La théorie de Galois en MPSI

Christophe Bertault

SOMMAIRE

INTRODUCTION 3

0.1 Relations coefficients-racines et brisure de symétrie 4

0.2 Pourquoi une théorie des extensions ? 5

0.3 Les racines d'un polynôme se valent-elles ? 7

0.4 Un bref historique 8

CHAPITRE 1 **COMPLÉMENTS SUR LES POLYNÔMES** 10

1.1 Polynômes à coefficients dans un corps quelconque 11

1.2 Polynômes irréductibles à coefficients rationnels 12

CHAPITRE 2 **EXTENSIONS DE CORPS** 17

2.1 Algèbres sur un corps et extensions de corps 17

2.2 Degré d'une extension 18

2.3 Sous-algèbre et sous-extension engendrées par une partie 18

2.4 Corps de décomposition d'un polynôme et résolubilité par radicaux 20

CHAPITRE 3 **ÉLÉMENTS ALGÉBRIQUES** 22

3.1 Éléments algébriques, éléments transcendants 22

3.2 Polynôme minimal d'un élément algébrique 22

3.3 Extensions finies et éléments algébriques 23

3.4 Le théorème de l'élément primitif 26

CHAPITRE 4 **GROUPE DE GALOIS D'UNE EXTENSION** 28

4.1 Morphismes d'algèbres 28

4.2 Construction de morphismes d'algèbres 29

4.3 Groupe de Galois d'une extension finie 31

4.4 Extensions galoisiennes 32

4.5 Morphismes de groupes 34

4.6 Exemples de groupes de Galois 34

CHAPITRE 5 **LA CORRESPONDANCE DE GALOIS 1** 38

5.1 Le théorème d'Artin 38

5.2 La correspondance de Galois 1 39

CHAPITRE 6 **COMPLÉMENTS DE THÉORIE DES GROUPES** 42

6.1 Sous-groupe engendré par une partie 42

6.2 Le théorème de Lagrange 43

6.3 Sous-groupes distingués et groupes quotients ... 45
6.4 Le théorème d'isomorphisme ... 48
6.5 Ordre d'un élément et théorème de Cauchy ... 50
6.6 Groupes résolubles ... 52
6.7 Non-résolubilité du groupe symétrique S_n pour $n \geqslant 5$ ... 54
CHAPITRE 7 **LA CORRESPONDANCE DE GALOIS 2** ... 56
CHAPITRE 8 **RÉSOLUBILITÉ PAR RADICAUX** ... 59
8.1 Résolubilité par radicaux et groupe de Galois ... 59
8.2 Exemples de polynômes non résolubles par radicaux ... 62

INTRODUCTION

Pré-requis :

Ce texte n'est pas un cours classique de théorie de Galois. Enseignée à l'université en troisième ou quatrième année de mathématiques post-bac, la théorie de Galois vient toujours après d'autres enseignements pour les couronner — théorie des groupes, théorie des anneaux, théorie des corps et algèbre linéaire. J'ai conçu mon texte au contraire comme une œuvre autonome dont le seul pré-requis est une maîtrise parfaite du programme d'algèbre de MPSI. Pour être honnête, je me suis permis deux petites entorses.

— Les anneaux $\frac{\mathbb{Z}}{n\mathbb{Z}}$, n décrivant $\mathbb{N}^*$, sont supposés connus. Alors qu'ils ne figurent qu'au programme de MP, les deux dernières pages de mon cours « Structures de groupe et d'anneau » leur sont tout de même consacrées.

— J'admettrai sans autre forme de procès que l'algèbre linéaire qu'on développe en MPSI sur $\mathbb{R}$ et $\mathbb{C}$ reste valable sur n'importe quel corps. De fait, nous quitterons rarement $\mathbb{C}$.

Toute autre notion requise par la théorie de Galois sera introduite en cours de route au moment qui m'a paru le plus opportun, du théorème de Lagrange à la notion de morphisme de groupes/algèbres en passant par les groupes quotients, les groupes résolubles et, par exemple, les polynômes irréductibles à coefficients rationnels.

À l'attention des amateurs chevronnés de la théorie de Galois :

Mon choix d'exposition de la théorie de Galois surprendra peut-être les connaisseurs s'il prenait à certains l'envie de me lire. Ce texte est avant tout un exposé de niveau MPSI de la théorie des extensions de corps dont le fil directeur est la résolution par radicaux des équations polynomiales. Il ne faut pas m'en vouloir dans ces conditions d'introduire les morphismes d'algèbres avant les morphismes de groupes et même la correspondance de Galois avant le banal théorème de Lagrange ! En outre, s'il est un peu question de corps finis dans ce texte, c'est seulement pour étudier l'irréductibilité des polynômes à coefficients entiers et je ne développerai qu'une théorie de Galois des sous-corps de $\mathbb{C}$. D'un point de vue technique, ce choix a des avantages clairs. On ne trouvera dans ce texte aucune occurrence des expressions *clôture algébrique* et *extension séparable*. Exit le *théorème de Steinitz* ! Mais exit aussi les *extensions normales*, dont le concept coïncidera ici avec celui d'extension galoisienne. Au fond, je n'ai conservé de la théorie de Galois que ses intuitions les plus galoisiennes.

À qui ce texte s'adresse-t-il finalement ?

Tout d'abord, bien sûr, aux étudiants de MPSI un peu fascinés par les mathématiques qu'un travail de lecture passionnant mais exigeant ne rebute pas. J'espère néanmoins que ce texte intéressera aussi quelques collègues désireux de renouer en douceur avec un joli morceau de maths. Dans une moindre mesure, il pourra peut-être aussi servir de complément aux étudiants qui suivent un cours classique de théorie de Galois.

Position du problème :

Pour le dire vite, une équation polynomiale est dite *résoluble par radicaux* si ses solutions peuvent être exprimées uniquement avec les symboles « + », « × » et « $\sqrt[n]{\cdot}$ » pour tout $n \geqslant 2$. On autorise aussi les soustractions et les quotients, qui ne sont que des déviations d'addition et de produit, ainsi que les racines $n^{\text{èmes}}$ généralisées qu'on peut trouver dans $\mathbb{C}$.

Toute équation polynomiale de degré 1 est ainsi résoluble par radicaux, car pour tous $a \in \mathbb{C}^*$ et $b \in \mathbb{C}$, l'équation $ax + b = 0$ d'inconnue $x \in \mathbb{C}$ admet $-\frac{b}{a}$ pour seule solution. De même, toute équation polynomiale de degré 2 est résoluble par radicaux, car pour tous $a \in \mathbb{C}^*$ et $b, c \in \mathbb{C}$, l'équation $ax^2 + bx + c = 0$ d'inconnue $x \in \mathbb{C}$ admet pour solutions $\frac{-b \pm \delta}{2a}$ où δ est l'une quelconque des racines carrées du discriminant $b^2 - 4ac$ dans $\mathbb{C}$. Nous verrons bientôt que des formules analogues existent pour les équations de degré 3 — ainsi que pour les équations de degré 4, mais nous ne nous y attarderons pas.

Introduite initialement par Galois dans le but de prouver que les équations polynomiales de degré supérieur ou égal à 5 ne sont pas toutes résolubles par radicaux, la théorie de Galois s'est peu à peu affranchie de ce problème très spécifique et on en trouve aujourd'hui la trace dans toutes les branches de l'algèbre ou presque. Nous nous en tiendrons quant à nous au problème initial de Galois, avec pour objectif final la compréhension de quelques exemples d'équations polynomiales non résolubles par radicaux. Nous montrerons ainsi que les polynômes :

$$X^5-5X-1, \qquad X^5-10X+5, \qquad 3X^7-7X^6-7X^3+21X^2-7 \qquad \text{et} \qquad X^7-3X^5-X^2+3X+1$$

ne sont pas résolubles par radicaux. Pourquoi ceux-là ? En quoi diffèrent-ils du polynôme X^5+X+1 ? Car ce polynôme, lui, est résoluble par radicaux. Il a pour racines deux racines cubiques de l'unité : $\mathrm{j}=\mathrm{e}^{\frac{2\mathrm{i}\pi}{3}}$ et $\mathrm{j}^2=\overline{\mathrm{j}}$, ainsi que :

$$\frac{1}{3}-\sqrt[3]{\frac{25+3\sqrt{69}}{54}}-\sqrt[3]{\frac{25-3\sqrt{69}}{54}}, \qquad \frac{1}{3}-\mathrm{j}\sqrt[3]{\frac{25+3\sqrt{69}}{54}}-\mathrm{j}^2\sqrt[3]{\frac{25-3\sqrt{69}}{54}} \qquad \text{et} \qquad \frac{1}{3}-\mathrm{j}^2\sqrt[3]{\frac{25+3\sqrt{69}}{54}}-\mathrm{j}\sqrt[3]{\frac{25-3\sqrt{69}}{54}}.$$

Que se passe-t-il donc d'incroyable à partir du degré 5 ? Alors que des méthodes générales de résolution par radicaux existent en-deçà, cela paraît déjà fou qu'une méthode générale ne puisse être trouvée à partir de l'entier 5, mais la situation est encore pire, certains polynômes ne sont même pas résolubles par radicaux à titre individuel. C'est à la compréhension de ce phénomène insolite que ce texte se propose de répondre.

Les lecteurs pressés peuvent éventuellement sauter la suite de cette introduction et passer directement au chapitre **1**. J'ai tenté néanmoins, dans les paragraphes qui suivent, de combler le gouffre géant qui sépare les motivations élémentaires de la théorie de Galois du cadre ultra-formel dans lequel elle est souvent présentée.

0.1 Relations coefficients-racines et brisure de symétrie

D'après le théorème de d'Alembert-Gauss, tout polynôme non constant de $\mathbb{C}[X]$ est scindé sur $\mathbb{C}$. Pour un tel polynôme $P=a_nX^n+\ldots+a_1X+a_0$ de degré n et de racines $x_1,\ldots,x_n$ dans $\mathbb{C}$ comptées avec multiplicité : $P=a_n(X-x_1)\ldots(X-x_n)$. On a coutume d'introduire alors les fonctions symétriques élémentaires $\sigma_1,\ldots,\sigma_n$, définies pour tout $k\in[\![1,n]\!]$ par la relation : $\sigma_k=\sum_{1\leqslant i_1<\ldots<i_k\leqslant n} x_{i_1}\ldots x_{i_k}$, avec par exemple : $\sigma_1=\sum_{i=1}^{n}x_i$, $\sigma_2=\sum_{1\leqslant i<j\leqslant n}x_ix_j$ et $\sigma_n=\prod_{i=1}^{n}x_i$.

Ces quantités sont dites symétriques parce que les nombres $x_1,\ldots,x_n$ y jouent strictement le même rôle. On le voit bien sur σ_1 et σ_n notamment, qu'aucune permutation de $x_1,\ldots,x_n$ ne saurait affecter. Qu'on attache aux racines de P des quantités symétriques ne devrait pas constituer une surprise à vrai dire, car si les coefficients $a_0,\ldots,a_n$ de P sont ordonnés naturellement par le degré du monôme dans lequel chacun figure, les racines $x_1,\ldots,x_n$ forment un paquet sans ordre. Elles viennent ensemble d'un coup d'un seul, a priori indiscernables.

On obtient tout de même d'importantes relations entre $x_1,\ldots,x_n$ et $a_0,\ldots,a_n$ — les relations coefficients-racines par simple identification polynomiale dans l'égalité : $a_nX^n+\ldots+a_1X+a_0=a_n(X-x_1)\ldots(X-x_n)$. En l'occurrence, pour tout $k\in[\![1,n]\!]$: $\sigma_k=(-1)^k\dfrac{a_{n-k}}{a_n}$. Si ces relations témoignent d'un lien fort entre les racines de P et ses coefficients, le système ainsi obtenu est composé de n équations symétriques à n inconnues $x_1,\ldots,x_n$ qu'on ne sait pas résoudre a priori. Les relations coefficients-racines fournissent $\sigma_1,\ldots,\sigma_n$ quand on connaît $a_0,\ldots,a_n$, mais comment en déduit-on individuellement $x_1,\ldots,x_n$? Comment distinguer les indiscernables ?

On peut toujours combiner les quantités $\sigma_1,\ldots,\sigma_n$ entre elles par combinaison linéaire et produit/quotient, on n'obtient hélas ainsi que des quantités symétriques. Par exemple, pour $n=3$: $\sigma_1=x_1+x_2+x_3$, $\sigma_2=x_1x_2+x_1x_3+x_2x_3$ et $\sigma_3=x_1x_2x_3$, et on voit bien que $\sigma_1^2-2\sigma_2=x_1^2+x_2^2+x_3^2$ est encore symétrique, de même que le rapport $\dfrac{\sigma_2}{\sigma_3}=\dfrac{1}{x_1}+\dfrac{1}{x_2}+\dfrac{1}{x_3}$ si x_1, x_2 et x_3 sont non nuls. Résoudre une équation polynomiale revient dès lors à briser la symétrie des relations coefficients-racines. Qu'une telle brisure de symétrie soit possible ou non, voilà l'une des questions auxquelles la théorie de Galois apporte une réponse. Comme le dit Galois lui-même, la théorie de Galois est avant tout une *théorie de l'ambiguïté* née pour mesurer l'indiscernabilité des racines d'un polynôme.

On n'a jamais espéré cela dit résoudre l'équation $x^2=2$ d'inconnue $x\in\mathbb{C}$ en faisant seulement des combinaisons linéaires et des produits/quotients à partir des coefficients entiers du polynôme X^2-2. On n'obtient d'ailleurs ainsi que des rationnels alors que $\sqrt{2}$ et $-\sqrt{2}$ ne le sont pas. L'utilisation de racines $n^{\text{èmes}}$ s'impose naturellement. Pour tous $n\in\mathbb{N}^*$ et $a\in\mathbb{C}^*$, le polynôme X^n-a offre une perspective de résolution intéressante car nous savons discerner ses racines et en donner une expression satisfaisante. En notant a sous la forme $a=re^{\mathrm{i}\theta}$ avec $r\geqslant 0$ et $\theta\in\mathbb{R}$, les racines de X^n-a sont les racines $n^{\text{èmes}}$ de a, i.e. les nombres $\sqrt[n]{r}\mathrm{e}^{\frac{\mathrm{i}\theta}{n}+\frac{2\mathrm{i}k\pi}{n}}$, k décrivant $[\![0,n-1]\!]$. Les deux exemples qui suivent illustrent la manière dont les racines $n^{\text{èmes}}$ peuvent briser la symétrie des relations coefficients-racines.

Exemple Soient $a\in\mathbb{C}^*$ et $b,c\in\mathbb{C}$. Le polynôme aX^2+bX+c possède deux racines x_1 et x_2 dans $\mathbb{C}$ — éventuellement égales. Les relations coefficients-racines s'écrivent ici : $x_1+x_2=-\dfrac{b}{a}$ et $x_1x_2=\dfrac{c}{a}$. Comment briser leur symétrie ?

Or, si la quantité x_1-x_2 n'est pas symétrique, son carré $(x_1-x_2)^2$ l'est. Il vaut : $(x_1-x_2)^2=(x_1+x_2)^2-4x_1x_2=\dfrac{b^2-4ac}{a^2}$. En notant δ une racine carrée quelconque du discriminant b^2-4ac, on obtient $x_1-x_2=\pm\dfrac{\delta}{a}$, et comme on connaît aussi x_1+x_2, on peut conclure : $\{x_1,x_2\}=\left\{\dfrac{-b\pm\delta}{2a}\right\}$. On a brisé la symétrie des relations coefficients-racines en s'autorisant une racine carrée.

Exemple On s'intéresse maintenant à la *méthode de Cardan* de résolution des équations de degré 3.

- Soient $a\in\mathbb{C}^*$ et $b,c,d\in\mathbb{C}$. On cherche les racines du polynôme aX^3+bX^2+cX+d, mais il est équivalent de chercher les racines du polynôme $a\left(X-\dfrac{b}{3a}\right)^3+b\left(X-\dfrac{b}{3a}\right)^2+c\left(X-\dfrac{b}{3a}\right)+d$, lequel est de la forme X^3+pX+q au facteur a près avec $p\in\mathbb{C}^*$ et $q\in\mathbb{C}$.
- Notons x_1,x_2,x_3 les racines de X^3+pX+q dans $\mathbb{C}$ comptées avec multiplicité. Les relations coefficients-racines donnent ici : $x_1+x_2+x_3=0$, $x_1x_2+x_1x_3+x_2x_3=p$ et $x_1x_2x_3=-q$.

  On introduit alors deux quantités non symétriques : $u=\dfrac{x_1+\mathrm{j}x_2+\mathrm{j}^2x_3}{3}$ et $v=\dfrac{x_1+\mathrm{j}^2x_2+\mathrm{j}x_3}{3}$. Aussitôt :
  $$u+v=0+u+v=\frac{(x_1+x_2+x_3)+\left(x_1+\mathrm{j}x_2+\mathrm{j}^2x_3\right)+\left(x_1+\mathrm{j}^2x_2+\mathrm{j}x_3\right)}{3}=x_1\qquad\text{car } 1+\mathrm{j}+\mathrm{j}^2=0,$$
  et de même : $x_2=\mathrm{j}^2u+\mathrm{j}v$ et $x_3=\mathrm{j}u+\mathrm{j}^2v$. Ces expressions de x_1, x_2 et x_3 en fonction de u et v donnent à penser que u et v nous ont permis de briser la symétrie des relations coefficients-racines, mais encore faut-il calculer u et v ! Or il se trouve que $p=x_1x_2+x_1x_3+x_2x_3=-3uv$ et :
  $$-q=x_1x_2x_3=(u+v)\left(\mathrm{j}^2u+\mathrm{j}v\right)\left(\mathrm{j}u+\mathrm{j}^2v\right)=u^3+v^3\qquad\text{après calcul, toujours grâce à la relation : } 1+\mathrm{j}+\mathrm{j}^2=0.$$
  Pour calculer $\{u,v\}$, on va ainsi plutôt calculer la paire $\{u^3,v^3\}$, solution du système somme-produit : $\begin{cases}u^3+v^3=-q\\u^3v^3=-\dfrac{p^3}{27}\end{cases}$.

  En d'autres termes, u^3 et v^3 sont les deux racines — éventuellement égales — du polynôme $X^2+qX-\dfrac{p^3}{27}$, que l'on sait exprimer par radicaux.

  Une fois qu'on connaît $\{u^3,v^3\}$, on remonte à $\{u,v\}$ grâce à des racines cubiques. Cela donne lieu a priori à 6 paires $\{u,v\}$, mais la condition de normalisation $uv=-\dfrac{p}{3}$ exclut certaines possibilités et l'on obtient en fait que 3 paires $\{u,v\}$, dont on déduit enfin x_1, x_2 et x_3.
- En résumé, on a ramené une équation de degré 3 à une équation de degré 2 grâce à des racines cubiques et la résolution complète a occasionné deux brisures de symétrie — une pour les racines cubiques, une autre pour la racine carrée cachée derrière l'équation de degré 2. L'expression finale des racines en porte la marque comme on le voit sur l'exemple du polynôme X^3+3X-2. Dans son cas : $\{u^3,v^3\}=\left\{1+\sqrt{2},1-\sqrt{2}\right\}$ avec la condition de normalisation $uv=-1$. Les racines de X^3+3X-2 sont finalement : $\sqrt[3]{\sqrt{2}+1}-\sqrt[3]{\sqrt{2}-1}$, $\mathrm{j}\sqrt[3]{\sqrt{2}+1}-\mathrm{j}^2\sqrt[3]{\sqrt{2}-1}$ et $\mathrm{j}^2\sqrt[3]{\sqrt{2}+1}-\mathrm{j}\sqrt[3]{\sqrt{2}-1}$.

Un travail semblable peut être mené pour les équations de degré 4, mais nous nous l'épargnerons. Nous voulons plutôt comprendre pourquoi rien de tel ne peut être mené en général pour les équations de degré supérieur.

0.2 Pourquoi une théorie des extensions ?

Le bon cadre pour définir les polynômes est celui des anneaux commutatifs, car pour définir la somme et le produit de deux polynômes, il est suffisant de savoir additionner et multiplier leurs coefficients — avec commutativité pour que tout se passe bien. À tout anneau commutatif A, on sait ainsi associer l'anneau $A[X]$ des polynômes à une indéterminée X à coefficients dans A. Si on veut garantir que les équations polynomiales aient des racines, le cadre des corps est cependant plus adapté. On est en effet vite amené à diviser quand on résout une équation polynomiale, c'est déjà vrai pour les équations de degré 1. Cela dit, le fait d'avoir un corps ne suffit pas. Si on veut des expressions par radicaux, il faut des corps assez gros susceptibles de contenir certaines racines $n^{\text{èmes}}$.

Si un corps L en contient un autre K pour les mêmes lois, on dit que L est une *extension de K* ou que K est un *sous-corps de L*. Le plus petit sous-corps de $\mathbb{C}$ est le corps $\mathbb{Q}$ car tout sous-corps de $\mathbb{C}$ contient 1, donc aussi : $\dfrac{2}{3}=\dfrac{1+1}{1+1+1}$ par exemple, mais finalement $\mathbb{Q}$ tout entier.

Ensuite, pour tout sous-corps K de $\mathbb{C}$ et pour tous $x_1,\dots,x_n \in \mathbb{C}$, on note $K(x_1,\dots,x_n)$ et on appelle *extension de K engendrée par $x_1,\dots,x_n$* l'ensemble de toutes les constructions qu'on peut faire à partir des éléments de K et de $x_1,\dots,x_n$ par somme/différence et produit/quotient. Cet ensemble contient K et $x_1,\dots,x_n$, mais aussi des nombres plus compliqués comme $x_1^2 - x_2x_3$ ou $\dfrac{x_1x_n^5}{3x_2^2+1}$. Stable par somme/différence et produit/quotient, $K(x_1,\dots,x_n)$ est de fait un corps.

Exemple

- $\mathbb{Q}(3) = \mathbb{Q}$ car $3 \in \mathbb{Q}$, donc 3 n'apporte aucune construction nouvelle.
- $\mathbb{Q}\big(\sqrt{2},-\sqrt{2}\big) = \mathbb{Q}\big(\sqrt{2}\big)$ car $-\sqrt{2} \in \mathbb{Q}\big(\sqrt{2}\big)$, donc $-\sqrt{2}$ n'apporte aucune construction nouvelle.
- De même : $\mathbb{Q}\big(1+\sqrt{2}\big) = \mathbb{Q}\big(\sqrt{2}\big)$, $\mathbb{Q}\big(\mathrm{j},\mathrm{j}^2\big) = \mathbb{Q}(\mathrm{j})$ et $\mathbb{Q}\big(\sqrt{2},\sqrt{3},\sqrt{6}\big) = \mathbb{Q}\big(\sqrt{2},\sqrt{3}\big)$.

Donnons-nous à présent un sous-corps K de $\mathbb{C}$ et un polynôme $P = a_nX^n + \dots + a_1X + a_0$ non constant de degré n à coefficients dans K, de racines $x_1,\dots,x_n$ dans $\mathbb{C}$ comptées avec multiplicité. Certaines racines de P appartiennent peut-être à K, mais d'autres peuvent ne pas lui appartenir si leur expression requiert des racines carrées, cubiques ou plus. On appelle *corps de décomposition de P sur K* l'extension $K(x_1,\dots,x_n)$ de K engendrée par $x_1,\dots,x_n$. Ce corps est le plus petit à contenir à la fois K et les racines de P, c'est le plus petit corps contenant K sur lequel P est scindé.

Revenons-en maintenant à la notion de polynôme résoluble par radicaux. Nous avons dit au début de ce texte qu'un polynôme est résoluble par radicaux quand ses racines ne requièrent que les opérations de somme/différence, produit/quotient et racines $n^{\text{èmes}}$ pour être exprimées — mais sur quels nombres initiaux ces opérations sont-elles censées travailler ? Il ne suffit pas d'imposer des opérations, il faut aussi imposer des nombres comme point de départ. Pour un polynôme à coefficients dans un sous-corps K de $\mathbb{C}$, il paraît naturel d'exiger que les opérations de somme/différence, produit/quotient et racines $n^{\text{èmes}}$ portent sur les éléments de K. On ne peut pas dire en fait qu'un polynôme est résoluble par radicaux tout court, il l'est *sur K*. Le plus souvent, K sera le corps $\mathbb{Q}$ car notre esprit manipule mieux les polynômes à coefficients entiers.

La résolubilité par radicaux d'un polynôme est assez facile à traduire dans le vocabulaire des extensions. Commençons par l'exemple simple du polynôme X^2-2 à coefficients dans $\mathbb{Q}$, de corps de décomposition sur $\mathbb{Q}$: $\mathbb{Q}\big(\sqrt{2},-\sqrt{2}\big) = \mathbb{Q}\big(\sqrt{2}\big)$. Alors que X^2-2 à coefficients dans $\mathbb{Q}$, il faut grimper jusqu'à $\mathbb{Q}\big(\sqrt{2}\big)$, plus gros, pour calculer ses racines. Il faut en d'autres termes ajouter à $\mathbb{Q}$ une certaine racine carrée, ici $\sqrt{2}$. La relation $\big(\sqrt{2}\big)^2 = 2 \in \mathbb{Q}$ traduit ce saut qu'on est obligé d'accepter pour passer de $\mathbb{Q}$ à $\mathbb{Q}\big(\sqrt{2}\big)$. C'est cela, la résolubilité par radicaux sur un exemple simple.

Penchons-nous maintenant sur le polynôme $P = X^4 - 6X^2 + 7$ à coefficients dans $\mathbb{Q}$, de racines distinctes : $\pm\sqrt{3\pm\sqrt{2}}$. Son corps de décomposition sur $\mathbb{Q}$ vaut : $\mathbb{Q}\Big(\sqrt{3+\sqrt{2}},\sqrt{3-\sqrt{2}},-\sqrt{3+\sqrt{2}},-\sqrt{3-\sqrt{2}}\Big) = \mathbb{Q}\Big(\sqrt{3+\sqrt{2}},\sqrt{3-\sqrt{2}}\Big)$. Comment passe-t-on « par radicaux » de $\mathbb{Q}$ à ce corps de décomposition un peu compliqué ? Réponse : par des ajouts « radicaux » successifs.

1) On adjoint $\sqrt{2}$ pour passer de $\mathbb{Q}$ à $\mathbb{Q}\big(\sqrt{2}\big)$ via la relation $\big(\sqrt{2}\big)^2 = 2 \in \mathbb{Q}$.
2) On adjoint $\sqrt{3+\sqrt{2}}$ pour passer de $\mathbb{Q}\big(\sqrt{2}\big)$ à $\mathbb{Q}\Big(\sqrt{2},\sqrt{3+\sqrt{2}}\Big)$ via la relation $\Big(\sqrt{3+\sqrt{2}}\Big)^2 = 3+\sqrt{2} \in \mathbb{Q}\big(\sqrt{2}\big)$.
3) On adjoint $\sqrt{3-\sqrt{2}}$ pour passer de $\mathbb{Q}\Big(\sqrt{2},\sqrt{3+\sqrt{2}}\Big)$ à $\mathbb{Q}\Big(\sqrt{2},\sqrt{3+\sqrt{2}},\sqrt{3-\sqrt{2}}\Big)$ via la relation :
$$\Big(\sqrt{3-\sqrt{2}}\Big)^2 = 3-\sqrt{2} \in \mathbb{Q}\Big(\sqrt{2},\sqrt{3+\sqrt{2}}\Big).$$

Construit de proche en proche comme on vient de le faire, le corps $\mathbb{Q}\Big(\sqrt{2},\sqrt{3+\sqrt{2}},\sqrt{3-\sqrt{2}}\Big)$ est appelé une *extension radicale de $\mathbb{Q}$*, et tout a été fait pour que ce corps contienne le corps de décomposition de P sur $\mathbb{Q}$ — il lui est ici égal, mais ce n'est pas toujours le cas.

