a la plus grande partie réelle et une partie imaginaire positive :

$$\exp(2i\pi/5) = \frac{1}{4}(-1 + \sqrt{5} + i\sqrt{10+2\sqrt{5}}$$

Montrons que $a = i + \exp(2i\pi/5)$ est un élément primitif. De :

$$1 = (a-i)^5 = a^5 - 5ia^4 - 10a^3 + 10ia^2 + 5a - i$$

on déduit :

$$i = \frac{a^5 - 10a^3 + 5a - 1}{5a^4 - 10a^2 + 1},$$

puis :

$$\exp(2i\pi/5) = a - i = \frac{4a^5 - 4a + 1}{5a^4 - 10a^2 + 1},$$

les e_n et les ie_n.

On peut aussi choisir $a = i + \sqrt{10 + 2\sqrt{5}}$ comme élément primitif. On a successivement :

$$(a-i)^2 = 10 + 2\sqrt{5},\ ((a-i)^2 - 10)^2 = 20$$

d'où i en fonction (algébrique) de a, ainsi que $\sqrt{10 + 2\sqrt{5}}$ et $\sqrt{5}$. Comme $\sqrt{10 + 2\sqrt{5}}\sqrt{10 - 2\sqrt{5}} = 4\sqrt{5}$, on obtient également $\sqrt{10 - 2\sqrt{5}}$, d'où finalement toutes les racines.

(9) Les coefficients du polynôme $P = X^5 + 2X^3 + 2X^2 + 4$, à l'exception du premier, sont multiples du nombre premier 2, mais le terme constant est multiple de 2^2, et le critère d'Eiseinstein ne s'applique pas. De fait, P est réductible ($P = X^2 + 2)(X^3 + 2)$), et ses racines sont $\pm i\sqrt{2}$, $-\sqrt[3]{2}$, $-j\sqrt[3]{2}$ et $-j^2\sqrt[3]{2}$. Voir l'exemple 7.2.1.

Une base de $\mathbb{L}$ sur $\mathbb{Q}$ est :

$$\{1, i, \sqrt{2}, i\sqrt{2}, \sqrt[3]{2}, j\sqrt[3]{2}, \sqrt[3]{4}, j\sqrt[3]{4}, \sqrt[6]{2}, j\sqrt[6]{2}, \sqrt[6]{32}, j\sqrt[6]{32}\}$$

car, d'une part, i j et $\sqrt{2}$ sont liés ($2j = i + \sqrt{2}$), et, d'autre part, les produits et quotients des racines carrées et cubiques donnent des $\sqrt[6]{2}$ et des $\sqrt[6]{32}$. Elle est donc de degré 12.

On retrouve ce résultat en mettant $\mathbb{L}$ sous la forme $\Big[\mathbb{Q}[i]\,[\sqrt{2}]\Big]\,[\sqrt[3]{2}]$, d'où :

$$[\mathbb{L} : \mathbb{Q}] = 2 \times 2 \times 3 = 12.$$

Ceci nous donne également la tour radicale $\mathbb{Q}_0 \subset \mathbb{Q}_1 \subset \mathbb{Q}_2 \subset \mathbb{Q}_3$, avec $\mathbb{Q}_0 = \mathbb{Q}$, $\mathbb{Q}_1 = \mathbb{Q}_0[i]$, $\mathbb{Q}_2 = \mathbb{Q}_1[\sqrt{2}]$ et $\mathbb{Q}_3 = \mathbb{Q}_2[\sqrt[3]{2}] = \mathbb{L}$, et les sous-groupes d'ordre 2, 2 et 3.

Les 12 $\mathbb{Q}$-automorphismes sont obtenus à partir des 6 définis dans l'exemple 2.1.1 et de la symétrie sur $\sqrt{2} = d$:

$$\begin{cases} \sigma_{11} = i_d, & \sigma_{12} : (a,b,c,d) \mapsto (a,b,c,-d), \\ \sigma_{21} : (a,b,c,d) \mapsto (b,a,c,d), & \sigma_{22} : (a,b,c,d) \mapsto (b,a,c,-d), \\ \sigma_{31} : (a,b,c,d) \mapsto (c,b,a,d), & \sigma_{32} : (a,b,c,d) \mapsto (c,b,a,-d), \\ \sigma_{41} : (a,b,c,d) \mapsto (a,c,b,d), & \sigma_{42} : (a,b,c,d) \mapsto (a,c,b,-d), \\ \sigma_{51} : (a,b,c,d) \mapsto (b,c,a,d), & \sigma_{52} : (a,b,c,d) \mapsto (b,c,a,-d), \\ \sigma_{61} : (a,b,c,d) \mapsto (c,a,b,d), & \sigma_{62} : (a,b,c,d) \mapsto (c,a,b,-d), \end{cases}$$

Pour que $a = j + \sqrt{2} + \sqrt[3]{2}$ soit un élément primitif, il suffit que les $\sigma_{ij}(a)$ soient deux à deux distincts (proposition 2.1), ce qui se voit sans peine : ainsi l'image $(c, b, a, -d)$ n'apparait qu'une fois $(\sigma_{32}(a, b, c, d))$...

Terminons par la correspondance de Galois. On a :

$$\begin{cases} \mathrm{Gal}[\mathbb{Q}_3/\mathbb{Q}_2] = \mathbb{Z}/3\mathbb{Z}, \\ \mathrm{Gal}(\mathbb{Q}_3 : \mathbb{Q}_1) = (\mathbb{Z}/2\mathbb{Z})^2 \times (\mathbb{Z}/3\mathbb{Z}), \\ \mathrm{Gal}(\mathbb{Q}_3 : \mathbb{Q}_0) = (\mathbb{Z}/2\mathbb{Z})^2 \times (\mathbb{Z}/3\mathbb{Z}). \end{cases}$$

Les éléments invariants par $\mathrm{Gal}[\mathbb{Q}_3/\mathbb{Q}_i]$, $0 \leq i \leq 3$, sont ceux de $\mathbb{Q}_i$. D'où le tableau :

$$\begin{array}{cccccccc} & & \mathbb{Q} & \subset & \mathbb{Q}_1 & \subset & \mathbb{Q}_2 & \subset & \mathbb{Q}_3 = \mathbb{L} \\ u & \downarrow & & & & & & & \\ & & (\mathbb{Z}/2\mathbb{Z})^2 \times (\mathbb{Z}/3\mathbb{Z}) & \subset & \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/3\mathbb{Z}) & \subset & \mathbb{Z}/3\mathbb{Z} & \subset & I \\ v & \downarrow & & & & & & & \\ & & \mathbb{Q} & \subset & \mathbb{Q}_1 & \subset & \mathbb{Q}_2 & \subset & \mathbb{Q}_3 \end{array}$$

Les groupes-quotients sont, successivement, $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/3\mathbb{Z}$. Ils sont cycliqus d'ordre premier.

Index