On pourrait procéder de même avec n'importe quel polynôme résoluble par radicaux. Le corps de décomposition d'un polynôme résoluble par radicaux est toujours inclus dans une extension radicale. Réciproquement, les éléments d'une extension radicale peuvent tous être exprimés par radicaux. Cette caractérisation de la résolubilité par radicaux en termes d'extensions nous tiendra en fait lieu de définition quand nous viserons plus de rigueur.

Faisons par exemple l'hypothèse que le corps de décomposition sur $\mathbb{Q}$ d'un certain polynôme P est inclus dans l'extension $\mathbb{Q}\Big(\sqrt[3]{3},\sqrt{1+\sqrt[3]{3}},\sqrt{5}\Big)$. Cette extension de $\mathbb{Q}$ est radicale car : $\big(\sqrt[3]{3}\big)^3 = 3 \in \mathbb{Q}$, $\Big(\sqrt{1+\sqrt[3]{3}}\Big)^2 = 1+\sqrt[3]{3} \in \mathbb{Q}\big(\sqrt[3]{3}\big)$ et $\big(\sqrt{5}\big)^2 = 5 \in \mathbb{Q}\Big(\sqrt[3]{3},\sqrt{1+\sqrt[3]{3}}\Big)$. Savoir que le corps de décomposition de P sur $\mathbb{Q}$ est inclus dans $\mathbb{Q}\Big(\sqrt[3]{3},\sqrt{1+\sqrt[3]{3}},\sqrt{5}\Big)$ ne nous permet pas de décrire précisément les racines de P, mais nous savons au moins qu'elles peuvent être exprimées par de simples sommes/différences et produits/quotients à partir de $\mathbb{Q}$ et des radicaux $\sqrt[3]{3}$, $\sqrt{1+\sqrt[3]{3}}$ et $\sqrt{5}$. Comme voulu, P est ainsi résoluble par radicaux sur $\mathbb{Q}$.

Conclusion : si nous voulons comprendre pourquoi certains polynômes ne sont pas résolubles par radicaux, nous allons devoir trouver une caractérisation éclairante des extensions radicales. Il sera alors peut-être possible de savoir si le corps de décomposition d'un polynôme est inclus dans l'une d'elles ou non, i.e. de savoir si ce polynôme est résoluble par radicaux.

0.3 Les racines d'un polynôme se valent-elles ?

Nous l'avons vu, la symétrie des relations coefficients-racines exclut qu'on en tire individuellement les racines d'un polynôme à partir de simples combinaisons linéaires et produits/quotients. Nous avons aussi vu sur l'exemple des équations de degré 2 et 3 comment l'utilisation de racines $n^{\text{èmes}}$ pouvait briser cette symétrie. La question se pose dès lors de savoir jusqu'où l'ensemble des racines d'un polynôme est lui-même symétrique. Que les relations coefficients-racines soient symétriques, c'est une chose, mais les racines se valent-elles réellement toutes du point de vue des opérations « + » et « × » ? Sont-elles parfaitement interchangeables ? Car après tout, les relations coefficients-racines ne sont peut-être que des relations parmi d'autres entre racines. D'autres relations non symétriques les relient peut-être, qui faciliteraient une expression par radicaux.

Et il se trouve en effet que les racines d'un polynôme ne se valent pas du tout les unes les autres. En quel sens ? Si les racines $x_1,\dots,x_n$ dans $\mathbb{C}$ comptées avec multiplicité d'un polynôme P donné se valent toutes, toute relation qu'on peut trouver entre elles doit être invariante par permutation. Par exemple, s'il est vrai que $x_1^2-x_2x_3+5x_3=7$, d'autres relations en découlent par permutation des indices :

— grâce à la transposition $(1\ 2)$: $x_2^2-x_1x_3+5x_3=7$,

— grâce au 3-cycle $(1\ 2\ 3)$: $x_2^2-x_3x_1+5x_1=7$.

Nous ne nous intéresserons ici qu'à des relations à base de combinaisons linéaires et produits/quotients. Encore faut-il s'entendre sur ce qu'on appelle combinaison linéaire. Comme au paragraphe précédent, si notre polynôme P est à coefficients dans un sous-corps K, nous nous autorisons des combinaisons K-linéaires, mais pas plus.

Exemple On note P le polynôme X^4-2 à coefficients dans $\mathbb{Q}$. Ses racines sont : $x_1=\sqrt[4]{2}$, $x_2=-\sqrt[4]{2}$, $x_3=\mathrm{i}\sqrt[4]{2}$ et $x_4=-\mathrm{i}\sqrt[4]{2}$. Deux relations non symétriques entre x_1, x_2, x_3 et x_4 sautent aux yeux : $x_1+x_2=0$ et $x_3+x_4=0$. Si les racines de P étaient interchangeables, on pourrait affirmer, en permutant la relation $x_1+x_2=0$ grâce au 3-cycle $(1\ 2\ 3)$, que $x_2+x_3=0$ — or c'est faux ! Conclusion : les racines de P forment un tout inhomogène que des relations comme $x_1+x_2=0$ et x_3+x_4 structurent.

Exemple On note P le polynôme $\big(X^2-4X+2\big)\big(X^2+1\big)^2$ à coefficients dans $\mathbb{Q}$. Ses racines comptées avec multiplicité sont : $x_1=2+\sqrt{2}$, $x_2=2-\sqrt{2}$, $x_3=\mathrm{i}$, $x_4=\mathrm{i}$, $x_5=-\mathrm{i}$ et $x_6=-\mathrm{i}$. De nouveau, certaines relations non symétriques entre x_1, x_2, x_3, x_4, x_5 et x_6 sautent aux yeux :

$$x_1+x_2=4 \quad\text{et}\quad x_1x_2=2 \quad \text{(relations coefficients-racines du polynôme } X^2-4X+2\text{)},$$
$$x_3+x_5=0 \quad\text{et}\quad x_3x_5=1 \quad \text{(relations coefficients-racines du polynôme } X^2+1\text{)}$$

ainsi que $x_3=x_4$ et $x_5=x_6$. Il est en revanche impossible d'exploiter la transposition $(1\ 3)$ dans les relations $x_1x_2=2$ et $x_3=x_4$, car il est faux que $x_3x_2=2$ et faux aussi que $x_1=x_4$. Décidément, les racines ne se valent pas.

Donnons-nous à présent un sous-corps K de $\mathbb{C}$ et un polynôme $P=a_nX^n+\dots+a_1X+a_0$ à coefficients dans K de racines $x_1,\dots,x_n$ dans $\mathbb{C}$ comptées avec multiplicité. Les relations non symétriques des exemples précédents structurent l'ensemble $\{x_1,\dots,x_n\}$, mais comme nous ne nous intéressons qu'à des combinaisons linéaires et des produits/quotients, ces relations structurent aussi le corps de décomposition $L=K(x_1,\dots,x_n)$ de P sur K. Pour mesurer la ressemblance des racines $x_1,\dots,x_n$ entre elles, plutôt que de nous intéresser à des permutations abstraites comme nous venons de le faire, nous allons nous intéresser plutôt aux bijections de L sur lui-même qui préservent l'addition et la multiplication et qui fixent les éléments de K — de manière à ne pas affecter les coefficients des combinaisons K-linéaires. Ces bijections g qu'on appelle des *K-automorphismes de L* obéissent en d'autres termes aux règles de calcul suivantes :

$$\forall x,y\in L,\quad g(x+y)=g(x)+g(y)\quad\text{et}\quad g(xy)=g(x)g(y)\qquad\text{et}\qquad\forall\lambda\in K,\quad g(\lambda)=\lambda.$$

Il paraît clair que les composées et réciproques de telles bijections sont encore des bijections du même type. L'ensemble des K-automorphismes de L est ainsi un groupe pour la composition. On l'appelle le *groupe de Galois de L sur K*, noté $\mathrm{Gal}(L|K)$.

Soit $g\in\mathrm{Gal}(L|K)$. Pour tout $i\in[\![1,n]\!]$, x_i est racine de P, donc $a_nx_i^n+\dots+a_1x_i+a_0=0$. Composons maintenant par g. D'après les propriétés qui définissent g : $a_ng(x_i)^n+\dots+a_1g(x_i)+a_0=0$, autrement dit $g(x_i)$ est aussi racine de P. Ce petit calcul montre que les éléments du groupe de Galois permutent $x_1,\dots,x_n$. Nous retrouvons ici un peu les permutations des indices dont nous avons parlé plus haut, mais de manière moins formelle. Mais s'il permute les racines, le groupe de Galois permute donc aussi toutes les relations non symétriques qu'on peut trouver entre elles. Une relation comme $x_1+3x_2=x_3$ contraint le groupe de Galois à ne pas être trop gros en excluant certaines permutations. Par exemple, pour $P=X^4-2$, nous avons vu plus haut qu'aucun élément du groupe de Galois ne peut correspondre à la permutation $(1\ 2\ 3)$. En résumé, quand le groupe de Galois est gros, il y a beaucoup de K-automorphismes, donc peu de relations contraignantes entre les racines, et donc sans doute peu de chances qu'on sache exprimer les racines par radicaux. Le groupe de Galois mesure finalement l'indiscernabilité des racines, et ce n'est pas tant le haut degré d'une équation polynomiale qui la rend difficile à résoudre que la taille et la complexité de son groupe de Galois.

Nous sommes à présent en mesure de raconter informellement la manière dont la théorie de Galois répond au problème de la résolubilité par radicaux des équations polynomiales.

— Un polynôme est résoluble par radicaux si son corps de décomposition est inclus dans une extension radicale. Le groupe de Galois associé possède dans ce cas une propriété spéciale propre à la théorie des groupes que nous définirons en temps voulu, on dit qu'il est *résoluble*. Au contraire, quand le groupe de Galois n'est pas résoluble, le polynôme n'est pas résoluble par radicaux.

— Le groupe symétrique S_n de toutes les permutations de $[\![1,n]\!]$ est résoluble si et seulement si $n \in [\![1,4]\!]$. Du coup, si les racines d'un polynôme de degré supérieur ou égal à 5 se valent suffisamment les unes les autres, i.e. sont suffisamment indiscernables, autrement si le groupe de Galois associé permet toutes les permutations des racines qu'on peut imaginer, alors ce groupe n'est pas résoluble, et donc le polynôme étudié n'est pas résoluble par radicaux.

— Pour finir, nous verrons qu'il existe bel et bien de tels polynômes !

0.4 Un bref historique

Nous achèverons cette introduction par une histoire accélérée de la résolution des équations polynomiales à travers les siècles.

- **Équations de degré 2 :**

  La résolution des équations de degré 2 remonte à loin dans le temps. Environ 2000 ans avant J.-C., et alors qu'ils ne disposaient d'aucune notation algébrique, les Babyloniens savaient déjà que le réel $-\frac{b}{2}+\sqrt{\left(\frac{b}{2}\right)^2+c}$ est racine du polynôme X^2+bX-c lorsque c est positif. Les Égyptiens avaient des connaissances semblables à une époque proche. Les Grecs et les Chinois savaient de leur côté résoudre géométriquement un certain nombre d'équations de degré 2 entre le $4^{\text{ème}}$ et le $2^{\text{ème}}$ siècles avant J.-C.

  Au $7^{\text{ème}}$ siècle après J.-C., le mathématicien indien Brahmagupta sait que le réel $\frac{\sqrt{4ac+b^2}-b}{2a}$ est racine du polynôme aX^2-bX-c. Au $9^{\text{ème}}$ siècle, le mathématicien perse Al-Khwârizmî, qui ignore toutefois les nombres négatifs, est le premier à résoudre de manière un tant soit peu exhaustive les équations de degré 2. Le mathématicien indien Sridharacharya propose un travail semblable à la même époque.

  Ces découvertes n'atteignent l'Europe qu'au $12^{\text{ème}}$ siècle grâce au travail de diffusion du mathématicien juif espagnol Savasorda.

- **Équations de degrés 3 et 4 :**

  Il faut ensuite attendre le $16^{\text{ème}}$ siècle pour que le mystère des équations de degré 3 soit levé. La solution nous vient d'Italie, où les mathématiciens Tartaglia et Scipione del Ferro découvrent à peu près en même temps ce qu'on appelle aujourd'hui la *méthode de Cardan*. Cardan, quant à lui, a plus ou moins volé le travail de Tartaglia et l'a publié en son nom. Incidemment, c'est tout de même dans l'œuvre de Cardan qu'apparaissent pour la première fois dans l'histoire les nombres complexes.

  Quelques années plus tard, un certain Ferrari, élève de Cardan, résout quant à lui les équations de degré 4.

- **Équations de degré supérieur ou égal à 5 :**

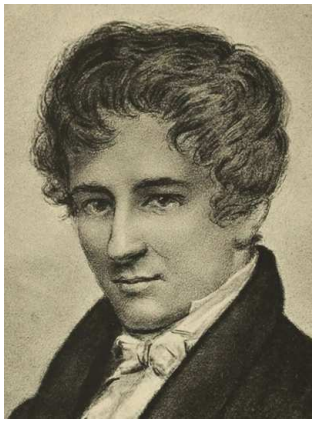
  En 1770, le mathématicien français Joseph-Louis Lagrange (1736-1813) est le premier à percevoir l'importance des permutations de racines que les résolutions antérieures des équations de degré 2, 3 et 4 exploitaient abondamment, mais aveuglément. En 1799, le mathématicien italien Paolo Ruffini (1765-1822) pousse le travail de Lagrange un peu plus loin, mais son texte est difficile à lire et passe à peu près inaperçu.

  En 1824, dans un texte qui restera lui aussi incompris quelques années, le mathématicien norvégien Niels Henrik Abel (1802-1829) montre qu'aucune formule générale de résolution des équations polynomiales de degré supérieur ou égal à 5 n'est possible. Ce résultat majeur, dit *théorème d'Abel* ou *théorème d'Abel-Ruffini*, laisse hélas en suspens la question de savoir si une équation polynomiale donnée est résoluble par radicaux ou non.

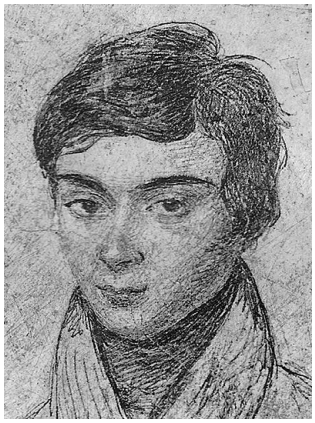
  Il revient finalement à Évariste Galois (1811-1832) de clore ce long processus de décantation en explicitant un critère de résolubilité des équations polynomiales de degré quelconque. Galois meurt hélas dans un duel à l'âge de 20 ans, lui aussi incompris, mais le mathématicien français Joseph Liouville (1809-1882) publie ses œuvres scientifiques quatorze ans plus tard à titre posthume.

  L'algèbre moderne naît dans la foulée. Implicites dans le travail de Galois, la théorie des groupes et la théorie des corps émergent dans la deuxième moitié du $19^{\text{ème}}$ siècle, notamment grâce aux travaux de Louis-Augustin Cauchy

(1789-1857), Arthur Cayley (1821-1895) et Camille Jordan (1838-1922). La définition moderne du groupe de Galois comme groupe d'automorphismes attendra encore un peu que tous ces concepts soient digérés. Elle sera l'œuvre du mathématicien autrichien Emil Artin (1898-1962).



Niels Henrik Abel



Évariste Galois

CHAPITRE 1 COMPLÉMENTS SUR LES POLYNÔMES

Si l'on y réfléchit bien, la notion de polynôme qu'on introduit d'abord avec des coefficients dans $\mathbb{R}$ ou $\mathbb{C}$ pourrait être définie sans plus difficulté avec des coefficients dans un anneau commutatif quelconque. Pour additionner et multiplier deux polynômes, on a en effet seulement besoin de pouvoir additionner et multiplier leurs coefficients. Pour tout anneau commutatif A, il est ainsi possible de noter $A[X]$ l'ensemble des polynômes à une indéterminée X à coefficients dans A. Nous travaillerons cela dit dans ce texte essentiellement avec des corps.

Au-delà du programme de MPSI, nous nous intéresserons souvent à des polynômes à coefficients dans $\mathbb{Q}$ ou $\mathbb{Z}$, mais il faut quitter franchement $\mathbb{C}$ si l'on veut un vrai sentiment d'exotisme. Notre dépaysement à nous, ce seront les anneaux $\frac{\mathbb{Z}}{n\mathbb{Z}}$, n décrivant $\mathbb{N}^*$, que je suppose connus dans ce texte et qui ne sont finalement qu'une copie tronquée de $\mathbb{Z}$ dans laquelle toute addition et toute multiplication sont effectuées modulo n. L'anneau $\frac{\mathbb{Z}}{n\mathbb{Z}}$ est un ensemble de cardinal n dont nous noterons $0, 1, \dots, n-1$ les éléments. Parce que ce choix de notation peut prêter à confusion, il faut toujours bien se demander dans quel monde on travaille.

Exemple Dans $\frac{\mathbb{Z}}{10\mathbb{Z}}$: $\quad 3\times 5+7 = 15-3 = 5-3 = 2 \quad$ et dans $\frac{\mathbb{Z}}{4\mathbb{Z}}$: $\quad 2\times 2 = 4 = 0.$

Exemple Dans $\frac{\mathbb{Z}}{6\mathbb{Z}}[X]$: $\quad (2X-1)(X+5) = 2X^2+9X-5 = 2X^2+3X+1.$

Dans l'exemple précédent, le calcul est entièrement effectué dans $\frac{\mathbb{Z}}{6\mathbb{Z}}[X]$, mais toute identité dans $\mathbb{Z}[X]$ peut par ailleurs être réduite modulo n pour tout $n \in \mathbb{N}^*$ et devient ainsi une identité dans $\frac{\mathbb{Z}}{n\mathbb{Z}}[X]$.

Exemple La relation : $\quad X^4-10X^3+35X^2-50X+24 = (X-1)(X-2)(X-3)(X-4) \quad$ dans $\mathbb{Z}[X]$ devient dans $\mathbb{F}_5[X]$: $X^4-1 = (X-1)(X-2)(X+2)(X+1)$.

À présent, si un entier $n \in \mathbb{N}^*$ n'est pas premier, on peut l'écrire $n = ab$ pour certains $a, b \in [\![1, n-1]\!]$ et cette relation s'écrit dans $\frac{\mathbb{Z}}{n\mathbb{Z}}$: $\quad ab = 0 \quad$ avec $a \neq 0$ et $b \neq 0$. Par conséquent, $\frac{\mathbb{Z}}{n\mathbb{Z}}$ ne peut être intègre que si n est premier. A fortiori, ce ne peut être un corps que si n est premier.

Le calcul des inverses dans $\frac{\mathbb{Z}}{n\mathbb{Z}}$ repose quant à lui entièrement sur l'existence de relations de Bézout comme on le voit dans l'exemple qui suit. En l'occurrence, pour tout $x \in \mathbb{Z}$, x est inversible dans $\frac{\mathbb{Z}}{n\mathbb{Z}}$ si et seulement si x et n sont premiers entre eux.

Exemple 7 est inversible dans $\frac{\mathbb{Z}}{10\mathbb{Z}}$ et $7^{-1} = 3$.

Démonstration Les entiers 7 et 10 sont premiers entre eux. Or la relation de Bézout : $\quad 3\times 7 - 2\times 10 = 1$ s'écrit ainsi dans $\frac{\mathbb{Z}}{10\mathbb{Z}}$: $\quad 3\times 7 = 1, \quad$ donc en effet $7^{-1} = 3$.

Pour tout $p \in \mathbb{P}$, p est premier avec les entiers $1, 2, \dots, p-1$ mais pas avec 0, donc tout élément non nul de $\frac{\mathbb{Z}}{p\mathbb{Z}}$ y est inversible. En d'autres termes, $\frac{\mathbb{Z}}{p\mathbb{Z}}$ est un corps et nous pouvons même en faire un théorème.

Définition-théorème 1.0.1 **(Corps $\mathbb{F}_p$)** Pour tout $n \in \mathbb{N}^*$, l'anneau $\frac{\mathbb{Z}}{n\mathbb{Z}}$ est un corps si et seulement si n est premier. Pour tout $p \in \mathbb{P}$, on notera généralement $\mathbb{F}_p$ le corps $\frac{\mathbb{Z}}{p\mathbb{Z}}$.

À présent, pour tous $p \in \mathbb{P}$ et $k \in [\![1, p-1]\!]$: $k\binom{p}{k} = p\binom{p-1}{k-1}$ et p et k sont premiers entre eux, donc p divise $\binom{p}{k}$ d'après le théorème de Gauss, donc $\binom{p}{k} = 0$ dans $\frac{\mathbb{Z}}{p\mathbb{Z}}$. Il en découle que : $(x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k} = x^p + y^p$ pour tous $x, y \in \frac{\mathbb{Z}}{p\mathbb{Z}}$, puis que pour tout $x \in [\![0, p-1]\!]$: $x^p = \underbrace{(1+\ldots+1)^p}_{x \text{ fois}} = 1^p + \ldots + 1^p = 1 + \ldots + 1 = x$.

Théorème 1.0.2 **(Petit théorème de Fermat)** Soit $p \in \mathbb{P}$. Pour tout $x \in \mathbb{F}_p$: $x^p = x$, et pour tout $x \in \mathbb{F}_p^*$: $x^{p-1} = 1$.

Le petit théorème de Fermat énonce une relation inhabituelle de $\mathbb{F}_p$, mais cette relation s'impose aussi dans $\mathbb{F}_p[X]$.

Exemple Pour tous $p \in \mathbb{P}$ et $a \in \mathbb{F}_p$: $(X+a)^p = X^p + a$ dans $\mathbb{F}_p[X]$.

Démonstration $(X+a)^p = \sum_{k=0}^{p} \binom{p}{k} X^k a^{p-k} = X^p + a^p = X^p + a$.

1.1 Polynômes à coefficients dans un corps quelconque

Si les anneaux $\mathbb{R}[X]$ et $\mathbb{C}[X]$ se ressemblent énormément, nous savons aussi qu'ils diffèrent sur certains points. Ils n'ont pas les mêmes polynômes irréductibles par exemple. Qu'en est-il de l'anneau $K[X]$ pour un corps K quelconque ?

- Le premier point commun des anneaux $K[X]$, quel que soit le corps K, c'est qu'ils sont intègres, et c'est bien sûr essentiel dès qu'on veut calculer un peu. La preuve est la même que dans $\mathbb{R}[X]$ et $\mathbb{C}[X]$. Pour tous $P, Q \in K[X]$, si $PQ = 0$: $\deg(P) + \deg(Q) = -\infty$, donc $\deg(P) = -\infty$ ou $\deg(Q) = -\infty$, donc P ou Q est nul.
- Sur le terrain des racines, il est toujours vrai dans $K[X]$ pour tout corps K qu'un polynôme de degré n possède au plus n racines comptées avec multiplicité. Dans $\mathbb{R}[X]$ et $\mathbb{C}[X]$, on en déduit aussitôt que toute fonction polynomiale peut être identifiée au polynôme qui la définit, car pour tous $P, Q \in \mathbb{R}[X]$ par exemple :

$$\begin{aligned} \forall x \in \mathbb{R},\quad P(x) = Q(x) \quad &\iff P - Q \text{ admet tout réel pour racine} \\ &\iff P = Q \qquad \text{car } \mathbb{R} \text{ est un ensemble infini.} \end{aligned}$$

  Ce raisonnement échoue dans le cas d'un corps fini comme $\mathbb{F}_p$ où $p \in \mathbb{P}$. Donnons-nous en effet deux polynômes $P, Q \in \mathbb{F}_p[X]$ pour lesquels pour tout $x \in \mathbb{F}_p$: $P(x) = Q(x)$. Le fait que les fonctions $x \longmapsto P(x)$ et $x \longmapsto Q(x)$ coïncident implique-t-il que les polynômes P et Q coïncident ? Eh bien non !

$$\begin{aligned} \forall x \in \mathbb{F}_p,\quad P(x) = Q(x) \quad &\iff P - Q \text{ admet tout élément de } \mathbb{F}_p \text{ pour racine} \\ &\iff P - Q \text{ est divisible par } \prod_{x \in \mathbb{F}_p} (X - x). \end{aligned}$$

  Il reste à remarquer que le polynôme $X^p - X$ admet tout élément de $\mathbb{F}_p$ pour racine d'après le petit théorème de Fermat. Ce polynôme est donc scindé sur $\mathbb{F}_p$, et en l'occurrence : $X^p - X = \prod_{x \in \mathbb{F}_p} (X - x)$ pour une raison de degré.

  Finalement, P et Q définissent la même fonction polynomiale si et seulement si leur différence $P - Q$ est divisible par $X^p - X$. Il n'est donc vraiment pas possible d'identifier un polynôme à sa fonction polynomiale sur le corps $\mathbb{F}_p$. Par exemple, les polynômes X et X^2 ne sont pas égaux dans $\mathbb{F}_2[X]$ car ils n'ont pas le même degré, mais ils définissent pourtant la même fonction polynomiale sur $\mathbb{F}_2$.
- Autre point de désaccord entre les anneaux $K[X]$, la dérivation. Si les formules de dérivation sont les mêmes partout, certaines dérivations sont surprenantes. Pour tout $p \in \mathbb{P}$ par exemple, dans $\mathbb{F}_p[X]$: $\left(X^p\right)' = pX^{p-1} = 0$, et dans $\mathbb{F}_2[X]$: $\left(X^4 + X^3 + X^2 + X + 1\right)' = 4X^3 + 3X^2 + 2X + 1 = X^2 + 1$. En particulier, un polynôme de $\mathbb{F}_p[X]$ peut avoir une dérivée nulle sans être constant. En outre, la relation classique $\deg(P') = \deg(P) - 1$ pour tout $P \in \mathbb{F}_p[X]$ non constant est fausse. Elle reste vraie en fait tant que $\deg(P)$ n'est pas divisible par p.

  La formule de Taylor polynomiale, ensuite, est définitivement perdue dans $\mathbb{F}_p[X]$. Quel sens aurait en effet la relation : $P = \sum_{k=0}^{+\infty} \frac{P^{(k)}(\lambda)}{k!} (X - \lambda)^k$ pour tous $P \in \mathbb{F}_p[X]$ et $\lambda \in \mathbb{F}_p$ alors que $k! = 0$ pour tout $k \geqslant p$? Or ce n'est pas rien de perdre la formule de Taylor. Cela veut dire qu'on perd aussi la possibilité de calculer la multiplicité d'une racine en calculant son image par les dérivées successives.

- Sur le plan arithmétique, le vrai point commun des anneaux $K[X]$, c'est que le théorème de la division euclidienne y est vrai en toute généralité indépendamment de K — avec le même algorithme. À partir de ce théorème, le développement de la théorie est classique. On en tire comme dans $\mathbb{Z}$ une notion de PGCD avec algorithme d'Euclide, des relations de Bézout, une notion de polynômes premiers entre eux, un théorème de Gauss et une notion de PPCM.

  Ensuite, si l'existence d'une factorisation irréductible pour tout polynôme est triviale, son unicité à l'ordre près des facteurs unitaires découle du théorème de Gauss. Ce que chaque anneau $K[X]$ a de vraiment spécifique tout de même, ce sont ses irréductibles eux-mêmes. C'était déjà clair avec $\mathbb{R}[X]$ et $\mathbb{C}[X]$. Dans $\mathbb{C}[X]$ en effet, les polynômes irréductibles sont exactement les polynômes de degré 1 d'après le théorème de d'Alembert-Gauss, et dans $\mathbb{R}[X]$, il faut leur adjoindre les polynômes de degré deux sans racine réelle. Nous verrons plus loin que les polynômes irréductibles de l'anneau $\mathbb{Q}[X]$ sont nettement plus difficiles à décrire, de même que ceux de l'anneau $\mathbb{F}_p[X]$ pour tout $p \in \mathbb{P}$.

Nous consacrerons la fin de ce paragraphe à quelques remarques simples sur les polynômes irréductibles d'un corps quelconque K. Pour commencer, un polynôme de $K[X]$ qui possède une racine λ dans K est divisible par $X-\lambda$, donc non irréductible sur K. Ce qu'on découvre à présent, c'est que la réciproque est vraie pour les polynômes de degré 2 ou 3. Elle est fausse au-delà. Par exemple, le polynôme $\left(X^2+1\right)^2$, de degré 4, est sans racine dans $\mathbb{R}$, mais il n'y est pas irréductible.

Théorème 1.1.1 **(Polynômes irréductibles de petit degré)** Soit K un corps.

- Tout polynôme de degré 1 de $K[X]$ est irréductible sur K.
- Tout polynôme de degré 2 ou 3 de $K[X]$ sans racine dans K est irréductible sur K.

Démonstration Pour le deuxième point, un polynôme sans racine dans K n'a pas de diviseurs de degré 1, et pour la même raison, s'il est de degré 3, il n'a pas non plus de diviseurs de degré 2. Ses seuls diviseurs sont donc ses associés et les polynômes constants non nuls — d'où l'irréductibilité.

Exemple

- Le polynôme X^2+1 est irréductible sur $\mathbb{R}$ car il n'y a pas de racine réelle, mais il ne l'est pas sur $\mathbb{F}_2$ car dans $\mathbb{F}_2[X]$: $X^2+1 = X^2-2X+1 = (X-1)^2$.
- Le polynôme $P = X^3+X+1$ est irréductible sur $\mathbb{F}_5$ car : $P(0)=1$, $P(1)=3$, $P(2)=1$, $P(3)=1$ et $P(4)=4$.

L'énoncé qui suit n'a l'air de rien. Il aura pourtant une véritable importance par la suite. On y appelle *sous-corps de* $\mathbb{C}$ tout sous-anneau de $\mathbb{C}$ qui se trouve en fait être un corps. Par exemple, $\mathbb{Q}$ et $\mathbb{R}$ sont des sous-corps de $\mathbb{C}$.

Théorème 1.1.2 **(Racines d'un polynôme irréductible sur un sous-corps de $\mathbb{C}$)** Soit K un sous-corps de $\mathbb{C}$. Tout polynôme de $K[X]$ irréductible sur K est à racines simples dans $\mathbb{C}$.

Le résultat n'est pas vrai pour un corps quelconque, mais il l'est par exemple pour le corps $\mathbb{F}_p$ pour tout $p \in \mathbb{P}$. Ce n'est pas difficile à montrer, mais nous n'en aurons pas besoin.

Démonstration Soit $P \in K[X]$ irréductible sur K. En particulier, P n'est pas constant, donc comme on travaille dans $\mathbb{C}[X]$, P' est non nul — il ne faut pas oublier ici que pour tout $p \in \mathbb{P}$: $\left(X^p\right)' = 0$ dans $\mathbb{F}_p[X]$. Or de toute façon $\deg(P') < \deg(P)$, donc par irréductibilité de P, P et P' sont premiers entre eux dans $K[X]$, mais donc a fortiori dans $\mathbb{C}[X]$. Il en découle comme voulu que P et P' n'ont pas de racine commune dans $\mathbb{C}$.

1.2 Polynômes irréductibles à coefficients rationnels

Si quelqu'un vous demande un exemple de polynôme, vous lui donnerez certainement un exemple de polynôme à coefficients entiers car les entiers ou les rationnels se concoivent toujours mieux que les autres nombres. Pourtant, si les mondes $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ paraissent de plus en plus compliqués à mesure qu'on passe de l'un à l'autre en croissant, la complexité des mondes $\mathbb{Q}[X]$, $\mathbb{R}[X]$ et $\mathbb{C}[X]$ suit la logique inverse. Le monde $\mathbb{C}[X]$ est le plus simple des trois à décrire car ses irréductibles sont exactement les polynômes de degré 1. Le monde $\mathbb{R}[X]$ est un peu plus pénible à étudier, mais c'est sans commune mesure avec le monde $\mathbb{Q}[X]$. L'étude des polynômes irréductibles de $\mathbb{Q}[X]$ est un vrai casse-tête, une tâche infinie à laquelle nous allons nous atteler très modestement dans ce paragraphe autour de quelques idées simples.

Théorème 1.2.1 **(Racines rationnelles d'un polynôme à coefficients entiers)** Soit $P = a_n X^n + \ldots + a_1 X + a_0 \in \mathbb{Z}[X]$ ainsi que $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$ premiers entre eux. Si $\frac{p}{q}$ est racine de P, alors p divise a_0 et q divise a_n.

En particulier, si P est unitaire, toute racine rationnelle de P est un entier.

Démonstration Modulo p, la relation : $\sum_{k=0}^{n} a_k p^k q^{n-k} = q^n P\left(\frac{p}{q}\right) = 0$ s'écrit : $a_0 q^n \equiv 0\,[p]$, et comme p et q sont premiers entre eux, p divise a_0 d'après le théorème de Gauss. On procède de même pour l'autre relation de divisibilité en raisonnant modulo q.

Ce théorème de rien du tout permet déjà un certain nombre de choses, notamment pour les polynômes de degré 2 ou 3 via **1.1.1**.

Exemple Le polynôme $X^3 - X + 2$ est irréductible sur $\mathbb{Q}$.

Démonstration Il nous suffit d'après **1.1.1** de montrer que ce polynôme n'a pas de racine rationnelle. Or s'il en possède une, celle-ci est entière et divise 2 d'après **1.2.1**, donc vaut ± 1 ou ± 2, qui de fait ne sont pas racines.

Exemple Soient $d, k \in \mathbb{N}^*$. Si d n'est la puissance $k^{\text{ème}}$ d'aucun entier, alors $\sqrt[k]{d}$ est irrationnel.

Démonstration Le polynôme $X^k - d$, unitaire, admet $\sqrt[k]{d}$ pour racine. Du coup, par contraposition, si $\sqrt[k]{d}$ est rationnel, ce rationnel est un entier d'après **1.2.1**, autrement dit d est la puissance $k^{\text{ème}}$ d'un entier.

Exemple Les polynômes $X^2 - 2$ et $X^3 - 2$ sont irréductibles sur $\mathbb{Q}$.

Démonstration Les nombres $\sqrt{2}$ et $\sqrt[3]{2}$ sont irrationnels d'après l'exemple précédent. Le polynôme $X^2 - 2$ est ainsi de degré 2 sans racine dans $\mathbb{Q}$, et il en va de même du polynôme $X^3 - 2$ dont les racines sont $\sqrt[3]{2}$, $\mathrm{j}\sqrt[3]{2}$ et $\mathrm{j}^2\sqrt[3]{2}$ — les deux dernières ne sont même pas réelles.

On poursuit avec une remarque de bon sens, mais qui cache une subtilité. Il est clairement équivalent d'étudier l'irréductibilité sur $\mathbb{Q}$ des polynômes $\frac{5X^3}{2} - \frac{3X}{5} + \frac{3}{10}$ et $25X^3 - 6X + 3 = 10\left(\frac{5X^3}{2} - \frac{3X}{5} + \frac{3}{10}\right)$, et on peut toujours se ramener ainsi à des coefficients entiers, plus simples à manipuler. Cela dit, se demander si un polynôme à coefficients entiers est irréductible sur $\mathbb{Q}$, c'est quand même se demander s'il peut être décomposé à l'aide de polynômes à coefficients… rationnels. Ne peut-on pas se contenter de décompositions à coefficients entiers ? Ce n'est pas immédiat, mais nous allons voir que oui. L'irréductibilité d'un polynôme sur $\mathbb{Q}$ sera ainsi ramenée à son *irréductibilité sur* $\mathbb{Z}$, définie ci-dessous, autrement dit à la résolution d'un problème d'arithmétique des entiers.

Définition 1.2.2 **(Polynôme irréductible sur $\mathbb{Z}$)** Soit $P \in \mathbb{Z}[X]$. On dit que P est *irréductible sur* $\mathbb{Z}$ si $P \neq \pm 1$ et si pour tous $Q, R \in \mathbb{Z}[X]$: $P = QR \implies Q = \pm 1$ ou $R = \pm 1$.

Exemple Le polynôme $2X + 2$ est irréductible sur $\mathbb{Q}$ mais pas sur $\mathbb{Z}$ à cause de la factorisation : $2X + 2 = \underbrace{2}_{\in \mathbb{Z}[X]} \times \underbrace{(X+1)}_{\in \mathbb{Z}[X]}$.

Définition-théorème 1.2.3 **(Polynôme primitif)** Un polynôme de $\mathbb{Z}[X]$ est dit *primitif* si ses coefficients sont premiers entre eux dans leur ensemble.

Le produit de deux polynômes primitifs est lui-même primitif.

Un polynôme irréductible sur $\mathbb{Z}$ est toujours primitif, sans quoi on pourrait le factoriser de manière non triviale par le PGCD de ses coefficients.

Démonstration Soient $P, Q \in \mathbb{Z}[X]$. Si le produit PQ n'est pas primitif, son contenu est divisible par au moins un nombre premier p, et aussitôt dans $\mathbb{F}_p[X]$: $PQ = 0$. Comme $\mathbb{F}_p[X]$ est intègre, cela montre bien que $P = 0$ ou $Q = 0$ dans $\mathbb{F}_p[X]$, et donc que soit les coefficients de P, soit les coefficients de Q sont tous divisibles par p. L'un des deux polynômes n'est donc pas primitif.

Définition-théorème 1.2.4 **(Contenu d'un polynôme à coefficients entiers)** Pour tout $P \in \mathbb{Z}[X]$, on appelle *contenu de* P et on note $c(P)$ le PGCD de ses coefficients. Le polynôme $\frac{P}{c(P)}$ est clairement primitif.

Pour tous $P, Q \in \mathbb{Z}[X]$: $c(PQ) = c(P)\,c(Q)$.

Démonstration D'abord un rappel. Pour tous $a_1,\dots,a_n\in\mathbb{Z}$ et $k\in\mathbb{N}^*$: $(ka_1)\wedge\dots\wedge(ka_n)=k\big(a_1\wedge\dots\wedge a_n\big)$.

À présent, soient $P,Q\in\mathbb{Z}[X]$, que l'on peut supposer non nuls sans quoi le résultat est évident. Dans ce cas, les polynômes $\dfrac{P}{c(P)}$ et $\dfrac{Q}{c(Q)}$ sont à coefficients entiers et même primitifs. Leur produit $\dfrac{PQ}{c(P)c(Q)}$ est à son tour primitif d'après **1.2.3**, et aussitôt comme voulu : $c(PQ)=c(P)c(Q)$. ■

Théorème 1.2.5 **(Lemme de Gauss)** Soit $P\in\mathbb{Z}[X]$. Les assertions suivantes sont équivalentes :

(i) P est primitif et irréductible sur $\mathbb{Q}$.

(ii) P est irréductible sur $\mathbb{Z}$.

Démonstration

(i) $\Longrightarrow$ (ii) On suppose P primitif et irréductible sur $\mathbb{Q}$. En particulier, P n'est pas constant, donc $P\neq\pm1$. Soient ensuite $Q,R\in\mathbb{Z}[X]$ deux polynômes pour lesquels $P=QR$. L'un d'entre eux est forcément constant par irréductibilité de P sur $\mathbb{Q}$. Or par ailleurs : $c(Q)c(R)=c(QR)=c(P)=1$, donc $c(Q)$ et $c(R)$ valent ±1. Comme voulu : $Q=\pm1$ ou $R=\pm1$.

(ii) $\Longrightarrow$ (i) On suppose P irréductible sur $\mathbb{Z}$. Nous savons déjà qu'alors P est primitif, et comme $P\neq\pm1$, P n'est pas constant. Soient ensuite $Q,R\in\mathbb{Q}[X]$ deux polynômes pour lesquels $P=QR$. Le polynôme Q (resp. R) est à coefficients rationnels, mais on peut rendre ses coefficients entiers en le multipliant par un entier convenable q (resp. r). Les polynômes $\dfrac{qQ}{c(qQ)}$ et $\dfrac{rR}{c(rR)}$ sont alors à coefficients entiers et primitifs et : $\dfrac{qQ}{c(qQ)}\times\dfrac{rR}{c(rR)}=\dfrac{qrQR}{c(qQ)c(rR)}=\dfrac{qrP}{c(qrQR)}=\dfrac{qrP}{c(qrP)}\overset{c(P)=1}{=}\dfrac{qrP}{qr}=P$. Ainsi, par irréductibilité de P sur $\mathbb{Z}$: $\dfrac{qQ}{c(qQ)}=\pm1$ ou $\dfrac{rR}{c(rR)}=\pm1$, et donc comme voulu, Q ou R est constant. ■

En ramenant toute question d'irréductibilité sur $\mathbb{Q}$ à une question d'irréductibilité sur $\mathbb{Z}$, le lemme de Gauss nous permet d'exploiter les mondes $\mathbb{F}_p[X]$ au profit de $\mathbb{Q}[X]$.

Théorème 1.2.6 **(Irréductibilité sur $\mathbb{F}_p$, irréductibilité sur $\mathbb{Q}$)** Soient $P\in\mathbb{Z}[X]$ non constant et $p\in\mathbb{P}$. Si le coefficient dominant de P n'est pas divisible par p et si la réduction de P dans $\mathbb{F}_p[X]$ est irréductible sur $\mathbb{F}_p$, alors P est irréductible sur $\mathbb{Q}$.

Attention, la réciproque est fausse ! Par exemple, X^2+1 est irréductible sur $\mathbb{Q}$, mais dans $\mathbb{F}_2[X]$: $X^2+1=(X-1)^2$.

Démonstration Par contraposition, supposons que la réduction de P dans $\mathbb{F}_p[X]$ est irréductible sur $\mathbb{F}_p$, mais que P ne l'est pas sur $\mathbb{Q}$. A fortiori, P n'est donc pas irréductible sur $\mathbb{Z}$, donc $P=QR$ pour certains $Q,R\in\mathbb{Z}[X]$ non constants. Cette égalité est aussitôt vraie dans $\mathbb{F}_p[X]$, mais comme P est irréductible sur $\mathbb{F}_p$, l'un des polynômes Q ou R y est constant, disons Q. Or Q n'est pas constant dans $\mathbb{Z}[X]$, donc le fait qu'il le soit dans $\mathbb{F}_p[X]$ montre que son coefficient dominant dans $\mathbb{Z}$ est divisible par p. Le coefficient dominant de P l'est lui aussi a fortiori. ■

Exemple Le polynôme X^3-X-1 est irréductible sur $\mathbb{Q}$.

Démonstration La fonction polynomiale $x\longmapsto x^3-x$ est nulle sur $\mathbb{F}_3$ d'après le petit théorème de Fermat, donc le polynôme X^3-X-1 n'a pas de racine dans $\mathbb{F}_3$. De degré 3, il est irréductible sur $\mathbb{F}_3$ d'après **1.1.1**, mais donc aussi sur $\mathbb{Q}$ d'après **1.2.6**.

Après tant d'exemples de polynômes de degré 2 ou 3, est-il vraiment si difficile de prouver d'un polynôme de degré supérieur est irréductible ? Ce qui est certain, c'est que l'absence de racines ne suffit plus. Le polynôme $\big(X^2+1\big)^2$, par exemple, est sans racine réelle mais réductible sur $\mathbb{R}$. Dans $\mathbb{F}_p[X]$, pour tout $p\in\mathbb{P}$, l'*algorithme de Berlekamp* factorise efficacement les polynômes, donc en particulier teste leur irréductibilité, mais nous n'en parlerons pas davantage. Assorti d'un tel algorithme, le théorème **1.2.6** offre de belles perspectives.

La réduction modulo un nombre premier a hélas ses limites. Non seulement il n'est pas toujours facile de trouver un nombre premier p pour lequel l'irréductibilité est vraie modulo p, mais certains polynômes irréductibles sur $\mathbb{Q}$ ne le sont sur aucun corps $\mathbb{F}_p$.

Exemple Le polynôme X^4-10X^2+1 est irréductible sur $\mathbb{Z}$, mais pas sur $\mathbb{F}_p$, quelque nombre premier p qu'on considère.

Démonstration Nous démontrerons l'irréductibilité sur $\mathbb{Z}$ un peu plus loin. Donnons-nous pour le moment un nombre premier p. Nous allons distinguer trois cas, et dans ces trois cas, X^4-10X^2+1 sera réductible sur $\mathbb{F}_p$.

— Si 2 est un carré dans $\mathbb{F}_p$, disons $2=a^2$ avec $a\in\mathbb{F}_p$, alors :
$$X^4-10X^2+1=\big(X^2-1\big)^2-8X^2=\big(X^2-1\big)^2-(2aX)^2=\big(X^2+2aX-1\big)\big(X^2-2aX-1\big).$$
— Si 3 est un carré dans $\mathbb{F}_p$, disons $3=b^2$ avec $b\in\mathbb{F}_p$, alors :
$$X^4-10X^2+1=\big(X^2+1\big)^2-12X^2=\big(X^2+1\big)^2-(2bX)^2=\big(X^2+2bX+1\big)\big(X^2-2bX+1\big).$$
— Et si ni 2 ni 3 n'est un carré dans $\mathbb{F}_p$? Nous allons montrer qu'alors 6 en est forcément un, disons $6=c^2$. Il en découlera que : $X^4-10X^2+1=\big(X^2-5\big)^2-24=\big(X^2-5\big)^2-(2c)^2=\big(X^2+2c-5\big)\big(X^2-2c-5\big)$.

La fin de la preuve mériterait un cours en soi, mais nous sortirions du cadre de ce texte. Remarquons tout d'abord que pour tout $x\in\mathbb{F}_p^*$, d'après le petit théorème de Fermat : $\big(x^2\big)^{\frac{p-1}{2}}=x^{p-1}=1$. En outre, pour tous $x,y\in\mathbb{F}_p^*$: $x^2=y^2\iff x=\pm y$, donc l'application $x\longmapsto x^2$ de $\mathbb{F}_p^*$ dans lui-même donne à chaque carré de $\mathbb{F}_p^*$ exactement deux antécédents. L'ensemble $\mathbb{F}_p^*$ contient ainsi exactement $\dfrac{p-1}{2}$ carrés. Pour finir, le polynôme $X^{p-1}-1$ admet tout élément de $\mathbb{F}_p^*$ pour racine d'après le petit théorème de Fermat, et $X^{p-1}-1=\Big(X^{\frac{p-1}{2}}-1\Big)\Big(X^{\frac{p-1}{2}}+1\Big)$. Conclusion : les $\dfrac{p-1}{2}$ carrés de $\mathbb{F}_p^*$ sont exactement les racines de $X^{\frac{p-1}{2}}$, et a fortiori les $\dfrac{p-1}{2}$ non carrés de $\mathbb{F}_p^*$ sont les racines de $X^{\frac{p-1}{2}}$. Finalement, pour tout $x\in\mathbb{F}_p^*$, $x^{\frac{p-1}{2}}$ vaut ±1, et x est un carré si et seulement si $x^{\frac{p-1}{2}}=1$.

Revenons enfin à notre exemple. Si 2 et 3 ne sont pas des carrés dans $\mathbb{F}_p$: $2^{\frac{p-1}{2}}=3^{\frac{p-1}{2}}=-1$, donc par produit comme voulu : $6^{\frac{p-1}{2}}=1$ et donc 6 est un carré !

Le critère d'irréductibilité qui suit n'est qu'un critère parmi d'autres, mais il est bien pratique et facile à prouver.

Théorème 1.2.7 **(Critère d'Eisenstein)** Soit $P=a_nX^n+\ldots+a_1X+a_0\in\mathbb{Z}[X]$ non constant. On suppose que pour un certain $p\in\mathbb{P}$, p divise $a_0,\ldots,a_{n-1}$ sans diviser a_n et p^2 ne divise pas a_0. Alors P est irréductible sur $\mathbb{Q}$.

Démonstration Quitte à le diviser par son contenu, nous pouvons supposer P primitif sans perte de généralité et étudier son irréductibilité sur $\mathbb{Z}$ d'après le lemme de Gauss. Soient donc $Q,R\in\mathbb{Z}[X]$ pour lesquels $P=QR$. Si Q est constant, la relation $c(Q)\,c(R)=c(P)=1$ montre que $Q=\pm c(Q)=\pm1$ et on raisonne de même si R est constant. Supposons désormais Q et R non constants et cherchons une contradiction. Le produit de leurs coefficients dominants vaut a_n et n'est par hypothèse pas nul dans $\mathbb{F}_p$, donc les réductions de Q et R dans $\mathbb{F}_p[X]$ sont également des polynômes non constants.

Or par hypothèse, p divise $a_0,\ldots,a_{n-1}$ sans diviser a_n, donc dans $\mathbb{F}_p[X]$: $a_nX^n=QR$ avec $a_n\neq0$. Cette égalité force Q et R à être des monômes — non constants — donc à être chacun de la forme λX^d pour certains $\lambda\in\mathbb{F}_p$ et $d\in\mathbb{N}^*$. Il en découle dans $\mathbb{F}_p$ que $Q(0)=R(0)=0$, puis dans $\mathbb{Z}$, que $Q(0)$ et $R(0)$ sont divisibles par p. En retour, $a_0=P(0)=Q(0)R(0)$ est divisible par p^2 — contradiction. ∎

Exemple

- Les polynômes $X^2-5X+10$ et $3X^7-7X^6-7X^3+21X^2-7$ sont irréductibles sur $\mathbb{Q}$.
- Pour tous $n\in\mathbb{N}^*$ et $p\in\mathbb{P}$, le polynôme X^n-p est irréductible sur $\mathbb{Q}$.

Bien souvent, cela dit, pour prouver l'irréductibilité sur $\mathbb{Q}$ d'un polynôme $P\in\mathbb{Z}[X]$ grâce au critère d'Eisenstein, on n'applique pas ce critère à P directement mais à l'un de ses translatés $P(X+k)$ pour un certain $k\in\mathbb{Z}$ bien choisi. Cette possibilité nous est offerte par la remarque suivante.

Théorème 1.2.8 **(D'un polynôme irréductible à l'autre)** Soient K un corps et $P\in K[X]$.

- Pour tous $\lambda,\mu\in K$ avec $\lambda\neq0$, P est irréductible sur K si et seulement si $P(\lambda X+\mu)$ l'est.
- Si $P=a_nX^n+a_{n-1}X^{n-1}+\ldots+a_1X+a_0$ avec $a_0\neq0$ et $a_n\neq0$, P est irréductible sur K si et seulement si le polynôme $a_0X^n+a_1X^{n-1}+\ldots+a_{n-1}X+a_n$ l'est.

Démonstration Pour le deuxième point, supposons P réductible sur K, disons $P=QR$ pour certains $Q,R\in K[X]$ non constants de degrés respectifs q et r. Aussitôt :
$$a_0X^n+a_1X^{n-1}+\ldots+a_{n-1}X+a_n=X^nP\left(\frac{1}{X}\right)=X^qQ\left(\frac{1}{X}\right)\times X^rR\left(\frac{1}{X}\right)$$

et les fractions rationnelles $X^r Q\left(\frac{1}{X}\right)$ et $X^{n-r}R\left(\frac{1}{X}\right)$ sont bel et bien des polynômes, non constants qui plus est, donc $a_0X^n + a_1X^{n-1} + \ldots + a_{n-1}X + a_n$ est réductible sur K. ■

Exemple Le polynôme $X^4 - 10X^2 + 1$ est irréductible sur $\mathbb{Q}$.

Démonstration Il est équivalent de montrer l'irréductibilité sur $\mathbb{Q}$ du polynôme :

$$-\frac{1}{8}\Big((2X+1)^4 - 10(2X+1)^2 + 1\Big) = -2X^4 - 4X^3 + 2X^2 + 4X + 1,$$

et donc aussi équivalent de la montrer pour le polynôme renversé $X^4 + 4X + 2X^2 - 4X - 2$. Or ce polynôme est irréductible sur $\mathbb{Q}$ d'après le critère d'Eisenstein.

Exemple Le polynôme $X^p - pX - 1$ est irréductible sur $\mathbb{Q}$ pour tout $p \in \mathbb{P}$.

Démonstration Il suffit de montrer que le polynôme $(X+1)^p - p(X+1) - 1$ est irréductible sur $\mathbb{Q}$, et pour ce faire, nous pouvons appliquer le critère d'Eisenstein car :

$$(X+1)^p - p(X+1) - 1 = \left(\sum_{k=0}^{p} \binom{p}{k} X^k\right) - pX - p - 1 = X^p + \sum_{k=2}^{p-1} \binom{p}{k} X^k - p.$$

Il faut bien sûr avoir en tête que pour tout $k \in [\![1, p-1]\!]$, $\binom{p}{k}$ est divisible par p.

Exemple Le polynôme $X^{p-1} + X^{p-2} + \ldots + X + 1$ est irréductible sur $\mathbb{Q}$ pour tout $p \in \mathbb{P}$.

Démonstration Si on le note P : $\quad P(X+1) = \sum_{k=0}^{p-1} (X+1)^k = \frac{(X+1)^p - 1}{(X+1) - 1} = \sum_{k=1}^{p} \binom{p}{k} X^{k-1}$.

On pourrait multiplier à l'envi les critères d'irréductibilité sur $\mathbb{Q}$. Je n'en rajouterai qu'un pour le plaisir, et parce qu'il n'a rien à voir avec une quelconque réduction modulo un nombre premier. De nombreux critères d'irréductibilité découlent d'une analyse plus ou moins fine des racines du polynôme étudié.

Théorème 1.2.9 **(Un critère d'irréductibilité sur $\mathbb{Q}$ en termes de primalité)** Soit $P = a_nX^n + \ldots + a_1X + a_0 \in \mathbb{Z}[X]$ de degré n et $r \in \mathbb{Z}$ un entier pour lequel : $\quad |r| \geqslant 2 + \max_{1 \leqslant i \leqslant n-1} \left|\frac{a_i}{a_n}\right|$. Si $P(r)$ est premier, alors P est irréductible sur $\mathbb{Q}$.

Démonstration

- Posons $d = \max_{1 \leqslant i \leqslant n-1} \left|\frac{a_i}{a_n}\right|$. Nous allons d'abord montrer que toute racine de P dans $\mathbb{C}$ a un module strictement inférieur à $d+1$. Le résultat est bien sûr vrai pour les racines de module inférieur ou égal à 1, et pour une racine z de module strictement supérieur à 1 :

$$|z|^n = \frac{|-a_nz^n|}{|a_n|} = \frac{\left|a_{n-1}z^{n-1} + \ldots + a_1z + a_0\right|}{|a_n|} \leqslant \sum_{k=0}^{n-1} \left|\frac{a_k}{a_n}\right| \times |z|^k \leqslant d\sum_{k=0}^{n-1} |z|^k = d \times \frac{|z|^n - 1}{|z| - 1} < \frac{d|z|^n}{|z| - 1}.$$

  Comme voulu : $\quad |z| < d + 1$.

- Venons-en maintenant au théorème à proprement parler. D'après le lemme de Gauss, nous pouvons nous contenter d'une irréductibilité sur $\mathbb{Z}$. Raisonnant par l'absurde, donnons-nous deux polynômes $Q, R \in \mathbb{Z}[X]$ non constants pour lesquels $P = QR$. Par hypothèse, $P(r)$ est premier, donc $Q(r) = \pm 1$ par exemple. Or Q est scindé sur $\mathbb{C}$, disons $Q = a(X - z_1)\ldots(X - z_q)$ avec $a \in \mathbb{Z} \setminus \{0\}$ et où les nombres complexes $z_1, \ldots, z_q$ sont aussi des racines de P. Finalement, d'après le premier point :

$$1 = \big|Q(r)\big| \geqslant |a| \prod_{k=1}^{q} \big(|r| - |z_k|\big) > |a| \prod_{k=1}^{q} \big(|r| - d - 1\big) \geqslant |a| \prod_{k=1}^{q} 1 = |a| \geqslant 1 \quad \text{— contradiction.}$$ ■

Par exemple, tout polynôme P non constant à coefficients ± 1 pour lequel $P(3)$ est premier est irréductible sur $\mathbb{Q}$.

Exemple Le polynôme $X^4 + X + 1$ est irréductible sur $\mathbb{Q}$.

Démonstration Avec les notations de la preuve précédente : $\quad d = 1$, $\quad$ et il se trouve que $(-3)^4 + (-3) + 1 = 79$ est premier.

CHAPITRE 2 EXTENSIONS DE CORPS

2.1 ALGÈBRES SUR UN CORPS ET EXTENSIONS DE CORPS

Le corps $\mathbb{C}$ contient le corps $\mathbb{R}$, et cette inclusion fait naturellement de $\mathbb{C}$ un $\mathbb{R}$-espace vectoriel. Plus généralement, si un corps L possède un sous-anneau K qui est lui-même un corps, on sait additionner les éléments de L entre eux et les multiplier par un élément de K. Il n'en faut pas plus, d'après les axiomes de la structure de corps, pour faire de L un K-espace vectoriel. En résumé, un corps qui contient un corps est à la fois un anneau et un espace vectoriel.

L'algèbre linéaire offre de son côté d'autres exemples anneaux qui sont aussi des espaces vectoriels. Pour tout corps K, l'anneau $K[X]$ des polynômes à coefficients dans K est un K-espace vectoriel, de même que le corps $K(X)$ des fractions rationnelles, l'anneau $\mathscr{M}_n(K)$ des matrices carrées de taille n, mais aussi l'anneau $\mathscr{L}(E)$ des endomorphismes d'un K-espace vectoriel E quelconque. Après tant d'exemples, une définition s'impose.

Définition-théorème 2.1.1 **(Algèbre sur un corps, sous-algèbre)** Soit K un corps.

- On appelle *algèbre sur K* ou *K-algèbre* tout quadruplet $(A, +, \cdot, \times)$ pour lequel :
  - $(A, +, \cdot)$ est un K-espace vectoriel,
  - $(A, +, \times)$ est un anneau commutatif,
  - pour tous $a, a' \in A$ et $\lambda \in K$: $\lambda \cdot (a \times a') = a \times (\lambda \cdot a')$.
- Soit A une K-algèbre. On appelle *sous-K-algèbre de A* toute partie de A qui est elle-même une K-algèbre pour les lois de A. En d'autres termes, une sous-K-algèbre de A est une partie de A qui en est à la fois un sous-K-espace vectoriel et un sous-anneau.

Exemple Pour tout corps K, $K[X]$ est une sous-K-algèbre de $K(X)$.

La situation de deux corps emboîtés, que nous allons passer tout ce texte à étudier, mérite une définition à part.

Définition 2.1.2 **(Extension de corps, sous-extension)** Soit K un corps.

- On appelle *extension de K* tout corps L dont K est un sous-anneau. On dit alors que K est un *sous-corps de L*. Il est équivalent de dire que L est une K-algèbre contenant K dont l'anneau sous-jacent est un corps.
- Soit L une extension de K. On appelle *sous-K-extension de L* toute extension de K qui est un sous-corps de L.

En résumé, une sous-K-extension de L est un corps intermédiaire entre K et L.

Exemple

- $\mathbb{C}$ est une extension de $\mathbb{R}$ et $\mathbb{R}$ une extension de $\mathbb{Q}$. On peut donc aussi dire que $\mathbb{R}$ est une sous-$\mathbb{Q}$-extension de $\mathbb{C}$.
- Pour tout corps K, l'ensemble $K(X)$ des fractions rationnelles à coefficients dans K est une extension de K. Les éléments de K sont ici identifiés à des fractions rationnelles constantes.

2.2 Degré d'une extension

Définition 2.2.1 **(Extension finie, degré)** Soient K un corps et L une extension de K. On dit que L est *finie* (resp. *infinie*) *sur* K si sa dimension comme K-espace vectoriel l'est. Cette dimension est alors appelée le *degré de* L *sur* K et notée $\big[L:K\big]$ — éventuellement $+\infty$.

Comme un corps n'est jamais réduit à un singleton : $\big[L:K\big]\geqslant 1$.

Théorème 2.2.2 **(Dimension d'une extension d'extension)** Soient K un corps, L une extension finie de K et M une extension finie de L. Alors M est une extension finie de K et : $\big[M:K\big]=\big[M:L\big]\times\big[L:K\big]$.

En particulier, $\big[L:K\big]$ est un diviseur de $\big[M:K\big]$.

Démonstration Soient $(l_i)_{1\leqslant i\leqslant r}$ une K-base de L et $(m_j)_{1\leqslant j\leqslant s}$ une L-base de M. Il nous suffit de montrer que $\big(l_im_j\big)_{i,j}$ est une K-base de M.

- **Caractère générateur :** Soit $x\in M$. Pour certains $\lambda_1,\dots,\lambda_s\in L$: $x=\sum_{j=1}^{s}\lambda_jm_j$ et pour tout $j\in[\![1,s]\!]$, il existe $\kappa_{1j},\dots,\kappa_{rj}\in K$ pour lesquels $\lambda_j=\sum_{i=1}^{r}\kappa_{ij}l_i$, donc $x=\sum_{i,j}\kappa_{ij}(l_im_j)$.
- **Liberté :** Soient $\kappa_{11},\dots,\kappa_{rs}\in K$. On suppose que $\sum_{i,j}\kappa_{ij}(l_im_j)=0$. On a donc aussi :
$$\sum_{j=1}^{s}\Bigg(\underbrace{\sum_{i=1}^{r}\kappa_{ij}l_i}_{\in L}\Bigg)m_j=0,\qquad\text{donc par liberté de }(m_j)_{1\leqslant j\leqslant r}:\quad\sum_{i=1}^{r}\kappa_{ij}l_i=0\quad\text{pour tout }j\in[\![1,s]\!],$$
et enfin par liberté de $(l_i)_{1\leqslant i\leqslant r}$: $\kappa_{11}=\dots=\kappa_{rs}=0$.

Exemple $\big[\mathbb{C}:\mathbb{R}\big]=2$ car $(1,\mathrm{i})$ est une $\mathbb{R}$-base de $\mathbb{C}$.

Exemple Pour tout corps K : $\big[K(X):K\big]=+\infty$ car la famille $\big(X^k\big)_{k\in\mathbb{N}}$ est K-libre.

Exemple $\big[\mathbb{R}:\mathbb{Q}\big]=+\infty$ car les réels $\ln p$, p décrivant l'ensemble des nombres premiers, sont $\mathbb{Q}$-linéairement indépendants.

Démonstration Soient $p_1,\dots,p_n$ des nombres premiers distincts et $r_1,\dots,r_n\in\mathbb{Q}$. On fait l'hypothèse que $\sum_{i=1}^{n}r_i\ln p_i=0$. On peut réduire les rationnels $r_1,\dots,r_n$ au même dénominateur : $r_1=\dfrac{k_1}{m}$, …, $r_n=\dfrac{k_n}{m}$ avec $k_1,\dots,k_n\in\mathbb{Z}$ et $m\in\mathbb{N}^*$, et quitte à réordonner, on peut supposer $k_1,\dots,k_s$ positifs ou nuls et $k_{s+1},\dots,k_n$ strictement négatifs. Aussitôt : $\sum_{i=1}^{s}k_i\ln p_i=-\sum_{j=s+1}^{n}k_j\ln p_j$, puis $\prod_{i=1}^{s}p_i^{k_i}=\prod_{j=s+1}^{n}p_j^{-k_j}$. Par unicité de la factorisation première, on en déduit comme voulu que $k_1=\dots=k_n=0$, i.e. $r_1=\dots=r_n=0$.

2.3 Sous-algèbre et sous-extension engendrées par une partie

Nous ne rentrerons pas dans les détails, mais on peut définir pour tout corps K des polynômes à plusieurs indéterminées et noter $K[X_1,\dots,X_n]$ l'ensemble des polynômes à n indéterminées $X_1,\dots,X_n$ à coefficients dans K, qui est comme $K[X]$ une K-algèbre. Par exemple : $X^2Y+3XY-4\in K[X,Y]$ et $X_1X_2+7X_2^3X_3-X_1^2X_3\in K[X_1,X_2,X_3]$.

Définition-théorème 2.3.1 **(Sous-algèbre et sous-extension engendrées par une partie)** Soient K un corps.

- Soient A une K-algèbre et $x_1,\dots,x_n \in A$. L'ensemble : $K[x_1,\dots,x_n] = \left\{P(x_1,\dots,x_n) \mid P \in K[X_1,\dots,X_n]\right\}$ est une sous-K-algèbre de A, et c'est même la plus petite sous-K-algèbre de A contenant $x_1,\dots,x_n$. On l'appelle la *sous-K-algèbre de A engendrée par $x_1,\dots,x_n$*.
- Soient L une extension de K et $x_1,\dots,x_n \in L$. L'ensemble :
$$K(x_1,\dots,x_n) = \left\{\frac{P(x_1,\dots,x_n)}{Q(x_1,\dots,x_n)} \;\middle|\; P,Q \in K[X_1,\dots,X_n] \quad \text{et} \quad Q(x_1,\dots,x_n) \neq 0\right\}$$
est une sous-K-extension de L, et c'est même la plus petite sous-K-extension de L contenant $x_1,\dots,x_n$. On l'appelle la *sous-K-extension de L engendrée par $x_1,\dots,x_n$*.

  Clairement : $K \subset K[x_1,\dots,x_n] \subset K(x_1,\dots,x_n)$.

Démonstration Le fait que $K[x_1,\dots,x_n]$ et $K(x_1,\dots,x_n)$ soient des K-algèbres traduit essentiellement le fait qu'ils sont stables par combinaison K-linéaire et produit, à un ou deux détails près. Il est clair par ailleurs que $K(x_1,\dots,x_n)\setminus\{0\}$ est stable par inversion, ce qui fait de $K(x_1,\dots,x_n)$ un corps.

Ensuite, pourquoi $K[x_1,\dots,x_n]$ est-elle la plus petite sous-K-algèbre contenant $x_1,\dots,x_n$? Pour commencer, $K[x_1,\dots,x_n]$ contient $x_1,\dots,x_n$ car pour tout $i \in [\![1,n]\!]$: $x_i = P(x_1,\dots,x_n)$ pour $P(X_1,\dots,X_n) = X_i$. Inversement, toute sous-K-algèbre de A contenant $x_1,\dots,x_n$ contient aussi toutes les quantités qu'on peut former à partir d'eux par combinaison K-linéaire et produit, autrement dit contient $K[x_1,\dots,x_n]$. On raisonne de manière analogue avec $K(x_1,\dots,x_n)$.

Parce qu'il est de dimension infinie comme K-espace vectoriel, $K[X]$ est beaucoup plus gros que K, et $K(X)$ l'est bien sûr encore plus. Les exemples qui suivent montrent que $K[x_1,\dots,x_n]$ et $K(x_1,\dots,x_n)$ peuvent être au contraire assez proches de K en taille et qu'ils peuvent aussi coïncider. Nous y verrons plus clair au prochain chapitre.

Exemple Pour tout corps K et pour tout $x \in K$: $K(x) = K[x] = K$. Par exemple : $\mathbb{Q}\left(\frac{3}{5}\right) = \mathbb{Q}$.

Démonstration Quelle est la plus petite sous-K-extension de K contenant x ? Comme $x \in K$, c'est bien sûr K lui-même ! Conclusion : $K(x) = K$.

Exemple $\mathbb{R}(\mathrm{i}) = \mathbb{R}[\mathrm{i}] = \mathbb{C}$.

Démonstration Comme $\mathbb{R}[\mathrm{i}]$ et $\mathbb{R}(\mathrm{i})$ contiennent i, ils contiennent $a+\mathrm{i}b$ pour tous $a,b \in \mathbb{R}$, autrement dit $\mathbb{C}$, et l'égalité en découle car ce sont des parties de $\mathbb{C}$.

Le fait que $\mathbb{R}(X)$ soit beaucoup plus volumineux que $\mathbb{R}[X]$ n'empêche manifestement pas $\mathbb{R}(\mathrm{i})$ et $\mathbb{R}[\mathrm{i}]$ de coïncider. De même, $\mathbb{R}[X]$ a beau être de dimension infinie sur $\mathbb{R}$, $\mathbb{R}[\mathrm{i}] = \mathbb{C}$ n'est que de dimension 2. La raison de cette perte est bien simple : $\mathrm{i}^2 = -1$. Cette relation ramène en effet toute puissance de i à l'un des nombres ± 1 ou $\pm\mathrm{i}$ et permet de faire monter au numérateur, grâce à un conjugué, tous les i qu'on peut trouver au dénominateur. Il n'y a ainsi pas plus de fractions en i que de quantités affines $a+\mathrm{i}b$ avec $a,b \in \mathbb{R}$. Par exemple :
$$2\mathrm{i}^3 - 3\mathrm{i}^2 + 4\mathrm{i} + 1 = -2\mathrm{i} + 3 + 4\mathrm{i} + 1 = 4 + 2\mathrm{i} \qquad \text{et} \qquad \frac{2+\mathrm{i}}{3-4\mathrm{i}} = \frac{(2+\mathrm{i})(3+4\mathrm{i})}{3^2+4^2} = \frac{2}{25} + \mathrm{i}\,\frac{11}{25}.$$

L'exemple qui suit fonctionne sur le même principe avec $\left(\sqrt{2}\right)^2 = 2$ pour relation-clé à la place de $\mathrm{i}^2 = -1$.

Exemple $\mathbb{Q}\left(\sqrt{2}\right) = \mathbb{Q}\left[\sqrt{2}\right] = \left\{a + b\sqrt{2} \mid a,b \in \mathbb{Q}\right\}$.

Démonstration L'inclusion : $\mathbb{Q}\left(\sqrt{2}\right) \subset \left\{a + b\sqrt{2} \mid a,b \in \mathbb{Q}\right\}$ suffira et nous nous contenterons momentanément d'une preuve par l'exemple. Posons $x = \sqrt{2}$. Grâce à la relation $x^2 = 2$, tout polynôme en x peut être écrit sous forme affine $ax+b$ avec $a,b \in \mathbb{Q}$. Par exemple :
$$x^5 - 7x^4 + 2x^3 + x^2 - 2x + 5 = 4x - 28 + 4x + 2 - 2x + 5 = 6x - 21.$$
Il paraît moins simple de se débarrasser des dénominateurs d'une fraction rationnelle en x, mais c'est compter sans les quantités conjuguées, qui sont une autre manière d'exploiter la relation $x^2 = 2$. Par exemple :
$$\frac{1}{3x+4} = \frac{-3x+4}{(3x+4)(-3x+4)} = \frac{-3x+4}{16-9x^2} = \frac{-3x+4}{16-18} = \frac{3}{2}x - 2.$$
Finalement, sur une fraction rationnelle un peu quelconque en x :
$$\frac{x^4-x^3-x-2}{x^3-3x+1} = \frac{4-2x-x-2}{2x-3x+1} = \frac{2-3x}{-x+1} = \frac{(2-3x)(x+1)}{(-x+1)(x+1)} = \frac{-3x^2-x+2}{1-x^2} = \frac{-6-x+2}{1-2} = x+4.$$

Exemple $\mathbb{Q}(j) = \mathbb{Q}(i\sqrt{3})$.

Démonstration Tout d'abord : $j = e^{\frac{2i\pi}{3}} = -\frac{1}{2} + i\frac{\sqrt{3}}{2} \in \mathbb{Q}(i\sqrt{3})$ donc comme $\mathbb{Q}(j)$ est la plus petite sous-$\mathbb{Q}$-extension de $\mathbb{C}$ contenant j : $\mathbb{Q}(j) \subset \mathbb{Q}(i\sqrt{3})$. On démontre de même l'inclusion réciproque en observant que $i\sqrt{3} = 2j + 1 \in \mathbb{Q}(j)$.

Exemple $\mathbb{Q}\left(\sqrt{2}, e^{\frac{i\pi}{4}}\right) = \mathbb{Q}(i, \sqrt{2})$.

Démonstration Tout d'abord : $e^{\frac{i\pi}{4}} = \frac{1+i}{\sqrt{2}} \in \mathbb{Q}(i, \sqrt{2})$ donc : $\mathbb{Q}\left(\sqrt{2}, e^{\frac{i\pi}{4}}\right) \subset \mathbb{Q}(i, \sqrt{2})$, et pour l'inclusion réciproque : $i = \sqrt{2}\, e^{\frac{i\pi}{4}} - 1 \in \mathbb{Q}\left(\sqrt{2}, e^{\frac{i\pi}{4}}\right)$.

Exemple $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}, \sqrt{4}, \sqrt{5}, \sqrt{6}\right) = \mathbb{Q}\left(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{6}\right) = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ car : $\sqrt{4} = 2 \in \mathbb{Q}$ et $\sqrt{6} = \sqrt{2} \times \sqrt{3}$.

Une dernière remarque avant de clore ce paragraphe, dont nous nous servirons constamment sans la rappeler.

Théorème 2.3.2 **(À propos des sous-extensions de sous-extensions)** Soient K un corps et L une extension de K. Pour tous $x_1, \dots, x_m, y_1, \dots, y_n \in L$: $K(x_1, \dots, x_m, y_1, \dots, y_n) = K(x_1, \dots, x_m)(y_1, \dots, y_n)$, où $K(x_1, \dots, x_m)(y_1, \dots, y_n)$ désigne la sous-$K(x_1, \dots, x_m)$-extension de L engendrée par $y_1, \dots, y_n$.

En particulier, pour deux éléments $x, y \in L$: $K(x, y) = K(x)(y) = K(y)(x)$. D'un point de vue calculatoire, ce résultat signifie juste que dans une expression rationnelle en x et y, les termes peuvent être rangés au numérateur et au dénominateur selon les puissances de y. Par exemple :

$$\frac{3x^3y^2 + x^2y + 2xy^2 + 5xy + 2x + 3y - 1}{x^2y + 2xy^3 + x + 2} = \frac{\left(3x^3 + 2x\right)y^2 + \left(x^2 + 5x + 3\right)y + (2x - 1)}{(2x)\,y^3 + \left(x^2\right)y + (x + 2)} \in K(x)(y)$$
$$= \frac{\left(3y^2\right)x^3 + (y)\,x^2 + \left(2y^2 + 5y + 2\right)x + (3y - 1)}{(y)\,x^2 + \left(2y^3 + 1\right)x + 2} \in K(y)(x).$$

Démonstration Pour commencer, $K(x_1, \dots, x_m, y_1, \dots, y_n)$ est une extension de K et contient $x_1, \dots, x_m$, donc contient $K(x_1, \dots, x_m)$. Mais $K(x_1, \dots, x_m, y_1, \dots, y_n)$ contient aussi $y_1, \dots, y_n$, donc :

$$K(x_1, \dots, x_m)(y_1, \dots, y_n) \subset K(x_1, \dots, x_m, y_1, \dots, y_n).$$

Inversement, $K(x_1, \dots, x_m)(y_1, \dots, y_n)$ contient $K(x_1, \dots, x_m)$ et $y_1, \dots, y_n$, donc aussi K et $x_1, \dots, x_m, y_1, \dots, y_n$. Comme voulu : $K(x_1, \dots, x_m, y_1, \dots, y_n) \subset K(x_1, \dots, x_m)(y_1, \dots, y_n)$.

2.4 Corps de décomposition d'un polynôme et résolubilité par radicaux

Dans les cours classiques de théorie de Galois, la notion de *corps de décomposition* d'un polynôme est assez longue à développer parce qu'on travaille avec des corps quelconques. Pour nous qui ne sortirons pas de $\mathbb{C}$, la notion est très facile à présenter grâce au théorème de d'Alembert-Gauss selon lequel tout polynôme non constant de $\mathbb{C}[X]$ est scindé sur $\mathbb{C}$.

Définition 2.4.1 **(Corps de décomposition d'un polynôme)** Soient K un sous-corps de $\mathbb{C}$ et $P \in K[X]$. On appelle *corps de décomposition de P sur K* la sous-K-extension $K(x_1, \dots, x_n)$ de $\mathbb{C}$ engendrée par les racines $x_1, \dots, x_n$ de P dans $\mathbb{C}$ comptées avec multiplicité, i.e. la plus petite sous-K-extension de $\mathbb{C}$ sur laquelle P est scindé.

Le corps de décomposition de P sur K est le plus petit monde dans lequel il est raisonnable d'étudier les racines de P pour, éventuellement, les exprimer par radicaux avec des coefficients dans K.

Exemple

- Le corps de décomposition de $X^2 - 2$ sur $\mathbb{Q}$ est $\mathbb{Q}\left(\sqrt{2}, -\sqrt{2}\right) = \mathbb{Q}(\sqrt{2})$.
- Le corps de décomposition de $X^2 - 4X - 7$ sur $\mathbb{Q}$ est $\mathbb{Q}\left(2 + \sqrt{11}, 2 - \sqrt{11}\right) = \mathbb{Q}(\sqrt{11})$.

- Le corps de décomposition de X^3-1 sur $\mathbb{Q}$ est $\mathbb{Q}\big(1,\mathrm{j},\mathrm{j}^2\big)=\mathbb{Q}\big(\mathrm{j}\big)$.
- Le corps de décomposition de X^3-2 sur $\mathbb{Q}$ est $\mathbb{Q}\big(\sqrt[3]{2},\mathrm{j}\sqrt[3]{2},\mathrm{j}^2\sqrt[3]{2}\big)=\mathbb{Q}\big(\sqrt[3]{2},\mathrm{j},\mathrm{j}^2\big)=\mathbb{Q}\big(\mathrm{j},\sqrt[3]{2}\big)$.

Pour finir, le vocabulaire des extensions radicales a été rapidement présenté dans l'introduction de ce texte, mais nous ne nous en servirons pas en réalité car la définition qui suit est suffisante.

Définition 2.4.2 **(Polynôme résoluble par radicaux)** Soient K un sous-corps de $\mathbb{C}$ et $P\in K[X]$. On dit que P est *résoluble par radicaux sur K* s'il existe des éléments $x_1,\dots,x_n\in\mathbb{C}$ et des entiers $r_1,\dots,r_n\in\mathbb{N}^*$ pour lesquels :

— P est scindé sur $K(x_1,\dots,x_n)$, autrement dit le corps de décomposition de P sur K est inclus dans $K(x_1,\dots,x_n)$,

— pour tout $i\in[\![1,n]\!]$: $\quad x_i^{r_i}\in K(x_1,\dots,x_{i-1})\quad$ avec par convention, pour $i=1$: $\quad K(x_1,\dots,x_{i-1})=K$.

Toute extension $K(x_1,\dots,x_n)$ du type de celle qui vient d'être décrite est dite *radicale sur K*.

Exemple Le polynôme $P=X^3+3X-2$ est résoluble par radicaux sur $\mathbb{Q}$.

Démonstration À ce stade, bien sûr, c'est en calculant ses racines que nous allons montrer cette propriété du polynôme P, mais à terme, nous saurons montrer qu'un polynôme est résoluble par radicaux sans calculer ses racines. En l'occurrence, les racines de P sont :

$$\sqrt[3]{\sqrt{2}+1}-\sqrt[3]{\sqrt{2}-1},\qquad \mathrm{j}\sqrt[3]{\sqrt{2}+1}-\mathrm{j}^2\sqrt[3]{\sqrt{2}-1}\qquad\text{et}\qquad \mathrm{j}^2\sqrt[3]{\sqrt{2}+1}-\mathrm{j}\sqrt[3]{\sqrt{2}-1}.$$

Le corps $\mathbb{Q}\Big(\sqrt{2},\sqrt[3]{\sqrt{2}+1},\mathrm{j}\Big)$ contient donc le corps de décomposition de P sur $\mathbb{Q}$ — il faut remarquer ici que : $\sqrt[3]{\sqrt{2}+1}\times\sqrt[3]{\sqrt{2}-1}=1$. Or comme requis par la définition de la résolubilité par radicaux :

$$\big(\sqrt{2}\big)^2=2\in\mathbb{Q},\qquad\Big(\sqrt[3]{\sqrt{2}+1}\Big)^3=\sqrt{2}+1\in\mathbb{Q}\big(\sqrt{2}\big)\qquad\text{et}\qquad \mathrm{j}^3=1\in\mathbb{Q}\Big(\sqrt{2},\sqrt[3]{\sqrt{2}+1}\Big).$$

CHAPITRE 3 ÉLÉMENTS ALGÉBRIQUES

3.1 ÉLÉMENTS ALGÉBRIQUES, ÉLÉMENTS TRANSCENDANTS

Définition-théorème 3.1.1 **(Élément algébrique, élément transcendant)** Soient K un corps, L une extension de K et $x \in L$. Les assertions suivantes sont équivalentes :

(i) Il existe un polynôme NON NUL $P \in K[X]$ pour lequel $P(x) = 0$.

(ii) La famille $\left(x^k\right)_{k\in\mathbb{N}}$ est K-liée dans L.

On dit dans ce cas que x est *algébrique sur* K, et dans le cas contraire que x est *transcendant sur* K.

Démonstration La donnée d'un polynôme $P = \sum_{k=0}^{+\infty} a_k X^k \in K[X]$ NON NUL pour lequel $P(x) = 0$ équivaut à la donnée d'une famille $(a_k)_{k\in\mathbb{N}} \in K^{\mathbb{N}}$ presque nulle mais NON NULLE pour laquelle $\sum_{k=0}^{+\infty} a_k x^k = 0$.

Exemple

- i est algébrique sur $\mathbb{Q}$, racine du polynôme $X^2+1 \in \mathbb{Q}[X]$.
- $\sqrt{2}$ est algébrique sur $\mathbb{Q}$, racine du polynôme $X^2-2 \in \mathbb{Q}[X]$.
- $\sqrt[3]{2}$ est algébrique sur $\mathbb{Q}$, racine du polynôme $X^3-2 \in \mathbb{Q}[X]$.
- $1+\mathrm{i}$ est algébrique sur $\mathbb{Q}$, racine du polynôme $X^2-2X+2 \in \mathbb{Q}[X]$ car $(1+\mathrm{i})^2 = 2\mathrm{i} = 2(1+\mathrm{i})-2$.
- $\sqrt{2}+\sqrt{3}$ est algébrique sur $\mathbb{Q}$, racine du polynôme $X^4-10X^2+1 \in \mathbb{Q}[X]$ car si on pose $x = \sqrt{2}+\sqrt{3}$, alors $x^2 = 5+2\sqrt{6}$, donc $\left(x^2-5\right)^2 = 24$, et enfin $x^4-10x^2+1 = 0$.

Exemple i, $\sqrt{2}$, $\sqrt[3]{2}$, $1+\mathrm{i}$ et $\sqrt{2}+\sqrt{3}$ sont aussi algébriques sur $\mathbb{R}$, puisque $\mathbb{Q}$ est inclus dans $\mathbb{R}$, donc $\mathbb{Q}[X]$ dans $\mathbb{R}[X]$!

Exemple On peut montrer que π et e sont transcendants — sous-entendu « sur $\mathbb{Q}$ » — mais c'est difficile.

3.2 POLYNÔME MINIMAL D'UN ÉLÉMENT ALGÉBRIQUE

Par définition, un élément algébrique est annulé par au moins un polynôme non nul, mais il l'est en fait toujours par une infinité. Par exemple, le polynôme X^2-2 admet $\sqrt{2}$ pour racine, mais c'est vrai aussi de tout multiple de X^2-2, par exemple $\left(X^2-2\right)\left(X^3+X+7\right)$. Il est clair cependant sur cet exemple que c'est X^2-2 qui admet $\sqrt{2}$ pour racine et non pas X^3+X+7. En ce sens, X^2-2 est meilleur que $\left(X^2-2\right)\left(X^3+X+7\right)$, X^2-2 est plus concis, plus essentiel. Plus généralement, que peut-on dire des polynômes annulateurs d'un élément algébrique ? Qui sont les meilleurs d'entre eux ? Un seul peut-être ?

Définition-théorème 3.2.1 **(Polynôme minimal et degré d'un élément algébrique)** Soient K un corps, L une extension de K et $x \in L$ algébrique sur K.

Il existe un et un seul polynôme unitaire $\Pi \in K[X]$ pour lequel pour tout $P \in K[X]$: $\quad P(x) = 0 \iff \Pi$ divise P. On l'appelle le *polynôme minimal de* x *sur* K et on le note $\pi_{x,K}$. Le degré de $\pi_{x,K}$ est aussi appelé le *degré de* x *sur* K.

En particulier, x est racine de $\pi_{x,K}$ et : $\quad \deg\left(\pi_{x,K}\right) \geqslant 1$. Enfin, $\pi_{x,K}$ est irréductible sur K.

Le polynôme minimal $\pi_{x,K}$ est d'abord minimal au sens de la divisibilité, ce qui veut dire que tout polynôme de $K[X]$ qui admet x pour racine est divisible par $\pi_{x,K}$. A fortiori, il est également de degré minimal dans l'ensemble des polynômes non nuls qui admettent x pour racine.

Démonstration On note I l'ensemble $\big\{P \in K[X] \mid \quad P(x) = 0\big\}$. Comme x est algébrique sur K : $\quad I \neq \{0\}$. L'ensemble des degrés des éléments de $I \setminus \{0\}$ est alors une partie non vide de $\mathbb{N}$, donc possède un plus petit élément d, disons $d = \deg(\Pi)$ pour un certain polynôme $\Pi \in I \setminus \{0\}$ que nous pouvons choisir unitaire.

Nous allons montrer que $I = \Pi K[X]$, i.e. que I est l'ensemble des polynômes de $K[X]$ divisibles par Π.

- Par définition de Π : $\quad \Pi(x) = 0, \quad$ i.e. x est racine de Π, mais x est donc aussi racine de tout élément de l'ensemble $\Pi K[X]$. Conclusion : $\quad \Pi K[X] \subset I$.
- Réciproquement, soit $P \in I$. Écrivons la division euclidienne de P par Π : $\quad P = \Pi Q + R \quad$ pour certains $Q, R \in K[X]$ avec $\deg(R) < d$. Or x est racine de P et Π, donc il l'est aussi de R, ce qui signifie que R appartient à I. Par minimalité de d enfin : $\quad R = 0, \quad$ i.e. Π divise P, ou encore $P \in \Pi K[X]$.

Et l'unicité de Π ? Si $\widetilde{\Pi}$ est un autre polynôme unitaire de $K[X]$ pour lequel $I = \widetilde{\Pi} K[X]$, Π et $\widetilde{\Pi}$ se divisent mutuellement, donc sont égaux puisqu'ils sont unitaires.

Pour l'irréductibilité de $\pi_{x,K}$, remarquons d'abord que $\pi_{x,K}$ n'est pas constant. Donnons-nous ensuite deux polynômes $A, B \in K[X]$ pour lesquels $\pi_{x,K} = AB$. Aussitôt : $\quad A(x)B(x) = 0, \quad$ donc comme K est intègre : $\quad A(x) = 0$ ou $\quad B(x) = 0, \quad$ donc $\pi_{x,K}$ divise A ou B. A fortiori, A ou B est constant non nul. ∎

En pratique, si un polynôme $P \in K[X]$ est unitaire, admet x pour racine et est irréductible sur K, alors $\pi_{x,K} = P$.

Exemple Soient K un corps, L une extension de K et $x \in L$. Alors : $\quad x \in K \iff \deg\big(\pi_{x,K}\big) = 1, \quad$ et dans ce cas : $\pi_{x,K} = X - x$.

Démonstration Si $x \in K$, le polynôme $X - x$ est unitaire à coefficients dans K, admet x pour racine et est irréductible sur K. Réciproquement, si $\deg\big(\pi_{x,K}\big) = 1$, forcément $\pi_{x,K} = X - x$ car $\pi_{x,K}$ est unitaire et admet x pour racine.

Exemple $\pi_{\mathrm{i},\mathbb{Q}} = X^2 + 1, \quad \pi_{\sqrt{2},\mathbb{Q}} = X^2 - 2, \quad \pi_{\sqrt[3]{2},\mathbb{Q}} = X^3 - 2 \quad$ et $\quad \pi_{\sqrt{2}+\sqrt{3},\mathbb{Q}} = X^4 - 10X^2 + 1.$

Démonstration Nous avons vu au chapitre **1** que les polynômes unitaires X^2+1, X^2-2, X^3-2 et X^4-10X^2+1 sont irréductibles sur $\mathbb{Q}$, et nous savons aussi qu'ils admettent respectivement i, $\sqrt{2}$, $\sqrt[3]{2}$ et $\sqrt{2}+\sqrt{3}$ pour racines.

Nous utiliserons régulièrement dans les prochains chapitres le petit résultat qui suit sans le rappeler chaque fois.

Théorème 3.2.2 **(À propos des racines d'un polynôme minimal)** Soient K un corps, L une extension de K et $x \in L$ algébrique sur K. Alors pour tout $y \in L$ racine de $\pi_{x,K}$: $\quad \pi_{x,K} = \pi_{y,K}$.

Démonstration Comme y est racine de $\pi_{x,K}$, $\pi_{y,K}$ divise $\pi_{x,K}$. Or $\pi_{x,K}$ est irréductible sur K et $\pi_{y,K}$ n'est pas constant, donc $\pi_{x,K} = \pi_{y,K}$. ∎

Exemple

- $\mathrm{j}\sqrt[3]{2}$ est racine de $X^3 - 2$ et $\pi_{\sqrt[3]{2},\mathbb{Q}} = X^3 - 2$, donc $\pi_{\mathrm{j}\sqrt[3]{2},\mathbb{Q}} = X^3 - 2$.
- Il n'est pas dur de vérifier que $\sqrt{2} - \sqrt{3}$ est racine de $X^4 - 10X^2 + 1$, or $\pi_{\sqrt{2}+\sqrt{3},\mathbb{Q}} = X^4 - 10X^2 + 1$, donc $\pi_{\sqrt{2}+\sqrt{3},\mathbb{Q}} = X^4 - 10X^2 + 1$.

3.3 Extensions finies et éléments algébriques

Au chapitre précédent, les égalités : $\quad \mathbb{R}(\mathrm{i}) = \mathbb{R}[\mathrm{i}] = \mathbb{C} \quad$ et $\quad \mathbb{Q}\big(\sqrt{2}\big) = \mathbb{Q}\big[\sqrt{2}\big] = \big\{a + b\sqrt{2} \mid \quad a, b \in \mathbb{Q}\big\} \quad$ pouvaient surprendre au premier abord quand on sait à quel point, pour tout corps K, $K(X)$ est plus gros que $K[X]$. Le théorème qui suit, fondamental, apporte à ces égalités un éclairage définitif. En résumé, l'algébricité est une propriété de finitude.

Théorème 3.3.1 (Caractérisation de l'algébricité d'un élément en termes d'extension finie) Soient K un corps, L une extension de K et $x \in L$.

$$x \text{ est algébrique sur } K \text{ si et seulement si } K(x) \text{ est une extension finie de } K.$$

Dans ce cas, si on pose $n = \deg(\pi_{x,K})$, alors $(1, x, x^2, \dots, x^{n-1})$ est une K-base de $K(x)$.
En particulier : $K(x) = K[x]$ et $[K(x) : K] = n$.

Démonstration

- Si x est transcendant sur K, la famille $(x^k)_{k\in\mathbb{N}}$ est K-libre dans L, mais aussi dans $K(x)$. En particulier, $K(x)$ est de dimension infinie comme K-espace vectoriel, i.e. comme extension de K.
- Supposons ensuite x algébrique sur K. Il nous suffit de montrer que la famille $(1, x, \dots, x^{n-1})$ est une K-base de $K(x)$.

  Liberté : Soient $\lambda_0, \dots, \lambda_{n-1} \in K$. Si $\lambda_0 + \dots + \lambda_{n-1}x^{n-1} = 0$, le polynôme $\lambda_{n-1}X^{n-1} + \dots + \lambda_1 X + \lambda_0$ admet x pour racine, donc est divisible par $\pi_{x,K}$, donc est nul pour une raison de degré. Conclusion : $\lambda_0 = \dots = \lambda_{n-1} = 0$.

  Caractère générateur : Par définition, $K(x)$ est l'ensemble des fractions rationnelles en x à coefficients dans K, mais nous voulons les transformer toutes en de simples combinaisons linéaires de $1, x, \dots, x^{n-1}$. Deux identités importantes vont nous y aider. Pour tout $P \in K[X]$:

  — si $P(x) \neq 0$, toute relation de Bézout entre $\pi_{x,K}$ et P transforme $\dfrac{1}{P(x)}$ en un polynôme en x,

  — la division euclidienne de P par $\pi_{x,K}$ transforme $P(x)$ en une combinaison linéaire de $1, x, \dots, x^{n-1}$.

  Détaillons. Pour le premier point, si x n'est pas racine de P, $\pi_{x,K}$ ne divise pas P, donc comme $\pi_{x,K}$ est irréductible, $\pi_{x,K}$ et P sont premiers entre eux, donc d'après le théorème de Bézout : $U\pi_{x,K} + VP = 1$ pour certains $U, V \in K[X]$. Après évaluation en x : $V(x)P(x) = 1$, donc $\dfrac{1}{P(x)} = V(x) \in K[x]$.

  Pour le deuxième point, écrivons la division euclidienne de P par $\pi_{x,K}$: $P = \pi_{x,K}Q + R$ avec $Q, R \in K[X]$ et $\deg(R) < n$. Après évaluation en x, $P(x) = R(x)$ est combinaison linéaire de $1, x, \dots, x^{n-1}$.

Exemple

- $\mathbb{Q}(\mathrm{i})$ admet $(1, \mathrm{i})$ comme $\mathbb{Q}$-base car $\pi_{\mathrm{i},\mathbb{Q}} = X^2 + 1$.
- $\mathbb{Q}(\sqrt{2})$ admet $(1, \sqrt{2})$ comme $\mathbb{Q}$-base car $\pi_{\sqrt{2},\mathbb{Q}} = X^2 - 2$.
- $\mathbb{Q}(\sqrt[3]{2})$ admet $\left(1, \sqrt[3]{2}, \left(\sqrt[3]{2}\right)^2\right)$ comme $\mathbb{Q}$-base car $\pi_{\sqrt[3]{2},\mathbb{Q}} = X^3 - 2$.

Exemple Quand nous avons illustré sur des exemples l'égalité : $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}] = \left\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\right\}$ au chapitre précédent, les dénominateurs de nos fractions rationnelles en $\sqrt{2}$ montaient au numérateur grâce à l'utilisation de quantités conjuguées dont on ne voit pas a priori la trace dans la preuve du théorème précédent. Et pourtant… Posons $x = \sqrt{2}$ et intéressons-nous par exemple à la quantité $2x + 3$. Au chapitre précédent, nous aurions écrit ceci :

$$\frac{1}{2x+3} = \frac{-2x+3}{(2x+3)(-2x+3)} = \frac{-2x+3}{9-4x} = \frac{-2x+3}{9-8} = -2x+3.$$

Dans le présent chapitre, on part d'une relation de Bézout entre $2X+3$ et $\pi_{\sqrt{2},\mathbb{Q}} = X^2 - 2$: $4\pi_{\sqrt{2},\mathbb{Q}} + (2X+3)(-2X+3) = 1$, puis on l'évalue en x : $(2x+3)(-2x+3) = 1$. On retrouve bien ainsi la relation $\dfrac{1}{2x+3} = -2x+3$.

En revanche, alors que les relations $\mathrm{i}^2 = -1$ et $\left(\sqrt{2}\right)^2 = 2$ permettent une définition simple des quantités conjuguées, on voit moins bien a priori comment la relation $\left(\sqrt[3]{2}\right)^3 = 2$ pourrait être exploitée dans un but analogue. Les relations de Bézout sont incontournables.

Exemple $\dfrac{1+\sqrt[3]{2}}{3+\sqrt[3]{2}} = \dfrac{11}{29} + \dfrac{6}{29}\sqrt[3]{2} - \dfrac{2}{29}\left(\sqrt[3]{2}\right)^2$.

Démonstration On pose : $x = \sqrt[3]{2}$ et on calcule d'une relation de Bézout entre $X+3$ et $\pi_{x,\mathbb{Q}} = X^3 - 2$: $(X+3)\left(X^2 - 3X + 9\right) - \pi_{x,\mathbb{Q}} = 29$. On l'évalue en x : $(x+3)\left(x^2 - 3x + 9\right) = 29$. Aussitôt :

$$\frac{x+1}{x+3} = (x+1) \times \frac{x^2-3x+9}{29} = \frac{x^3-2x^2+6x+9}{29} \overset{x^3=2}{=} \frac{-2x^2+6x+11}{29}.$$

En guise de conclusion au théorème **3.3.1**, remarquez bien que tout calcul qu'on fait dans $K(x)$ se ramène à un calcul polynomial dans lequel $\pi_{x,K}$ tient le rôle principal. On vient d'insister sur le calcul des inverses via le théorème de Bézout, mais c'est d'abord et surtout grâce à des divisions euclidiennes par $\pi_{x,K}$ qu'on additionne et qu'on multiplie dans $K(x)$.

Exemple $\left(2+\left(\sqrt[3]{2}\right)^2\right)\left(4+3\sqrt[3]{2}+\left(\sqrt[3]{2}\right)^4\right)=18+10\sqrt[3]{2}+4\left(\sqrt[3]{2}\right)^2$.

Démonstration On pose $x=\sqrt[3]{2}$ et on calcule la division euclidinne de $\left(X^2+2\right)\left(X^4+3X+4\right)$ par $\pi_{x,\mathbb{Q}}$:

$$\left(X^2+2\right)\left(X^4+3X+4\right)=X^6+2X^4+3X^3+4X^2+6X+8=\left(X^3+2X+5\right)\pi_{x,\mathbb{Q}}+4X^2+10X+18.$$

Il ne reste plus qu'à évaluer en x : $\left(x^2+2\right)\left(x^4+3x+4\right)=4x^2+10x+18$.

Théorème 3.3.2 **(Caractérisation de la finitude d'une extension en termes d'éléments algébriques)** Soient K un corps et L une extension de K. Les assertions suivantes sont équivalentes :

(i) L est une extension finie de K.

(ii) Il existe des éléments $x_1,\dots,x_n\in L$ algébriques sur K pour lesquels $L=K(x_1,\dots,x_n)$.

Dans ce cas : $K(x_1,\dots,x_n)=K[x_1,\dots,x_n]$ et $\left[K(x_1,\dots,x_n):K\right]\leqslant\prod_{i=1}^{n}\left[K(x_i):K\right]$.

Démonstration

(i) $\Longrightarrow$ (ii) Si L est une extension finie de K, nous pouvons nous en donner une base $(x_1,\dots,x_n)$. La sous-K-algèbre $K[x_1,\dots,x_n]$ de L contient alors $x_1,\dots,x_n$, donc coïncide avec L tout entier. A fortiori, pour une raison d'inclusion : $K(x_1,\dots,x_n)=K[x_1,\dots,x_n]$.

(ii) $\Longrightarrow$ (i) Faisons l'hypothèse que $L=K(x_1,\dots,x_n)$ pour certains $x_1,\dots,x_n\in L$ algébriques sur K. Pour tout $i\in[\![0,n-1]\!]$, $K(x_1,\dots,x_{i+1})$ est une extension de $K(x_1,\dots,x_i)$ engendrée par x_{i+1}. Or si on pose $n_i=\deg\left(\pi_{x_i,K}\right)$, la famille $\left(1,x_i,\dots,x_i^{n_i-1}\right)$ est K-liée, donc a fortiori $K(x_1,\dots,x_i)$-liée. Ainsi, d'après **3.3.1** notamment : $\left[K(x_1,\dots,x_{i+1}):K(x_1,\dots,x_i)\right]\leqslant n_i=\deg\left(\pi_{x_i,K}\right)=\left[K(x_i):K\right]$.

Il découle de ces majorations que $K(x_1,\dots,x_n)$ est une extension finie de K d'une part, mais aussi d'autre part que : $\left[K(x_1,\dots,x_n):K\right]=\prod_{i=0}^{n-1}\left[K(x_1,\dots,x_{i+1}):K(x_1,\dots,x_i)\right]\leqslant\prod_{i=0}^{n-1}\left[K(x_i):K\right]$. ∎

Exemple $\left[\mathbb{Q}\left(\mathrm{j},\sqrt[3]{2}\right):\mathbb{Q}\right]=6$.

Démonstration Pour commencer : $\pi_{\mathrm{j},\mathbb{Q}}=X^2+X+1$, donc $\left[\mathbb{Q}(\mathrm{j}):\mathbb{Q}\right]=2$. Du coup, d'après **3.3.2** : $\left[\mathbb{Q}\left(\mathrm{j},\sqrt[3]{2}\right):\mathbb{Q}\right]\leqslant\left[\mathbb{Q}(\mathrm{j}):\mathbb{Q}\right]\times\left[\mathbb{Q}\left(\sqrt[3]{2}\right):\mathbb{Q}\right]=2\times3=6$.

Ensuite : $\left[\mathbb{Q}\left(\mathrm{j},\sqrt[3]{2}\right):\mathbb{Q}\right]=\left[\mathbb{Q}\left(\mathrm{j},\sqrt[3]{2}\right):\mathbb{Q}(\mathrm{j})\right]\times\left[\mathbb{Q}(\mathrm{j}):\mathbb{Q}\right]$, donc $\left[\mathbb{Q}(\mathrm{j}):\mathbb{Q}\right]=2$ divise $\left[\mathbb{Q}\left(\mathrm{j},\sqrt[3]{2}\right):\mathbb{Q}\right]$. On montre de même que $\left[\mathbb{Q}\left(\sqrt[3]{2}\right):\mathbb{Q}\right]=3$ divise $\left[\mathbb{Q}\left(\mathrm{j},\sqrt[3]{2}\right):\mathbb{Q}\right]$. Le résultat en découle.

Le théorème qui suit n'est pas indispensable à notre propos, mais il découle du précédent et répond à une question naturelle — la somme et le produit de deux éléments algébriques sont-ils eux-mêmes algébriques ? Pour montrer par exemple que $\sqrt{2}+\sqrt{3}$ est algébrique sur $\mathbb{Q}$, nous avons dû trouver explicitement un polynôme non nul dont ce nombre est racine, mais d'après le théorème qui suit, il nous suffisait de savoir que $\sqrt{2}$ et $\sqrt{3}$ sont algébriques sur $\mathbb{Q}$, ce qui est beaucoup plus facile !

Théorème 3.3.3 **(Structure de corps sur l'ensemble des éléments algébriques d'une extension)** Soient K un corps et L une extension de K. L'ensemble des éléments de L algébriques sur K est une extension de K.

Démonstration Notons A l'ensemble des éléments de L algébriques sur K.

- Pour commencer, tout élément de K est algébrique sur K, donc A contient K — nous avons vu plus précisément que pour tout $x\in K$: $\pi_{x,K}=X-x$.
- Montrons ensuite que A est un corps, i.e. que A est stable par différence et quotient par un élément non nul. Soient $x,y\in A$. D'après le théorème **3.3.2**, x et y étant algébriques sur K, $K(x,y)$ est une extension finie de K.
  - L'extension $K(x,y)$ contient $x-y$, donc $K(x-y)$ tout entier. Or $K(x,y)$ est une extension finie de K, donc a fortiori $K(x-y)$ aussi, ce qui prouve que $x-y$ est algébrique sur K. Conclusion : $x-y\in A$.
  - Si $y\neq0$, on prouve de même que $\dfrac{x}{y}\in A$ par finitude de l'extension $K\left(\dfrac{x}{y}\right)$. ∎

La preuve qui précède a un défaut, elle n'est pas du tout constructive, i.e. ne permet aucun calcul explicite. Par exemple, il est facile d'affirmer de $\sqrt{2}+\sqrt[3]{2}$ est algébrique sur $\mathbb{Q}$, mais que valent son polynôme minimal et son degré ? Il se trouve que : $\pi_{\sqrt{2}+\sqrt[3]{2},\mathbb{Q}} = X^6-6X^4-4X^3+12X^2-24X-4$, mais quel lien avec $\pi_{\sqrt{2},\mathbb{Q}} = X^2-2$ et $\pi_{\sqrt[3]{2},\mathbb{Q}} = X^3-2$? Ce serait un peu trop long à expliquer ici, mais sachez qu'il est possible de calculer explicitement $\pi_{x+y,K}$ et $\pi_{xy,K}$ à partir de $\pi_{x,K}$ et $\pi_{y,K}$.

Nous terminerons cette partie par l'étude d'une famille d'extensions de $\mathbb{Q}$ assez naturelle, mais déjà pas simple à étudier.

Exemple Pour tous nombres premiers distincts $p_1,\dots,p_n$: $\left[\mathbb{Q}\left(\sqrt{p_1},\dots,\sqrt{p_n}\right):\mathbb{Q}\right] = 2^n$.

Plus précisément, la famille des nombres $\sqrt{p_1^{\varepsilon_1}\dots p_n^{\varepsilon_n}}$, $\varepsilon_1,\dots,\varepsilon_n$ décrivant $\{0,1\}$, est une $\mathbb{Q}$-base de $\mathbb{Q}\left(\sqrt{p_1},\dots,\sqrt{p_n}\right)$. Par exemple, $\left(1,\sqrt{2},\sqrt{3},\sqrt{6}\right)$ est une $\mathbb{Q}$-base de $\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)$.

Démonstration Nous allons en fait montrer que pour tous nombres premiers distincts $p_1,\dots,p_{n+1}$:

$$\left[\mathbb{Q}\left(\sqrt{p_1},\dots,\sqrt{p_{n+1}}\right):\mathbb{Q}\left(\sqrt{p_1},\dots,\sqrt{p_n}\right)\right] = 2,$$

ce qui revient aussi à dire que $\sqrt{p_{n+1}} \notin \mathbb{Q}\left(\sqrt{p_1},\dots,\sqrt{p_n}\right)$ car le polynôme X^2-p_{n+1} admet $\sqrt{p_{n+1}}$ pour racine. La conclusion souhaitée en découlera par simple produit :

$$\left[\mathbb{Q}\left(\sqrt{p_1},\dots,\sqrt{p_n}\right):\mathbb{Q}\right] = \prod_{i=0}^{n-1}\left[\mathbb{Q}\left(\sqrt{p_1},\dots,\sqrt{p_{i+1}}\right):\mathbb{Q}\left(\sqrt{p_1},\dots,\sqrt{p_i}\right)\right] = 2^n.$$

- Raisonnant par l'absurde, intéressons-nous à un entier n minimal et des nombres premiers distincts $p_1,\dots,p_{n+1}$ pour lequel le résultat est faux. En d'autres termes : $\sqrt{p_{n+1}} \in \mathbb{Q}\left(\sqrt{p_1},\dots,\sqrt{p_n}\right)$, mais pour tout $i \in [\![0,n-1]\!]$: $\left[\mathbb{Q}\left(\sqrt{p_1},\dots,\sqrt{p_{i+1}}\right):\mathbb{Q}\left(\sqrt{p_1},\dots,\sqrt{p_i}\right)\right] = 2$.
- En particulier, par produit : $\left[\mathbb{Q}\left(\sqrt{p_1},\dots,\sqrt{p_n}\right):\mathbb{Q}\right] = \prod_{i=0}^{n-1}\left[\mathbb{Q}\left(\sqrt{p_1},\dots,\sqrt{p_{i+1}}\right):\mathbb{Q}\left(\sqrt{p_1},\dots,\sqrt{p_i}\right)\right] = 2^n$.

  Or d'après **3.3.2** : $\mathbb{Q}\left(\sqrt{p_1},\dots,\sqrt{p_n}\right) = \mathbb{Q}\left[\sqrt{p_1},\dots,\sqrt{p_n}\right]$. Tout élément de $\mathbb{Q}\left(\sqrt{p_1},\dots,\sqrt{p_n}\right)$ peut donc être écrit comme une expression polynomiale à coefficients rationnels en les « variables » $\sqrt{p_1},\dots,\sqrt{p_n}$, et on peut même se contenter de puissances 0 ou 1 car pour tout $i \in [\![1,n]\!]$: $\sqrt{p_i}^{\,2} = p_i \in \mathbb{Q}$. La famille des nombres $\sqrt{p_1^{\varepsilon_1}\dots p_n^{\varepsilon_n}}$, $\varepsilon_1,\dots,\varepsilon_n$ décrivant $\{0,1\}$, engendre ainsi le $\mathbb{Q}$-espace vectoriel $\mathbb{Q}\left(\sqrt{p_1},\dots,\sqrt{p_n}\right)$, mais c'en est même une $\mathbb{Q}$-base pour une raison de dimension, que nous noterons $\mathscr{B}$.
- Revenons maintenant à notre hypothèse absurde :

  $$\sqrt{p_{n+1}} \in \mathbb{Q}\left(\sqrt{p_1},\dots,\sqrt{p_n}\right) = \mathbb{Q}\left(\sqrt{p_1},\dots,\sqrt{p_{k-1}},\sqrt{p_{k+1}},\dots,\sqrt{p_n}\right)\left(\sqrt{p_k}\right)$$

  et fixons $k \in [\![1,n]\!]$. Il existe des éléments $\alpha_k,\beta_k \in \mathbb{Q}\left(\sqrt{p_1},\dots,\sqrt{p_{k-1}},\sqrt{p_{k+1}},\dots,\sqrt{p_n}\right)$ pour lesquels $\sqrt{p_{n+1}} = \alpha_k + \beta_k\sqrt{p_k}$.

  — Par minimalité de n : $\sqrt{p_{n+1}} \notin \mathbb{Q}\left(\sqrt{p_1},\dots,\sqrt{p_{k-1}},\sqrt{p_{k+1}},\dots,\sqrt{p_n}\right)$, donc $\beta_k \neq 0$.

  — Mais par minimalité de n, il est également vrai que : $\sqrt{p_k} \notin \mathbb{Q}\left(\sqrt{p_1},\dots,\sqrt{p_{k-1}},\sqrt{p_{k+1}},\dots,\sqrt{p_n}\right)$.
  Comme par ailleurs : $p_{n+1} = \alpha_k^2 + 2\alpha_k\beta_k\sqrt{p_k} + p_k\beta_k^2$, on en tire ceci : $\alpha_k = 0$.

  Conclusion : $\sqrt{p_{n+1}} = \beta_k\sqrt{p_k}$, où β_k est combinaison linéaire des vecteurs de la base $\mathscr{B}$ dans lequel aucun $\sqrt{p_k}$ n'apparaît, et ceci est vrai pour tout $k \in [\![1,n]\!]$. Ces factorisations par $\sqrt{p_1},\dots,\sqrt{p_n}$ nous parlent en fait des coordonnées de $\sqrt{p_{n+1}}$ dans la base $\mathscr{B}$. Elles indiquent que la seule coordonnée éventuellement non nulle de $\sqrt{p_{n+1}}$ est sa coordonnée selon $\sqrt{p_1\dots p_n}$, seul vecteur de la base $\mathscr{B}$ dans lequel apparaissent à la fois $\sqrt{p_1},\dots,\sqrt{p_n}$. En d'autres termes : $\sqrt{p_{n+1}} = \dfrac{a}{b}\sqrt{p_1\dots p_n}$ pour certains $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Aussitôt : $b^2 p_{n+1} = a^2 p_1\dots p_n$, puis en termes de valuations p_{n+1}-adiques : $2v_{p_{n+1}}(b)+1 = 2v_{p_{n+1}}(a)$, et enfin modulo 2 : $1 \equiv 0\ [2]$ — contradiction.

3.4 Le théorème de l'élément primitif

Définition 3.4.1 **(Extension monogène)** Soient K un corps et L une extension de K. On dit que L est *monogène sur K* si $L = K(x)$ pour un certain $x \in L$. Un tel élément x est alors dit *primitif dans L sur K*.

D'après **3.3.1**, si l'extension L est à la fois monogène et finie, x est algébrique sur K.

Exemple $\mathbb{Q}\big(\sqrt{2},\sqrt{3}\big)$ est une extension monogène de $\mathbb{Q}$.

Démonstration Montrons que $\mathbb{Q}\big(\sqrt{2},\sqrt{3}\big) = \mathbb{Q}\big(\sqrt{2}+\sqrt{3}\big)$. L'inclusion $\mathbb{Q}\big(\sqrt{2}+\sqrt{3}\big) \subset \mathbb{Q}\big(\sqrt{2},\sqrt{3}\big)$ découle simplement de ce que $\sqrt{2}+\sqrt{3} \in \mathbb{Q}\big(\sqrt{2},\sqrt{3}\big)$. Pour l'inclusion inverse, posons $x = \sqrt{2}+\sqrt{3}$. D'après la formule du binôme : $x^3 = \big(\sqrt{2}\big)^3 + 3\big(\sqrt{2}\big)^2\sqrt{3} + 3\sqrt{2}\big(\sqrt{3}\big)^2 + \big(\sqrt{3}\big)^3 = 2\sqrt{2} + 6\sqrt{3} + 9\sqrt{2} + 3\sqrt{3} = 11\sqrt{2} + 9\sqrt{3}$, donc $x^3 - 9x = 2\sqrt{2}$, donc $\sqrt{2} = \dfrac{x^3-9x}{2} \in \mathbb{Q}(x)$. De même : $\sqrt{3} = \dfrac{11x-x^3}{2} \in \mathbb{Q}(x)$. Comme voulu : $\mathbb{Q}\big(\sqrt{2},\sqrt{3}\big) \subset \mathbb{Q}(x)$.

En particulier : $\big[\mathbb{Q}\big(\sqrt{2},\sqrt{3}\big) : \mathbb{Q}\big] = \big[\mathbb{Q}\big(\sqrt{2}+\sqrt{3}\big) : \mathbb{Q}\big] = \deg\big(\pi_{\sqrt{2}+\sqrt{3},\mathbb{Q}}\big) = \deg\big(X^4 - 10X^2 + 1\big) = 4$. Nous retrouvons ici à la main sur un exemple le résultat de l'exemple avancé par lequel nous avons conclu le paragraphe précédent.

L'extension $\mathbb{Q}\big(\sqrt{2},\sqrt{3}\big)$ est ainsi engendrée, au choix, soit par les deux éléments très simples $\sqrt{2}$ et $\sqrt{3}$, soit par le seul élément $\sqrt{2}+\sqrt{3}$, mais qui est plus compliqué à manipuler. Cette situation particulière s'avère en réalité d'une grande généralité. Le *théorème de l'élément primitif* et sa preuve montrent qu'on peut toujours réduire le nombre d'éléments algébriques qu'on utilise pour décrire une extension finie si on est prêt à les rendre plus « compliqués ». Ce qu'on perd en nombre, on le gagne en « complexité » et vice versa. En ce sens, le théorème de l'élément primitif est un théorème de conservation de la « complexité » pour les extensions finies.

Théorème 3.4.2 **(Théorème de l'élément primitif)** Soit K un sous-corps de $\mathbb{C}$. Toute sous-K-extension finie de $\mathbb{C}$ est monogène sur K.

Démonstration D'après **3.3.2**, toute extension finie de K est engendré par un nombre fini n d'éléments algébriques sur K. Nous n'avons rien à prouver si $n = 1$. Supposons désormais $n \geqslant 2$ et, raisonnant par récurrence, faisons l'hypothèse que le théorème de l'élément primitif est vrai de toute extension engendrée par strictement moins de n éléments.

Soit L une sous-K-extension de $\mathbb{C}$ engendrée par n éléments $x_1,\dots,x_n$: $L = K(x_1,\dots,x_n)$. Par hypothèse de récurrence : $K(x_2,\dots,x_n) = K(x_0)$ pour un certain $x_0 \in L$. En retour :

$$L = K(x_1,\dots,x_n) = K(x_2,\dots,x_n)(x_1) = K(x_0)(x_1) = K(x_0,x_1).$$

Soit $t \in K$ pour le moment quelconque. Posons $x = x_0 + tx_1$. Nous allons tâcher de montrer l'égalité $L = K(x)$, et il nous suffit pour cela de montrer que $x_1 \in K(x)$, car dans ce cas : $x_0 = x - tx_1 \in K(x)$.

Les polynômes $\pi_{x_1,K}$ — non nul — et $\pi_{x_0,K}(x-tX)$ de $K(x)[X]$ admettent tous les deux x_1 pour racine, donc possèdent un diviseur commun irréductible D. Si $\deg(D) = 1$: $D = X - x_1 \in K(x)[X]$, donc comme voulu $x_1 \in K(x)$. Se peut-il qu'on ait $\deg(D) > 1$? Supposons que ce soit le cas. Irréductible sur $K(x)$, D est à racines simples d'après **1.1.2**, donc possède une racine x_1' dans $\mathbb{C}$ autre que x_1. Par définition de D, x_1' est à la fois racine de $\pi_{x_1,K}$ et de $\pi_{x_0,K}(x-tX)$, donc $x - tx_1' = x_0'$ pour une certaine racine x_0' de $\pi_{x_0,K}$ dans $\mathbb{C}$, et par définition de x, du coup $t = -\dfrac{x_0-x_0'}{x_1-x_1'}$.
En résumé, si $\deg(D) > 1$, t est de la forme $-\dfrac{x_0-x_0'}{x_1-x_1'}$. Or ces quantités sont en nombre fini car d'une part x_0 et x_1 sont fixés, et d'autre part x_0' et x_1', respectivement racines de $\pi_{x_0,K}$ et $\pi_{x_1,K}$, ne peuvent prendre qu'un nombre fini de valeurs. De son côté, en tant que sous-corps de $\mathbb{C}$, K contient 1, donc $\mathbb{Z}$, donc $\mathbb{Q}$, donc est infini ! Finalement, nous avons choisi t quelconque dans K ci-dessus, mais nous pouvons lui imposer a posteriori de ne pas être de la forme $-\dfrac{x_0-x_0'}{x_1-x_1'}$, et dans ce cas, on l'a déjà dit : $\deg(D) = 1$, donc $x_1 \in K(x)$.

CHAPITRE 4 GROUPE DE GALOIS D'UNE EXTENSION

4.1 MORPHISMES D'ALGÈBRES

De même que les espaces vectoriels ont des sous-espaces vectoriels en eux et des applications linéaires entre eux, toute structure algébrique — groupe, anneau, corps, algèbre — a ses sous-structures et ce qu'on appelle ses *morphismes*. Un *morphisme d'espaces vectoriels*, par exemple, n'est rien d'autre qu'une application linéaire.

Définition 4.1.1 **(Morphisme d'anneaux, morphisme d'algèbres)**

- Soient A et B deux anneaux. On appelle *morphisme d'anneaux de A dans B* toute application $\varphi : A \longrightarrow B$ pour laquelle $\varphi(1) = 1$ et pour tous $x, y \in A$:
$$\varphi(x+y) = \varphi(x) + \varphi(y) \qquad \text{et} \qquad \varphi(xy) = \varphi(x)\varphi(y).$$
- Soient K un corps et A et B deux K-algèbres. On appelle *morphisme de K-algèbres (ou K-morphisme) de A dans B* toute application $\varphi : A \longrightarrow B$ pour laquelle $\varphi(1) = 1$ et pour tous $x, y \in A$ et $\lambda, \mu \in K$:
$$\varphi(\lambda x + \mu y) = \lambda\varphi(x) + \mu\varphi(y) \qquad \text{et} \qquad \varphi(xy) = \varphi(x)\varphi(y).$$
L'ensemble des K-morphismes de A dans B est noté $\mathrm{Hom}_K(A, B)$.

  En résumé, un morphisme d'algèbres est à la fois une application linéaire et un morphisme d'anneaux.

Un morphisme d'anneaux ou d'algèbres se comporte gentiment vis-à-vis de l'inversion. Pour tout $x \in A$ inversible, en effet : $x^{-1}x = 1$ donc $\varphi\big(x^{-1}\big)\varphi(x) = \varphi\big(x^{-1}x\big) = \varphi(1) = 1$, donc $\varphi\big(x^{-1}\big) = \varphi(x)^{-1}$.

Ensuite, comme en algèbre linéaire, on définit en théorie des anneaux et des algèbres les notions d'*endomorphisme*, d'*isomorphisme* et d'*automorphisme*. Par ailleurs, la composée de deux morphismes d'anneaux (resp. d'algèbres) est encore un morphisme d'anneaux (resp. d'algèbres), de même que la réciproque d'un isomorphisme.

Exemple La conjugaison complexe $z \longmapsto \overline{z}$ est un $\mathbb{R}$-automorphisme de $\mathbb{C}$.

Exemple Soit K un corps.

- Soit A une K-algèbre. L'application identité Id de A est un K-automorphisme de A.
- Soient L une extension de K et $x \in L$ fixé. L'application $P \longmapsto P(x)$ d'évaluation en x est un K-morphisme de $K[X]$ dans L.
- Pour toute matrice inversible $P \in \mathrm{GL}_n(K)$, l'application $M \longmapsto PMP^{-1}$ est un K-automorphisme de $\mathscr{M}_n(K)$.

Le petit résultat qui suit est à la fois totalement trivial et fondamental. Il raconte simplement que les morphismes d'algèbres préservent les expressions polynomiales, ce qui est assez clair par définition.

Théorème 4.1.2 **(Effet d'un K-morphisme sur une expression polynomiale)** Soient K un corps, A et B deux K-algèbres et $\varphi \in \mathrm{Hom}_K(A, B)$. Alors pour tous $a \in A$ et $P \in K[X]$: $\varphi\big(P(a)\big) = P\big(\varphi(a)\big)$. En particulier, si P annule a dans A, il annule $\varphi(a)$ dans B.

Démonstration On introduit les coefficients de P : $P = p_n X^n + \ldots + p_1 X + p_0$ avec $p_0, \ldots, p_n \in K$. Or φ préserve les produits et les combinaisons linéaires à coefficients dans K, donc :

$$P\big(\varphi(a)\big) = \sum_{k=0}^{n} p_k \varphi(a)^k = \sum_{k=0}^{n} p_k \varphi\big(a^k\big) = \varphi\left(\sum_{k=0}^{n} p_k a^k\right) = \varphi\big(P(a)\big).$$

Théorème 4.1.3 **(Deux propriétés importantes des morphismes d'algèbres entre extensions)** Soient K un corps, L et M deux extensions de K et $\varphi \in \mathrm{Hom}_K(L,M)$.

(i) φ fixe K, autrement dit pour tout $\lambda \in K$: $\varphi(\lambda) = \lambda$.

(ii) φ est injectif.

D'après (i), un K-morphisme entre extensions de K n'est jamais qu'un morphisme d'anneaux qui fixe K — et ce point de vue sera essentiel dans la suite de notre aventure. En effet, si φ est un morphisme d'anneaux qui fixe K, alors pour tous $x, y \in L$ et $\lambda, \mu \in K$: $\varphi(\lambda x + \mu y) = \varphi(\lambda)\varphi(x) + \varphi(\mu)\varphi(y) = \lambda\varphi(x) + \mu\varphi(y)$, donc φ est aussi K-linéaire.

Démonstration

(i) Pour tout $\lambda \in K$: $\varphi(\lambda) = \varphi(\lambda 1) = \lambda\varphi(1) = \lambda$.

(ii) Montrons que $\mathrm{Ker}\,\varphi = \{0\}$. Soit $x \in L$ pour lequel $\varphi(x) = 0$. Si $x \neq 0$, alors comme L est un corps, x est inversible, donc : $1 = \varphi(1) = \varphi\big(x^{-1}x\big) = \varphi\big(x^{-1}\big)\underbrace{\varphi(x)}_{=0} = 0$ — contradiction. Conclusion : $x = 0$.

Le théorème suivant est un résultat d'unicité pour les morphismes d'algèbres, selon lequel un morphisme d'algèbres est entièrement déterminé par la donnée de ses valeurs sur une famille d'éléments générateurs de l'algèbre de départ. Nous nous pencherons sur l'existence de tels morphismes au prochain paragraphe.

Théorème 4.1.4 **(Détermination d'un morphisme d'algèbres sur une partie génératrice)** Soient K un corps, L une extension finie de K engendrée par des éléments $x_1, \ldots, x_n$ et M une extension de K.

L'application $\varphi \longmapsto \big(\varphi(x_1), \ldots, \varphi(x_n)\big)$ est injective de $\mathrm{Hom}_K(L,M)$ dans M^n.

Démonstration Soient $\varphi, \varphi' \in \mathrm{Hom}_K(L,M)$. On suppose que pour tout $i \in [\![1,n]\!]$: $\varphi(x_i) = \varphi'(x_i)$. Nous allons montrer que l'ensemble $E = \big\{x \in L \mid \varphi(x) = \varphi'(x)\big\}$ est une sous-K-extension de L. Comme il contient K d'après **4.1.3** et $x_1, \ldots, x_n$ par hypothèse, on aura montré que $E = L$, autrement dit que $\varphi = \varphi'$.

Or pour tous $x, y \in E$ et $\lambda, \mu \in K$: $\varphi(\lambda x + \mu y) = \lambda\varphi(x) + \mu\varphi(y) \overset{x,y \in E}{=} \lambda\varphi'(x) + \mu\varphi'(y) = \varphi'(\lambda x + \mu y)$, donc $\lambda x + \mu y \in E$, et si $x \neq 0$: $\varphi\left(\frac{y}{x}\right) = \frac{\varphi(y)}{\varphi(x)} \overset{x,y \in E}{=} \frac{\varphi'(y)}{\varphi'(x)} = \varphi'\left(\frac{y}{x}\right)$, donc $\frac{y}{x} \in E$.

4.2 Construction de morphismes d'algèbres

La théorie de Galois va nous obliger à manipuler et construire beaucoup de morphismes d'algèbres. En algèbre linéaire, nous savons construire des applications linéaires à foison en les définissant seulement sur une base de l'espace de départ. Nous nous intéressons dans ce paragraphe à des résultats analogues adaptés à la structure d'algèbre.

Théorème 4.2.1 **(Prolongement polynomial d'un morphisme d'algèbres)** Soient K un corps, L et M deux extensions de K et $\varphi \in \mathrm{Hom}_K(L,M)$. Il existe un et un seul K-morphisme φ_X de $L[X]$ dans $M[X]$ prolongeant φ pour lequel $\varphi_X(X) = X$.

Par exemple, le $\mathbb{R}$-automorphisme $z \longmapsto \overline{z}$ de $\mathbb{C}$ se prolonge en un $\mathbb{R}$-endomorphisme $P \longmapsto \overline{P}$ de $\mathbb{C}[X]$ de la manière suivante — pour tout $P = \sum_{k=0}^{+\infty} a_k X^k \in \mathbb{C}[X]$: $\overline{P} = \sum_{k=0}^{+\infty} \overline{a_k} X^k$.

Démonstration

- **Analyse :** On suppose qu'il existe un K-morphisme φ_X de $L[X]$ dans $M[X]$ prolongeant φ. Alors pour tout $P = \sum_{k=0}^{+\infty} a_k X^k \in L[X]$: $\varphi_X(P) = \sum_{k=0}^{+\infty} \varphi_X(a_k)\,\varphi_X(X)^k = \sum_{k=0}^{+\infty} \varphi(a_k) X^k$.
- **Synthèse :** Notons φ_X l'unique application définie par l'expression précédente. Il est bien clair que φ_X prolonge φ car pour tout $t \in L$: $\varphi_X(t) = \varphi_X\big(t X^0 + 0X^1 + \dots\big) = \varphi(t)X^0 + \varphi(0)X^1 + \dots = \varphi(t)$. En particulier : $\varphi_X(1) = 1$.

  Il nous reste à montrer que : $\varphi_X(\lambda P + \mu Q) = \lambda\varphi_X(P) + \mu\varphi_X(Q)$ et $\varphi_X(PQ) = \varphi_X(P)\,\varphi_X(Q)$ pour tous $P = \sum_{k=0}^{+\infty} a_k X^k, Q = \sum_{k=0}^{+\infty} b_k X^k \in L[X]$ et $\lambda, \mu \in K$. Or :

$$\varphi_X(\lambda P+\mu Q) = \sum_{k=0}^{+\infty} \varphi(\lambda a_k+\mu b_k)X^k = \sum_{k=0}^{+\infty} \big(\lambda\varphi(x_k)+\mu\varphi(b_k)\big)X^k = \lambda\sum_{k=0}^{+\infty} \varphi(a_k)X^k+\mu\sum_{k=0}^{+\infty} \varphi(b_k)X^k = \lambda\varphi_X(P)+\mu\varphi_X(Q)$$

et : $$\varphi_X(PQ) = \varphi_X\left(\sum_{k=0}^{+\infty}\left(\sum_{i=0}^{k} a_i b_{k-i}\right)X^k\right) = \sum_{k=0}^{+\infty}\varphi\left(\sum_{i=0}^{k} a_i b_{k-i}\right)X^k = \sum_{k=0}^{+\infty}\left(\sum_{i=0}^{k}\varphi(a_i)\,\varphi(b_{k-i})\right)X^k$$
$$= \left(\sum_{k=0}^{+\infty}\varphi(a_k)X^k\right)\left(\sum_{k=0}^{+\infty}\varphi(b_k)X^k\right) = \varphi_X(P)\,\varphi_X(Q).$$

Rappelons à présent qu'il est très facile de construire des applications $\mathbb{R}$-linéaires de $\mathbb{Q}(\mathrm{i})$ dans $\mathbb{C}$. Parce que la famille $(1, \mathrm{i})$ est une $\mathbb{Q}$-base de $\mathbb{Q}(\mathrm{i})$, tout choix arbitraire de deux éléments $f(1)$ et $f(\mathrm{i})$ dans $\mathbb{C}$ définit une et une seule application $\mathbb{Q}$-linéaire f, ce qui laisse beaucoup de marge. Est-il aussi facile de construire un $\mathbb{Q}$-morphisme de $\mathbb{Q}(\mathrm{i})$ dans $\mathbb{C}$? Il faut pour cela imposer au moins la relation $f(1) = 1$, mais pas seulement. Les égalités $f(\mathrm{i})^2 = f\big(\mathrm{i}^2\big) = f(-1) = -1$ montrent que $f(\mathrm{i})$ doit être racine du polynôme $X^2 + 1$, autrement dit que $f(\mathrm{i})$ doit valoir $\pm\mathrm{i}$. Ainsi, s'il existe des $\mathbb{Q}$-morphismes de $\mathbb{Q}(\mathrm{i})$ dans $\mathbb{C}$, ils sont au plus deux. Inversement, il en existe bien deux, tout simplement les applications Id et $z \longmapsto \overline{z}$. Sous ses airs moins hospitaliers, le théorème qui suit ne dit pas grand-chose de plus.

Théorème 4.2.2 **(Construction d'un morphisme d'algèbres)** Soient K un sous-corps de $\mathbb{C}$, $x \in \mathbb{C}$ algébrique sur K et y une racine de $\pi_{x,K}$ dans $\mathbb{C}$. Il existe un et un seul K-morphisme φ de $K(x)$ dans $\mathbb{C}$ pour lequel $\varphi(x) = y$.

Nous démontrerons en fait une version un peu plus générale de ce résultat, qui ne nous servira jamais en pratique mais dont nous aurons besoin à la fin de ce paragraphe.

Théorème 4.2.3 **(Construction d'un morphisme d'algèbres, généralisation)** Soient K un sous-corps de $\mathbb{C}$, L une sous-K-extension de $\mathbb{C}$, $\varphi \in \mathrm{Hom}_K(L, \mathbb{C})$, $x \in \mathbb{C}$ algébrique sur L et y une racine de $\varphi_X\big(\pi_{x,L}\big)$ dans $\mathbb{C}$. Il existe un et un seul K-morphisme $\overline{\varphi}$ de $L(x)$ dans $\mathbb{C}$ prolongeant φ pour lequel $\overline{\varphi}(x) = y$.

On retrouve l'énoncé du théorème **4.2.2** pour $L = K$ et $\varphi = \mathrm{Id}$.

Démonstration On pose $n = \deg\big(\pi_{x,L}\big)$.

- **Analyse :** Faisons l'hypothèse qu'il existe un K-morphisme $\overline{\varphi}$ de $L(x)$ dans $\mathbb{C}$ prolongeant φ pour lequel $\overline{\varphi}(x) = y$. La famille $\big(1, x, \dots, x^{n-1}\big)$ est une L-base de $L(x)$ d'après **3.3.1**. Pour tout $z \in L(x)$ de coordonnées $(z_0, \dots, z_{n-1})$ dans cette L-base :
$$\overline{\varphi}(z) = \overline{\varphi}\left(\sum_{k=0}^{n-1} z_k x^k\right) = \sum_{k=0}^{n-1}\overline{\varphi}(z_k)\,\overline{\varphi}(x)^k = \sum_{k=0}^{n-1}\varphi(z_k)\,y^k.$$
- **Synthèse :** Notons $\overline{\varphi}$ l'unique application définie par l'expression précédente. Il est bien clair que $\overline{\varphi}$ prolonge φ car pour tout $t \in L$, les coordonnées de t dans la L-base $\big(1, x, \dots, x^{n-1}\big)$ sont $(t, 0, \dots, 0)$, donc : $\overline{\varphi}(t) = \varphi(t)\,y^0 + \varphi(0)\,y^1 + \dots + \varphi(0)\,y^{n-1} = \varphi(t)$. En particulier : $\overline{\varphi}(1) = \varphi(1) = 1$.

  Pour montrer que $\overline{\varphi}$ est un K-morphisme, il nous reste à montrer que : $\overline{\varphi}(\lambda z + \lambda' z') = \lambda\overline{\varphi}(z) + \lambda'\overline{\varphi}(z')$ et $\overline{\varphi}(zz') = \overline{\varphi}(z)\,\overline{\varphi}(z')$ pour tous $z, z' \in L(x)$ de coordonnées respectives $(z_0, \dots, z_{n-1}), (z'_0, \dots, z'_{n-1})$ dans la L-base $\big(1, x, \dots x^{n-1}\big)$ et pour tous $\lambda, \lambda' \in K$. Or :

$$\overline{\varphi}(\lambda z+\lambda' z') = \sum_{k=0}^{n-1} \varphi(\lambda z_k+\lambda' z'_k)y^k = \sum_{k=0}^{n-1} \big(\lambda\varphi(z_k)+\lambda'\varphi(z'_k)\big)y^k = \lambda\sum_{k=0}^{n-1} \varphi(z_k)y^k+\lambda'\sum_{k=0}^{n-1} \varphi(z'_k)y^k = \lambda\overline{\varphi}(z)+\lambda'\overline{\varphi}(z').$$

Pour la suite, partons de la division euclidienne de $\left(\sum_{k=0}^{n-1} z_k X^k\right)\left(\sum_{k=0}^{n-1} z'_k X^k\right)$ par $\pi_{x,L}$:

$$\clubsuit \quad \left(\sum_{k=0}^{n-1} z_k X^k\right)\left(\sum_{k=0}^{n-1} z'_k X^k\right) = \pi_{x,L} Q + \sum_{k=0}^{n-1} r_k X^k \qquad \text{pour certains } Q \in L[X] \text{ et } r_0, \dots, r_{n-1} \in L,$$

et transformons-la par le K-morphisme φ_X :

$$\spadesuit \quad \left(\sum_{k=0}^{n-1} \varphi(z_k) X^k\right)\left(\sum_{k=0}^{n-1} \varphi(z'_k) X^k\right) = \varphi_X\big(\pi_{x,L}\big)\,\varphi_X(Q) + \sum_{k=0}^{n-1} \varphi(r_k) X^k.$$

Évaluons finalement $\clubsuit$ en x : $zz' = \sum_{k=0}^{n-1} r_k x^k$, puis $\spadesuit$ en y : $\overline{\varphi}(z)\overline{\varphi}(z') = \sum_{k=0}^{n-1} \varphi(r_k) y^k$ en n'oubliant pas que y est racine de $\varphi_X\big(\pi_{x,L}\big)$. Ainsi : $\varphi(zz') = \varphi\left(\sum_{k=0}^{n-1} r_k x^k\right) = \sum_{k=0}^{n-1} \varphi(r_k) y^k = \overline{\varphi}(z)\overline{\varphi}(z')$. ∎

Théorème 4.2.4 **(Nombre de morphismes d'algèbres d'une extension finie à valeurs dans $\mathbb{C}$)** Soient K un sous-corps de $\mathbb{C}$ et L une sous-K-extension finie de $\mathbb{C}$. Alors : $\big|\mathrm{Hom}_K(L,\mathbb{C})\big| = \big[L : K\big]$.

Démonstration D'après le théorème de l'élément primitif : $L = K(x)$ pour un certain $x \in L$ algébrique sur K. Il nous suffit dès lors de montrer que l'application $\varphi \longmapsto \varphi(x)$ est une bijection de $\mathrm{Hom}_K(L,\mathbb{C})$ sur l'ensemble des racines de $\pi_{x,K}$ dans $\mathbb{C}$, de cardinal $\deg\big(\pi_{x,K}\big) \overset{3.3.1}{=} \big[L : K\big]$. Le fait que $\varphi(x)$ soit une racine de $\pi_{x,K}$ pour tout $\varphi \in \mathrm{Hom}_K(L,\mathbb{C})$ découle directement de **4.1.2**. Quant à la bijectivité de $\varphi \longmapsto \varphi(x)$, c'est une autre manière d'énoncer **4.2.2**. ∎

Théorème 4.2.5 **(Prolongement de morphismes d'algèbres à valeurs dans $\mathbb{C}$)** Soient K un sous-corps de $\mathbb{C}$, M une sous-K-extension de $\mathbb{C}$ et L une sous-K-extension de M. Si M est finie sur L, tout K-morphisme de L dans $\mathbb{C}$ peut alors être prolongé en un K-morphisme de M dans $\mathbb{C}$.

Démonstration Soit $\varphi \in \mathrm{Hom}_K(L,\mathbb{C})$. D'après le théorème de l'élément primitif : $M = L(x)$ pour un certain $x \in M$ algébrique sur L. En outre, d'après le théorème de d'Alembert-Gauss, le polynôme $\varphi_X\big(\pi_{x,L}\big)$ possède une racine y dans $\mathbb{C}$. Le théorème **4.2.3** garantit ainsi l'existence d'un K-morphisme $\overline{\varphi}$ de $M = L(x)$ dans $\mathbb{C}$ prolongeant φ pour lequel $\overline{\varphi}(x) = y$. ∎

4.3 Groupe de Galois d'une extension finie

Définition-théorème 4.3.1 **(Groupe de Galois d'une extension finie)** Soient K un sous-corps de $\mathbb{C}$ et L une sous-K-extension finie de $\mathbb{C}$. On appelle *groupe de Galois de L sur K* et on note $\mathrm{Gal}(L|K)$ l'ensemble des K-automorphismes de L, i.e. des automorphismes d'anneaux de L qui fixent K.

Comme son nom l'indique, $\mathrm{Gal}(L|K)$ est un groupe pour la composition des applications, et : $\big|\mathrm{Gal}(L|K)\big| \leqslant \big[L : K\big]$.

Démonstration Montrons que $\mathrm{Gal}(L|K)$ est un sous-groupe de S_L, le groupe symétrique de L, i.e. l'ensemble des bijections de L sur L. Pour commencer : $\mathrm{Gal}(L|K) \subset S_L$ et Id est bien un K-automorphisme de L. Ensuite, soient $g, g' \in \mathrm{Gal}(L|K)$. Montrons que $g^{-1}g' \in \mathrm{Gal}(L|K)$. Or déjà, nous savons bien que $g^{-1}g'$ est K-linéaire, et pour tous $x, y \in L$:

$$\begin{aligned} g^{-1}g'(xy) &= g^{-1}\big(g'(x)\,g'(y)\big) = g^{-1}\Big(gg^{-1}g'(x)\,gg^{-1}g'(y)\Big) \\ &= g^{-1}\Big(g\big(g^{-1}g'(x)\,g^{-1}g'(y)\big)\Big) = g^{-1}g'(x)\,g^{-1}g'(y). \end{aligned}$$

Pour finir : $\mathrm{Gal}(L|K) \subset \mathrm{Hom}_K(L,\mathbb{C})$, donc d'après **4.2.4** : $\big|\mathrm{Gal}(L|K)\big| \leqslant \big[L : K\big]$. ∎

Le petit résultat qui suit reformule simplement **4.1.2** dans le contexte des groupes de Galois.

Théorème 4.3.2 **(Action du groupe de Galois sur un élément algébrique)** Soient K un sous-corps de $\mathbb{C}$, L une sous-K-extension de $\mathbb{C}$ et $x \in L$ algébrique sur K. Alors pour tout $g \in \mathrm{Gal}(L|K)$, $g(x)$ est racine de $\pi_{x,K}$.

Exemple $\mathrm{Gal}(\mathbb{C}|\mathbb{R}) = \left\{\mathrm{Id}, z \longmapsto \overline{z}\right\}$.

Démonstration Pour tout $g \in \mathrm{Gal}(\mathbb{C}|\mathbb{R})$, $g(\mathrm{i})$ est racine de $\pi_{\mathrm{i},\mathbb{R}} = X^2+1$, donc $g(\mathrm{i})$ vaut $\pm\mathrm{i}$. Si $g(\mathrm{i}) = \mathrm{i}$, alors pour tout $z = x+\mathrm{i}y \in \mathbb{C}$ avec $x, y \in \mathbb{R}$: $g(z) = g(x+\mathrm{i}y) = g(x) + g(\mathrm{i})\,g(y) = x+\mathrm{i}y = z$, et dans l'autre cas : $g(z) = x - \mathrm{i}y = \overline{z}$. Inversement, Id et $z \longmapsto \overline{z}$ sont bien des $\mathbb{R}$-automorphismes de $\mathbb{C}$. ∎

Exemple $\mathrm{Gal}\left(\mathbb{Q}\left(\sqrt{2}\right)\middle|\mathbb{Q}\right) = \left\{\mathrm{Id}, \sigma\right\}$ si on note σ l'application $a+b\sqrt{2} \longmapsto a-b\sqrt{2}$ de $\mathbb{Q}\left(\sqrt{2}\right)$ dans lui-même.

Démonstration Comme dans l'exemple précédent, les seuls $\mathbb{Q}$-automorphismes possibles de $\mathbb{Q}\left(\sqrt{2}\right)$ sont Id et l'application σ… si toutefois elle est bien définie et constitue un $\mathbb{Q}$-automorphisme, ce qui n'a rien d'évident !

Or justement, d'après **4.2.2**, $-\sqrt{2}$ étant racine de $\pi_{\sqrt{2},\mathbb{Q}} = X^2-2$, il existe un et un seul $\mathbb{Q}$-endomorphisme σ de $\mathbb{Q}\left(\sqrt{2}\right)$ pour lequel $\sigma\left(\sqrt{2}\right) = -\sqrt{2}$. Plus explicitement : $\sigma\left(a+b\sqrt{2}\right) = a\sigma(1) + b\sigma\left(\sqrt{2}\right) = a-b\sqrt{2}$ pour tous $a, b \in \mathbb{Q}$. Pour finir, injectif d'après **4.1.3**, σ est un $\mathbb{Q}$-automorphisme de $\mathbb{Q}\left(\sqrt{2}\right)$ pour une raison de dimension.

Exemple $\mathrm{Gal}\left(\mathbb{Q}\left(\sqrt[3]{2}\right)\middle|\mathbb{Q}\right) = \left\{\mathrm{Id}\right\}$.

Démonstration On pose $x = \sqrt[3]{2}$. Soit $g \in \mathrm{Gal}\left(\mathbb{Q}(x)\middle|\mathbb{Q}\right)$. Alors $g(x)$ est une racine de $\pi_{x,\mathbb{Q}} = X^3-2$ dans $\mathbb{Q}(x)$, donc forcément $g(x) = x$ car les deux autres racines $\mathrm{j}x$ et j^2x de X^3-2 ne sont pas réelles alors que $\mathbb{Q}(x) \subset \mathbb{R}$. A fortiori $g\left(x^2\right) = g(x)^2 = x^2$, donc g fixe la $\mathbb{Q}$-base $\left(1, x, x^2\right)$ de $\mathbb{Q}(x)$. Par $\mathbb{Q}$-linéarité enfin : $g = \mathrm{Id}$.

Dans cet exemple, l'extension $\mathbb{Q}\left(\sqrt[3]{2}\right)$ n'est pas assez grosse pour posséder un $\mathbb{Q}$-automorphisme autre que l'identité. Pour que de tels $\mathbb{Q}$-automorphismes existent, il aurait fallu que $\mathbb{Q}\left(\sqrt[3]{2}\right)$ contiennent d'autres racines de X^3-2 que $\sqrt[3]{2}$ lui-même. Hélas, $\mathbb{Q}\left(\sqrt[3]{2}\right)$ n'est pas le corps de décomposition de X^3-2 sur $\mathbb{Q}$ — qui, rappelons-le, vaut $\mathbb{Q}\left(\sqrt[3]{2}, \mathrm{j}\sqrt[3]{2}, \mathrm{j}^2\sqrt[3]{2}\right) = \mathbb{Q}\left(\mathrm{j}, \sqrt[3]{2}\right)$. Nous ne nous intéresserons d'ailleurs plus désormais qu'à des corps de décomposition. Pourquoi ? En résumé, pour que les polynômes y aient assez de racines, et donc que les groupes de Galois associés soient assez gros. Nous ne saurons faire parler les groupes de Galois qu'à cette condition.

4.4 Extensions galoisiennes

La théorie de Galois à proprement parler ne s'intéresse pas à toutes les extensions d'un corps, mais seulement à certaines d'entre elles, dites *galoisiennes*. La définition que nous en donnons ci-dessous donnera à tort l'impression que le mot « galoisien » n'est qu'un mot inutile pour dire « corps de décomposition ». C'est vrai parce que nous travaillons dans $\mathbb{C}$ dans ce texte, mais les extensions galoisiennes sont un peu plus que cela dans le cas général.

Définition-théorème 4.4.1 **(Extension galoisienne)** Soient K un sous-corps de $\mathbb{C}$ et L une sous-K-extension finie de $\mathbb{C}$. Les assertions suivantes sont équivalentes :

(i) L est le corps de décomposition sur K d'un polynôme de $K[X]$.

(ii) $\left|\mathrm{Gal}(L|K)\right| = \left[L : K\right]$.

(iii) Pour tout $x \in L$, $\pi_{x,K}$ est scindé sur L.

On dit dans ce cas que L est *galoisienne sur* K.

L'équivalence des assertions (i) et (ii) est fondamentale et sa preuve mérite d'être parfaitement comprise.

— Tout d'abord, un K-morphisme de L dans $\mathbb{C}$ envoie toute racine d'un polynôme sur une autre racine de ce même polynôme d'après **4.1.2**. Dans le cas où L est le corps de décomposition sur K d'un certain polynôme P, tout K-morphisme de L dans $\mathbb{C}$ envoie donc toute racine de P sur une autre racine de P, donc envoie L sur L. Conclusion : $\mathrm{Gal}(L|K) = \mathrm{Hom}_K(L, \mathbb{C})$. Dans le cas général, seule l'inclusion $\mathrm{Gal}(L|K) \subset \mathrm{Hom}_K(L, \mathbb{C})$ est vraie.

— Ensuite, d'après **4.2.4** : $\left|\mathrm{Hom}_K(L, \mathbb{C})\right| = \left[L : K\right]$, donc si L est un corps de décomposition : $\left|\mathrm{Gal}(L|K)\right| = \left[L : K\right]$.

Démonstration

(i) $\Longrightarrow$ (ii) D'après **4.2.4** : $\left|\mathrm{Hom}_K(L,\mathbb{C})\right| = \left[L:K\right]$, et clairement $\mathrm{Gal}(L|K) \subset \mathrm{Hom}_K(L,\mathbb{C})$, donc il nous suffit de montrer l'inclusion réciproque.

Soit $\varphi \in \mathrm{Hom}_K(L,\mathbb{C})$. Par hypothèse, L est le corps de décomposition d'un certain polynôme $P \in K[X]$ de racines distinctes $x_1,\dots,x_n \in L$. Or pour tout $i \in [\![1,n]\!]$, d'après **4.1.2**, $\varphi(x_i)$ est aussi racine de P, donc appartient à $L = K(x_1,\dots,x_n)$. A fortiori $\varphi(L) \subset L$. Or L étant un corps, φ est injectif d'après **4.1.3**, et comme L est de dimension finie sur K, cela suffit à prouver que φ est un automorphisme K-linéaire de L. Comme voulu : $\varphi \in \mathrm{Gal}(L|K)$.

(ii) $\Longrightarrow$ (iii) D'après **4.2.4** : $\left|\mathrm{Hom}_K(L,\mathbb{C})\right| = \left[L:K\right]$, et par ailleurs $\mathrm{Gal}(L|K) \subset \mathrm{Hom}_K(L,\mathbb{C})$, donc l'assertion (iii) montre que $\mathrm{Hom}_K(L,\mathbb{C}) = \mathrm{Gal}(L|K)$.

Soit $x \in L$. Nous voulons montrer que $\pi_{x,K}$ est scindé sur L. Or en tout cas, $\pi_{x,K}$ est scindé sur $\mathbb{C}$ d'après le théorème de d'Alembert-Gauss. Soit $z \in \mathbb{C}$ une racine de $\pi_{x,K}$. D'après **4.2.2**, il existe un K-morphisme φ de $K(x)$ dans $\mathbb{C}$ pour lequel $\varphi(x) = z$, et d'après **4.2.5**, φ peut être prolongé en un K-morphisme de L dans $\mathbb{C}$ que nous noterons encore φ. L'égalité $\mathrm{Hom}_K(L,\mathbb{C}) = \mathrm{Gal}(L|K)$ montre alors que $\varphi(L) \subset L$, et donc en particulier que $z = \varphi(x) \in L$. Comme voulu, L contient toutes les racines de $\pi_{x,K}$ dans $\mathbb{C}$, autrement dit $\pi_{x,K}$ est scindé sur L.

(iii) $\Longrightarrow$ (i) D'après le théorème de l'élément primitif : $L = K(x)$ pour un certain $x \in L$ algébriques sur K. Or par hypothèse, $\pi_{x,K}$ est scindé sur L, donc L est le corps de décomposition de $\pi_{x,K}$ sur K. ∎

Nous venons de montrer en passant que dans le cas d'une extension galoisienne, pour toute racine de $\pi_{x,K}$ dans $\mathbb{C}$, il existe un K-automorphisme de L pour lequel $\varphi(x) = z$. Cette réciproque du théorème **4.3.2** justifie la définition suivante.

Définition-théorème 4.4.2 **(Conjugués d'un élément dans une extension galoisienne)** Soient K un sous-corps de $\mathbb{C}$, L une extension galoisienne de K et $x \in L$. Les assertions suivantes sont équivalentes :

(i) y est racine de $\pi_{x,K}$.

(ii) Pour un certain $g \in \mathrm{Gal}(L|K)$: $y = g(x)$.

On dit dans ce cas que y est un *conjugué de x dans L sur K*.

Si on note $x_1 = x, x_2, \dots, x_n$ les conjugués de x, alors pour tout $g \in \mathrm{Gal}(L|K)$, la restriction $g_{|\{x_1,\dots,x_n\}}$ est une injection de $\{x_1,\dots,x_n\}$ dans lui-même, mais donc déjà une bijection, autrement dit une permutation de $\{x_1,\dots,x_n\}$. On peut dire ainsi que le groupe $\mathrm{Gal}(L|K)$ *permute* les conjugués de x. Ce point de vue sera d'ailleurs bientôt approfondi.

Théorème 4.4.3 **(« Restriction » d'une extension galoisienne)** Soient K un sous-corps de $\mathbb{C}$, L une sous-K-extension de $\mathbb{C}$ et E une sous-K-extension de L. Si L est galoisienne sur K, elle l'est aussi sur E.

Attention, en revanche, E n'a aucune raison d'être galoisienne sur K, mais c'est justement un problème auquel la théorie de Galois apportera bientôt une réponse précise.

Démonstration Si L est galoisienne sur K : $L = K(x_1,\dots,x_n)$ pour un certain $P \in K[X]$ scindé sur L de racines $x_1,\dots,x_n$. Comme E est inclus dans L, il est aussitôt également vrai que $L = E(x_1,\dots,x_n)$, et on peut bien dire que P est à coefficients dans E. Ainsi, L est galoisienne sur E. ∎

Exemple Le corps de décomposition $\mathbb{Q}\big(\mathrm{j}, \sqrt[3]{2}\big)$ de X^3-2 sur $\mathbb{Q}$ est galoisien sur $\mathbb{Q}$, mais ce n'est pas le cas de la sous-extension $\mathbb{Q}\big(\sqrt[3]{2}\big)$, car elle contient $\sqrt[3]{2}$ sans que le polynôme $\pi_{\sqrt[3]{2},\mathbb{Q}}$ y soit scindé.

Cet exemple simple d'une extension de degré 3 non galoisienne contraste avec la situation générale des extensions de degré 2 que nous allons maintenant décrire.

Exemple Soit K un sous-corps de $\mathbb{C}$. Toute sous-K-extension de $\mathbb{C}$ de degré 2 est galoisienne sur K.

Démonstration Soit L une telle extension de K. Notons x un élément quelconque de $L \setminus K$. La famille $(1,x)$ est alors K-libre, donc est une K-base de L pour une raison de dimension. Il en découle que x^2 est combinaison K-linéaire de 1 et x, disons $x^2 = ax+b$ pour certains $a,b \in K$. Le polynôme X^2-aX-b admet ainsi x pour racine, et son autre racine dans $\mathbb{C}$ est $a-x$. Or $a-x \in L$, donc $L = K(x) = K(x,a-x)$, autrement dit L est le corps de décomposition de X^2-aX-b sur K. Comme voulu, L est galoisienne sur K.

4.5 Morphismes de groupes

Dans un cours d'algèbre classique, les *morphismes de groupes* sont les premiers morphismes qu'on a coutume d'introduire, avant les applications linéaires et les morphismes d'anneaux, mais j'ai décidé de n'introduire dans ce texte les concepts qu'à point nommé et a minima.

Les groupes abstraits de ce texte seront tous considérés comme des groupes multiplicatifs par convention et leur élément neutre sera noté simplement 1.

Définition 4.5.1 (Morphisme de groupes) Soient G et G' deux groupes. On appelle *morphisme de groupes de G dans G'* toute application $\varphi : G \longrightarrow G'$ pour laquelle pour tous $x, y \in G$: $\varphi(xy) = \varphi(x)\varphi(y)$.

En particulier : $\varphi(1)^2 = \varphi\big(1^2\big) = \varphi(1)$, donc après simplification par $\varphi(1)$ dans le groupe G' : $\varphi(1) = 1$. En outre, pour tout $x \in G$: $\varphi\big(x^{-1}\big) = \varphi(x)^{-1}$.

Comme les applications linéaires et les morphismes d'anneaux, les morphismes de groupes sont une façon de relier les groupes entre eux pour les comparer. Un morphisme de groupes φ de G dans G' transforme les relations dans G en des relations analogues dans G'. Par exemple, si $xyx = y$ avec $x, y \in G$, alors $x'y'x' = y'$ dans G' si on pose $x' = \varphi(x)$ et $y' = \varphi(y)$.

Parce que les espaces vectoriels, les anneaux et les algèbres sont des groupes additifs, leurs morphismes sont en particulier des morphismes de groupes. Par ailleurs, la théorie des groupes a elle aussi ses *endomorphismes*, ses *isomorphismes* et ses *automorphismes*, la composée de deux morphismes de groupes est encore un morphisme de groupes, de même que la réciproque d'un isomorphisme.

Exemple Toute proposition mathématique du genre : « Le machin des trucs est le truc des machins » cache un morphisme de groupes. Par exemple, l'exponentielle d'une somme est le produit des exponentielles, ou le carré d'un produit est le produit des carrés.

- La fonction $x \longmapsto x^2$ est un morphisme de groupes de $\mathbb{R}_+^*$ dans lui-même, et c'est même un automorphisme de réciproque $x \longmapsto \sqrt{x}$.
- L'exponentielle complexe est un morphisme de groupes de $\mathbb{C}$ dans $\mathbb{C}^*$.
- La fonction logarithme est un morphisme de groupes de $\mathbb{R}_+^*$ dans $\mathbb{R}$, et c'est même un isomorphisme de réciproque la fonction exponentielle sur $\mathbb{R}$.
- La fonction $k \longmapsto (-1)^k$ est un morphisme de groupes de $\mathbb{Z}$ dans $\big\{\pm 1\big\}$.
- Pour tout corps K, le déterminant est un morphisme de groupes de $\mathrm{GL}_n(K)$ dans $K \setminus \big\{0\big\}$.
- La signature ε est un morphisme de groupes de S_n dans $\big\{\pm 1\big\}$, où l'on rappelle que le groupe symétrique S_n est l'ensemble des permutations de $[\![1, n]\!]$.

Théorème 4.5.2 (Image d'un sous-groupe par un morphisme de groupes) Soient G et G' deux groupes, H un sous-groupe de G et $\varphi : G \longrightarrow G'$ un morphisme de groupes. L'image $\varphi(H)$ de H par φ est un sous-groupe de G'.

Dans le cas particulier où φ est injectif, la restriction $\varphi|_H$ est un isomorphisme de H sur son image $\varphi(H)$. On peut de cette manière identifier H à un sous-groupe de G', en l'occurrence $\varphi(H)$.

Démonstration D'abord : $1 = \varphi(1) \in \varphi(H)$ car $1 \in H$. Ensuite, pour tous $x', y' \in G'$, disons $x' = \varphi(x)$ et $y' = \varphi(y)$ avec $x, y \in G$: $x'^{-1}y' = \varphi(x)^{-1}\varphi(y) = \varphi\big(x^{-1}y\big) \in \varphi(H)$ car $x^{-1}y \in H$. ∎

4.6 Exemples de groupes de Galois

Comme nous l'avons déjà observé, le groupe de Galois d'une extension galoisienne « permute les conjugués ». Le théorème qui suit prolonge cette remarque et ramène le groupe de Galois d'une extension galoisienne à un sous-groupe de permutations. On rappelle à cette occasion que pour tout ensemble fini non vide X, l'ensemble des bijections de X sur lui-même, i.e. des permutations de X, est noté S_X et appelé le *groupe symétrique de X*. On l'appelle ainsi bien sûr car c'est un groupe, en l'occurrence pour la composition. En particulier, pour tout $n \in \mathbb{N}^*$: $S_n = S_{[\![1,n]\!]}$.

Théorème 4.6.1 **(Plongement du groupe de Galois dans un groupe symétrique)** Soient K un sous-corps de $\mathbb{C}$ et $P \in K[X]$. On note L le corps de décomposition de P sur K et $x_1, \dots, x_n$ les racines distinctes de P dans L. L'application $g \longmapsto g|_{\{x_1,\dots,x_n\}}$ est un morphisme de groupes injectif de $\mathrm{Gal}(L|K)$ dans le groupe symétrique $S_{\{x_1,\dots,x_n\}}$.

En particulier, on connaît complètement un K-automorphisme g de $\mathrm{Gal}(L|K)$ quand on connaît la manière dont il permute $x_1, \dots, x_n$. La permutation sous-jacente est en quelque sorte l'essence de g, une version simplifiée mais totale de g.

Si le théorème plonge $\mathrm{Gal}(L|K)$ dans $S_{\{x_1,\dots,x_n\}}$, nous pousserons généralement les choses plus loin par la suite et identifierons $\mathrm{Gal}(L|K)$ à un sous-groupe de $S_n = S_{[\![1,n]\!]}$ en identifiant 1 et x_1, 2 et x_2, …, n et x_n. Par exemple, pour $n = 3$, si un K-automorphisme g de L vérifie : $g(x_1) = x_2$, $g(x_2) = x_3$ et $g(x_3) = x_1$, nous identifierons g au 3-cycle (1 2 3), qui résume la manière dont g permute l'ensemble $\{x_1, x_2, x_3\}$. Autre exemple pour $n = 4$, si : $g(x_1) = x_2$, $g(x_2) = x_1$, $g(x_3) = x_4$ et $g(x_4) = x_3$, nous identifierons g à la permutation (1 2) (3 4).

Démonstration Nous avons déjà observé que le groupe $\mathrm{Gal}(L|K)$ permute les éléments conjugués $x_1, \dots, x_n$, cela justifie la bonne définition de l'application $g \overset{\iota}{\longmapsto} g|_{\{x_1,\dots,x_n\}}$ de $\mathrm{Gal}(L|K)$ dans $S_{\{x_1,\dots,x_n\}}$. Cette application ι est un morphisme de groupes car pour tous $g, g' \in \mathrm{Gal}(L|K)$: $(gg')|_{\{x_1,\dots,x_n\}} = g|_{\{x_1,\dots,x_n\}} g|_{\{x_1,\dots,x_n\}}$. Quant à son injectivité, elle découle directement du théorème **4.1.4** car $L = K(x_1, \dots, x_n)$. ∎

Exemple Nous avons déjà calculé le groupe de Galois de $\mathbb{C}$ sur $\mathbb{R}$: $\mathrm{Gal}(\mathbb{C}|\mathbb{R}) = \{\mathrm{Id}, z \longmapsto \overline{z}\}$. L'application $g \longmapsto g|_{\{\mathrm{i},-\mathrm{i}\}}$ est un morphisme de groupes injectif de $\mathrm{Gal}(\mathbb{C}|\mathbb{R})$ dans S_2 d'après **4.6.1** si on numérote i et $-$i respectivement 1 et 2, et comme $|S_2| = 2! = 2$, ce morphisme est même un isomorphisme. De cette manière, $\mathrm{Gal}(\mathbb{C}|\mathbb{R})$ peut être identifié au groupe S_2. On peut aussi l'identifier au groupe additif $\frac{\mathbb{Z}}{2\mathbb{Z}}$ car les groupes S_2 et $\frac{\mathbb{Z}}{2\mathbb{Z}}$ sont isomorphes via l'application : $\mathrm{Id} \longmapsto 0$ et $(1\ 2) \longmapsto 1$. Le tableau ci-dessous offre une vue synthétique des différentes identifications que l'on met ici en jeu par isomorphisme.

$\mathrm{Gal}(\mathbb{C}\|\mathbb{R})$	S_2	$\frac{\mathbb{Z}}{2\mathbb{Z}}$
Id	Id	0
$z \longmapsto \overline{z}$	(1 2)	1

Exemple On étudie de la même façon l'exemple de l'extension $L = \mathbb{Q}(\sqrt{2})$ de $\mathbb{Q}$, de groupe de Galois : $\mathrm{Gal}(L|\mathbb{Q}) = \{\mathrm{Id}, \sigma\}$ où σ est l'application $a + b\sqrt{2} \longmapsto a - b\sqrt{2}$. Dans le tableau ci-dessous, on a numéroté les nombres i et $-$i respectivement 1 et 2.

$\mathrm{Gal}(L\|\mathbb{Q})$	S_2	$\frac{\mathbb{Z}}{2\mathbb{Z}}$
Id	Id	0
σ	(1 2)	1

Exemple On s'intéresse maintenant au groupe de Galois de $L = \mathbb{Q}(\mathrm{j}, \sqrt[3]{2})$ sur $\mathbb{Q}$. On rappelle que $[L : \mathbb{Q}] = 6$ et que L est le corps de décomposition du polynôme $X^3 - 2$ sur $\mathbb{Q}$. À ce titre, L est galoisienne sur $\mathbb{Q}$, donc $|\mathrm{Gal}(L|\mathbb{Q})| = [L : \mathbb{Q}] = 6$, et l'application $g \longmapsto g|_{\{\sqrt[3]{2}, \mathrm{j}\sqrt[3]{2}, \mathrm{j}^2\sqrt[3]{2}\}}$ est un morphisme de groupes injectif de $\mathrm{Gal}(L|\mathbb{Q})$ dans S_3 d'après **4.6.1** si on numérote x, $\mathrm{j}x$ et $\mathrm{j}^2 x$ respectivement 1, 2 et 3. Comme $|S_3| = 3! = 6$, ce morphisme est même un isomorphisme. De cette manière, le groupe de Galois $\mathrm{Gal}(L|\mathbb{Q})$ peut être identifié au groupe S_3.

Ajoutons les détails à présent. Nous savons que : $S_3 = \{\mathrm{Id}, (1\ 2\ 3), (1\ 3\ 2), (1\ 2), (1\ 3), (2\ 3)\}$, mais à quels $\mathbb{Q}$-automorphismes de L ces permutations correspondent-elles ? Comme les $\mathbb{Q}$-automorphismes de L sont entièrement déterminés par leurs valeurs en j et en $\sqrt[3]{2}$ d'après **4.1.4**, nous pouvons représenter leur correspondance avec les éléments de S_3 sous la forme d'un tableau. Pour tout $g \in \mathrm{Gal}(L|\mathbb{Q})$, le calcul de $g(\mathrm{j})$ y est mené grâce à la relation $g(\mathrm{j}) = \dfrac{g(\mathrm{j}\sqrt[3]{2})}{g(\sqrt[3]{2})}$. Le résultat ne peut être que j ou j^2 car j est racine du polynôme $X^2 + X + 1 = (X - \mathrm{j})(X - \overline{\mathrm{j}})$. Par exemple, à quel $\mathbb{Q}$-automorphisme g la permutation (1 2) correspond-elle ? Par définition de cette permutation : $g(\sqrt[3]{2}) = \mathrm{j}\sqrt[3]{2}$, $g(\mathrm{j}\sqrt[3]{2}) = \sqrt[3]{2}$ et $g(\mathrm{j}^2\sqrt[3]{2}) = \mathrm{j}^2\sqrt[3]{2}$, donc $g(\mathrm{j}) = \dfrac{\sqrt[3]{2}}{\mathrm{j}\sqrt[3]{2}} = \mathrm{j}^2$.

Gal$(L\|\mathbb{Q})$ $g(\mathrm{j})$	Gal$(L\|\mathbb{Q})$ $g(\sqrt[3]{2})$	S_3
j	$\sqrt[3]{2}$	Id
j	$\mathrm{j}\sqrt[3]{2}$	(1 2 3)
j	$\mathrm{j}^2\sqrt[3]{2}$	(1 3 2)

Gal$(L\|\mathbb{Q})$ $g(\mathrm{j})$	Gal$(L\|\mathbb{Q})$ $g(\sqrt[3]{2})$	S_3
j^2	$\mathrm{j}\sqrt[3]{2}$	(1 2)
j^2	$\mathrm{j}^2\sqrt[3]{2}$	(1 3)
j^2	$\sqrt[3]{2}$	(2 3)

Exemple On s'intéresse ensuite au groupe de Galois de $L = \mathbb{Q}\big(\sqrt{2},\sqrt{3}\big)$ sur $\mathbb{Q}$. On rappelle que $\big[L : \mathbb{Q}\big] = 4$ et que $\mathbb{Q}\big(\sqrt{2},\sqrt{3}\big) = \mathbb{Q}\big(\sqrt{2}+\sqrt{3}\big)$ est le corps de décomposition du polynôme $X^4 - 10X^2 + 1$ sur $\mathbb{Q}$. Il sera plus pratique cela dit de voir L comme corps de décomposition du polynôme $\big(X^2-2\big)\big(X^2-3\big)$. À ce titre, L est galoisienne sur $\mathbb{Q}$, donc $\big|\mathrm{Gal}(L|\mathbb{Q})\big| = \big[L : \mathbb{Q}\big] = 4$.

- D'après **4.6.1**, l'application $g \longmapsto g_{|\{\sqrt{2},-\sqrt{2},\sqrt{3},-\sqrt{3}\}}$ est un morphisme de groupes injectif de $\mathrm{Gal}(L|\mathbb{Q})$ dans S_4 si on numérote $\sqrt{2}, -\sqrt{2}, \sqrt{3}$ et $-\sqrt{3}$ respectivement 1, 2, 3 et 4. La correspondance ainsi créée entre les $\mathbb{Q}$-automorphismes de L et les éléments de S_4 peut être représentée de nouveau sous forme de tableau — ci-dessous à gauche.
- Dans la mesure où, pour tout $g \in \mathrm{Gal}(L|\mathbb{Q})$, $g\big(\sqrt{2}\big)$ vaut $\pm\sqrt{2}$ et $g\big(\sqrt{3}\big)$ vaut $\pm\sqrt{3}$, on peut aussi s'intéresser à l'application $g \longmapsto (\varepsilon_2,\varepsilon_3)$ de $\mathrm{Gal}(L|\mathbb{Q})$ dans $\left(\dfrac{\mathbb{Z}}{2\mathbb{Z}}\right)^2$ définie par les relations : $\quad g\big(\sqrt{2}\big) = (-1)^{\varepsilon_3}\sqrt{2} \quad$ et $\quad g\big(\sqrt{3}\big) = (-1)^{\varepsilon_3}\sqrt{3}$. Le calcul de $(-1)^\varepsilon$ avec $\varepsilon \in \dfrac{\mathbb{Z}}{2\mathbb{Z}}$ ne pose pas de problème car pour tout $n \in \mathbb{Z}$, le calcul de $(-1)^n$ ne dépend que de n modulo 2. Il n'est pas dur de vérifier que cette application est un morphisme de groupes, injectif d'après **4.1.4** car tout $\mathbb{Q}$-automorphisme de L est entièrement caractérisé par l'image qu'il donne aux nombres $\sqrt{2}$ et $\sqrt{3}$. Ce morphisme de groupes s'avère finalement être un isomorphisme de groupes de $\mathrm{Gal}(L|\mathbb{Q})$ sur $\left(\dfrac{\mathbb{Z}}{2\mathbb{Z}}\right)^2$ pour une raison de cardinal. Le tableau de droite, ci-dessous, résume la situation.

Gal$(L\|\mathbb{Q})$ $g(\sqrt{2})$	Gal$(L\|\mathbb{Q})$ $g(\sqrt{3})$	S_4
$\sqrt{2}$	$\sqrt{3}$	Id
$\sqrt{2}$	$-\sqrt{3}$	(3 4)
$-\sqrt{2}$	$\sqrt{3}$	(1 2)
$-\sqrt{2}$	$-\sqrt{3}$	(1 2) (3 4)

Gal$(L\|\mathbb{Q})$ $g(\sqrt{2})$	Gal$(L\|\mathbb{Q})$ $g(\sqrt{3})$	$\left(\dfrac{\mathbb{Z}}{2\mathbb{Z}}\right)^2$
$\sqrt{2}$	$\sqrt{3}$	$(0,0)$
$\sqrt{2}$	$-\sqrt{3}$	$(0,1)$
$-\sqrt{2}$	$\sqrt{3}$	$(1,0)$
$-\sqrt{2}$	$-\sqrt{3}$	$(1,1)$

On reprend le même exemple à présent, mais en plus général.

Exemple Pour tous nombres premiers distincts $p_1,\dots,p_n$, $\mathbb{Q}\big(\sqrt{p_1},\dots,\sqrt{p_n}\big)$ est une extension galoisienne de $\mathbb{Q}$ et son groupe Galois est isomorphe à $\left(\dfrac{\mathbb{Z}}{2\mathbb{Z}}\right)^n$.

Démonstration On pose : $\quad L = \mathbb{Q}\big(\sqrt{p_1},\dots,\sqrt{p_n}\big), \quad G = \mathrm{Gal}(L|\mathbb{Q}) \quad$ et pour tout $i \in [\![1,n]\!]$:

$$L_i = \mathbb{Q}\big(\sqrt{p_1},\dots,\sqrt{p_{i-1}},\sqrt{p_{i+1}},\dots,\sqrt{p_n}\big).$$

Nous avons déjà montré l'égalité $\big[L : \mathbb{Q}\big] = 2^n$. Ce faisant, nous avons en fait établi que $\sqrt{p_i} \notin L_i$ pour tout $i \in [\![1,n]\!]$, de sorte que $\pi_{\sqrt{p_i},L_i} = X^2 - p_i$.

- Montrons d'abord que pour tout $g \in G$: $\quad g^2 = \mathrm{Id}, \quad$ ou encore $g^{-1} = g$. Soit $g \in G$. Pour tout $i \in [\![1,n]\!]$, $g\big(\sqrt{p_i}\big)$ est racine du polynôme $X^2 - p_i$ d'après **4.3.2**, donc vaut soit $\sqrt{p_i}$, soit $-\sqrt{p_i}$. Dans les deux cas : $g^2\big(\sqrt{p_i}\big) = \sqrt{p_i}$. On en déduit l'égalité $g^2 = \mathrm{Id}$ grâce au théorème **4.1.4**.

  Il en découle que pour tout $n \in \mathbb{Z}$: $\quad g^n = \begin{cases} \mathrm{Id} & \text{si } n \text{ est pair} \\ g & \text{si } n \text{ est impair.} \end{cases}$ Les puissances de g ne dépendent ainsi que de n modulo 2 et on pose $g^0 = \mathrm{Id}$ et $g^1 = g$ où 0 et 1 désignent les éléments de $\dfrac{\mathbb{Z}}{2\mathbb{Z}}$.

- Montrons maintenant que G est commutatif. Pour tous $g, g' \in G$, d'après le point précédent : $g^{-1} = g$, $g'^{-1} = g'$ et $(g'g)^{-1} = g'g$, donc : $gg' = g^{-1}g'^{-1} = (g'g)^{-1} = g'g$.
- À présent, pour tout $i \in [\![1, n]\!]$, nous pouvons noter g_i, d'après **4.2.2**, l'unique L_i-morphisme de $L_i\left(\sqrt{p_i}\right)$ pour lequel : $g_i\left(\sqrt{p_i}\right) = -\sqrt{p_i}$, qui est en fait un L_i-automorphisme de L. En d'autres termes, g_i fixe $\sqrt{p_1}, \dots, \sqrt{p_{i-1}}, \sqrt{p_{i+1}}, \dots, \sqrt{p_n}$, mais transforme $\sqrt{p_i}$ en son opposé.

  Notons enfin φ l'application $(\varepsilon_1, \dots, \varepsilon_n) \longmapsto g_1^{\varepsilon_1} \dots g_n^{\varepsilon_n}$ de $\left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^n$ dans G. Cette application est un morphisme de groupes par commutativité de G, car pour tous $(\varepsilon_1, \dots, \varepsilon_n), (\varepsilon'_1, \dots, \varepsilon'_n) \in \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^n$:

$$\varphi(\varepsilon_1 + \varepsilon'_1, \dots, \varepsilon_n + \varepsilon'_n) = g_1^{\varepsilon_1+\varepsilon'_1} \dots g_n^{\varepsilon_n+\varepsilon'_n} = \left(g_1^{\varepsilon_1} \dots g_n^{\varepsilon_n}\right)\left(g_1^{\varepsilon'_1} \dots g_n^{\varepsilon'_n}\right) = \varphi(\varepsilon_1, \dots, \varepsilon_n)\,\varphi(\varepsilon'_1, \dots, \varepsilon'_n),$$

  mais φ est aussi injective, car si $\varphi(\varepsilon_1, \dots, \varepsilon_n) = \varphi(\varepsilon'_1, \dots, \varepsilon'_n)$, alors $g_1^{\varepsilon_1} \dots g_n^{\varepsilon_n} = g_1^{\varepsilon'_1} \dots g_n^{\varepsilon'_n}$. Si on l'évalue en $\sqrt{p_i}$ pour tout $i \in [\![1, n]\!]$, cette identité montre que $\varepsilon_i = \varepsilon'_i$, et donc que : $(\varepsilon_1, \dots, \varepsilon_n) = (\varepsilon'_1, \dots, \varepsilon'_n)$.

  De l'injectivité de φ découle ceci en particulier $|G| \geqslant 2^n$. Or par ailleurs $|G| \leqslant \left[L : \mathbb{Q}\right] = 2^n$, donc en fait $|G| = \left[L : \mathbb{Q}\right]$, autrement dit L est galoisienne sur $\mathbb{Q}$. En retour, φ est maintenant un morphisme de groupes injectif de $\left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^n$ dans G où $\left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^n$ et G ont le même ordre. Comme voulu, φ est un isomorphisme de $\left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^n$ sur G.

CHAPITRE 5 LA CORRESPONDANCE DE GALOIS 1

Les outils sont en place, la théorie de Galois à proprement parler peut maintenant débuter. Pour en comprendre l'idée, donnons-nous un sous-corps K de $\mathbb{C}$ et L une sous-K-extension de $\mathbb{C}$.

— Pour toute sous-K-extension E de L, tout automorphisme d'anneau de L qui fixe E fixe a fortiori K, autrement dit en termes d'inclusion : $\mathrm{Gal}(L|E) \subset \mathrm{Gal}(L|K)$. Plus précisément, $\mathrm{Gal}(L|E)$ est un sous-groupe de $\mathrm{Gal}(L|K)$.

— Inversement, pour tout sous-groupe H de $\mathrm{Gal}(L|K)$, l'ensemble : $L^H = \left\{x \in L \mid \quad \forall h \in H, \quad h(x) = x\right\}$ est stable par combinaison K-linéaire et produit et contient K, donc est une sous-K-extension de L.

$$\left\{\begin{array}{c}\text{Sous-}K\text{-extensions}\\ \text{de } L\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\text{Sous-groupes}\\ \text{de Gal}(L|K)\end{array}\right\}$$

$$E \longmapsto \mathrm{Gal}(L|E)$$

$$L^H \longmapsto H$$

À présent, les deux applications $E \longmapsto \mathrm{Gal}(L|E)$ et $H \longmapsto L^H$ sont presque réciproques l'une de l'autre, mais peut-être pas tout à fait. En effet, pour toute sous-K-extension E de L, les E-automorphismes de L fixent E, donc $E \subset L^{\mathrm{Gal}(L|E)}$, et pour tout sous-groupe H de $\mathrm{Gal}(L|K)$, les éléments de H fixent L^H, donc $H \subset \mathrm{Gal}\left(L\middle|L^H\right)$. Peut-on dire davantage ? Les applications $E \longmapsto \mathrm{Gal}(L|E)$ et $H \longmapsto L^H$ sont-elles réellement réciproques l'une de l'autre ?

Pour que ce soit le cas, il faut au moins pouvoir garantir que $L^{\mathrm{Gal}(L|K)} = K$, or cette égalité est fausse en général. Par exemple : $\mathbb{Q}\left(\sqrt[3]{2}\right)^{\mathrm{Gal}\left(\mathbb{Q}\left(\sqrt[3]{2}\right)|\mathbb{Q}\right)} = \mathbb{Q}\left(\sqrt[3]{2}\right)^{\{\mathrm{Id}\}} = \mathbb{Q}\left(\sqrt[3]{2}\right) \neq \mathbb{Q}$. Que s'est-il passé ici ? Tout simplement, le groupe de Galois de $\mathbb{Q}\left(\sqrt[3]{2}\right)$ sur $\mathbb{Q}$ n'est pas assez gros. Il faut plus que le singleton $\{\mathrm{Id}\}$ pour voir $\mathbb{Q}\left(\sqrt[3]{2}\right)$ rétrécir jusqu'à devenir $\mathbb{Q}$. Et pourquoi le groupe de Galois n'est-il pas assez gros ? Parce que $\sqrt[3]{2}$ est la seule racine de $X^3 - 2$ dans $\mathbb{Q}\left(\sqrt[3]{2}\right)$. Comme nous l'avons déjà remarqué, c'est bien cela qui empêche l'existence de $\mathbb{Q}$-automorphismes autres que l'identité. On comprend mieux ainsi pourquoi la théorie de Galois est le règne des extensions galoisiennes, i.e. des corps de décomposition.

Dans le cas où L est galoisienne sur K, la *correspondance de Galois* sera ce couple d'applications $E \longmapsto \mathrm{Gal}(L|E)$ et $H \longmapsto L^H$ réciproques l'une de l'autre, qui met en relation bijective les sous-K-extensions de L et les sous-groupes de $\mathrm{Gal}(L|K)$. À terme, cette correspondance nous permettra d'exprimer dans le langage de la théorie des groupes certaines propriétés des extensions de corps, dont leur résolubilité par radicaux. Ce qu'il faut espérer bien sûr — et ce sera le cas — c'est que certains résultats de théorie des groupes pourront être transportés jusque dans la théorie des extensions et nous apporter des réponses non triviales.

5.1 LE THÉORÈME D'ARTIN

Le *théorème d'Artin* est l'un des préliminaires classiques dont la correspondance de Galois peut être déduite.

Théorème 5.1.1 **(Théorème d'Artin)** Soient K un sous-corps de $\mathbb{C}$, L une sous-K-extension finie de $\mathbb{C}$ et H un sous-groupe de $\mathrm{Gal}(L|K)$. On pose : $L^H = \left\{x \in L \mid \quad \forall h \in H, \quad h(x) = x\right\}$, qui est une sous-$K$-extension de L.

- L est une extension galoisienne de L^H.
- En outre : $\mathrm{Gal}\left(L\middle|L^H\right) = H$. En particulier : $\left[L : L^H\right] = |H|$.

Démonstration Par définition de L^H, H fixe tous les éléments L^H, donc $H \subset \mathrm{Gal}\big(L\big|L^H\big)$. Nous allons montrer que $\big[L : L^H\big] \leqslant |H|$. Comme par ailleurs $\big|\mathrm{Gal}\big(L\big|L^H\big)\big| \leqslant \big[L : L^H\big]$, il en découlera que : $\mathrm{Gal}\big(L\big|L^H\big) = H$ et $\big|\mathrm{Gal}\big(L\big|L^H\big)\big| = \big[L : L^H\big]$, ce qui prouvera au passage que L est galoisienne sur L^H.

Posons $n = |H|$. Pour montrer que $\big[L : L^H\big] \leqslant n$, nous allons montrer que toute famille de $n+1$ vecteurs de L est L^H-liée. Soit $(x_1, \dots, x_{n+1})$ une telle famille.

Nous allons nous intéresser, pour tout $h \in H$, à l'équation $\bigstar_h$ suivante : $\lambda_1 h(x_1) + \dots + \lambda_{n+1} h(x_{n+1}) = 0$ d'inconnue $(\lambda_1, \dots, \lambda_{n+1}) \in L^{n+1}$. Ces équations forment ensemble un système linéaire $\bigstar$ homogène de n équations à $n+1$ inconnues à coefficients dans L et nous savons bien qu'un tel système possède des solutions non nulles. Nous pouvons sans perte généralité en choisir une, disons $(\lambda_1, \dots, \lambda_{n+1})$, pour laquelle :

— dans un premier temps, le nombre de composantes non nulles est minimal,

— dans un deuxième temps, quitte à diviser un peu et à réordonner $x_1, \dots, x_{n+1}$: $\lambda_{n+1} = 1$.

En particulier, la relation $\bigstar_{\mathrm{Id}}$: $\lambda_1 x_1 + \dots + \lambda_n x_n + x_{n+1} = 0$ énonce une dépendance linéaire non triviale entre $x_1, \dots, x_{n+1}$, mais à coefficients dans L hélas ! Il nous reste à montrer, si c'est vrai, que les scalaires $\lambda_1, \dots, \lambda_n$ sont dans L^H. Fixons pour cela $\eta \in H$ et composons pour tout $h \in H$ la relation $\bigstar_{\eta^{-1}h}$ par η. Cela donne : $\eta(\lambda_1) h(x_1) + \dots + \eta(\lambda_n) h(x_n) + h(x_{n+1}) = 0$. Soustrayons aussitôt la relation $\bigstar_h$:

$$\forall h \in H, \quad \big(\eta(\lambda_1) - \lambda_1\big) h(x_1) + \dots + \big(\eta(\lambda_n) - \lambda_n\big) h(x_n) = 0.$$

En résumé, la famille $\big(\eta(\lambda_1) - \lambda_1, \dots, \eta(\lambda_n) - \lambda_n, 0\big)$ est une nouvelle solution du système $\bigstar$, mais avec une composante non nulle en moins. Par minimalité, forcément : $\eta(\lambda_1) - \lambda_1 = \dots = \eta(\lambda_n) - \lambda_n = 0$, autrement dit η fixe $\lambda_1, \dots, \lambda_n$. Comme c'est vrai pour tout $\eta \in H$, nous avons finalement prouvé que les scalaires $\lambda_1, \dots, \lambda_n$ sont dans L^H, et donc que la famille $(x_1, \dots, x_{n+1})$ est L^H-liée. ∎

5.2 La correspondance de Galois 1

Notre prochain théorème est le premier théorème fondamental de la théorie de Galois, dont nous n'énoncerons pour l'instant que la première partie. Conformément à l'introduction de ce chapitre, la correspondance de Galois qui y est présentée est un dictionnaire entre deux langues — la langue des sous-extensions d'une part, celle des sous-groupes du groupe de Galois d'autre part.

Théorème 5.2.1 **(Correspondance de Galois 1)** Soient K un sous-corps de $\mathbb{C}$ et L une extension galoisienne de K. L'application $E \longmapsto \mathrm{Gal}(L|E)$ est une bijection décroissante de l'ensemble des sous-K-extensions de L sur l'ensemble des sous-groupes de $\mathrm{Gal}(L|K)$. Sa réciproque est l'application $H \longmapsto L^H$, elle aussi décroissante.

Rappelons en passant que d'après **4.4.3**, avec les notations du théorème, L est toujours galoisienne sur E — alors que E n'est pas forcément galoisienne sur K, nous y reviendrons.

Démonstration

- Pour commencer, l'application $H \overset{\alpha}{\longmapsto} L^H$ est bien définie entre les ensembles indiqués dans le théorème d'après le théorème d'Artin. Pour l'application $E \overset{\beta}{\longmapsto} \mathrm{Gal}(L|E)$, remarquons simplement que pour toute sous-K-extension E de L, l'inclusion $K \subset E$ montre que $\mathrm{Gal}(L|E)$ est une partie de $\mathrm{Gal}(L|K)$, et a fortiori c'en est un sous-groupe.
- L'application α est ensuite décroissante car pour tous sous-groupes H et H' de $\mathrm{Gal}(L|K)$, si $H \subset H'$, alors clairement $L^{H'} \subset L^H$ car qui peut le plus peut le moins.
- D'après le théorème d'Artin, pour tout sous-groupe H de $\mathrm{Gal}(L|K)$: $\beta \circ \alpha(H) = \beta\big(L^H\big) = \mathrm{Gal}\big(L\big|L^H\big) = H$, donc $\beta \circ \alpha = \mathrm{Id}$.
- Pour calculer $\alpha \circ \beta$, donnons-nous une sous-K-extension E de L. D'après le théorème d'Artin appliqué au sous-groupe $\mathrm{Gal}(L|E)$ de $\mathrm{Gal}(L|K)$: $\big[L : L^{\mathrm{Gal}(L|E)}\big] = \big|\mathrm{Gal}(L|E)\big|$, mais comme par ailleurs L est galoisienne sur E : $\big|\mathrm{Gal}(L|E)\big| = \big[L : E\big]$, donc finalement $\big[L : L^{\mathrm{Gal}(L|E)}\big] = \big[L : E\big]$.

  Ensuite, E est fixé par tout E-morphisme de $\mathrm{Gal}(L|E)$, donc $E \subset L^{\mathrm{Gal}(L|E)}$, ce qui fait de $L^{\mathrm{Gal}(L|E)}$ une extension de E. Conclusion : $\big[L : L^{\mathrm{Gal}(L|E)}\big] = \big[L : E\big] = \big[L : L^{\mathrm{Gal}(L|E)}\big] \times \big[L^{\mathrm{Gal}(L|E)} : E\big]$, donc $\big[L^{\mathrm{Gal}(L|E)} : E\big] = 1$, i.e. $L^{\mathrm{Gal}(L|E)} = E$. Comme voulu : $\alpha \circ \beta(E) = \alpha\big(\mathrm{Gal}(L|E)\big) = L^{\mathrm{Gal}(L|E)} = E$, donc $\alpha \circ \beta = \mathrm{Id}$. ∎

Exemple On reprend l'exemple de l'extension galoisienne $L = \mathbb{Q}(\sqrt{2})$ de $\mathbb{Q}$, de groupe de Galois $\{\mathrm{Id}, \sigma\}$ où σ est l'application $a + b\sqrt{2} \longmapsto a - b\sqrt{2}$. Pour une raison de degré, les seules sous-$\mathbb{Q}$-extensions de $\mathbb{Q}(\sqrt{2})$ sont $\mathbb{Q}$ et $\mathbb{Q}(\sqrt{2})$. La correspondance de Galois peut être illustrée dans ce contexte au moyen de deux figures, avec à gauche les sous-$\mathbb{Q}$-extensions de L, et à droite les sous-groupes de $\mathrm{Gal}(L|\mathbb{Q})$. Notez bien sur ces figures l'impact de la décroissance des deux applications $E \longmapsto \mathrm{Gal}(L|E)$ et $H \longmapsto L^H$ — les sous-$\mathbb{Q}$-extensions de L grossissent de bas en haut, mais l'inverse vaut pour les sous-groupes de $\mathrm{Gal}(L|\mathbb{Q})$.

$$\begin{array}{ccc} L & & \{\mathrm{Id}\} = \mathrm{Gal}(L|L) \\ | & & | \\ \mathbb{Q} & & \{\mathrm{Id}, \sigma\} = \mathrm{Gal}(L|\mathbb{Q}) \end{array}$$

Exemple On reprend maintenant l'exemple de l'extension galoisienne $L = \mathbb{Q}(\mathrm{j}, \sqrt[3]{2})$ de $\mathbb{Q}$, de groupe de Galois isomorphe à S_3 si on numérote $\sqrt[3]{2}$, $\mathrm{j}\sqrt[3]{2}$ et $\mathrm{j}^2\sqrt[3]{2}$ respectivement 1, 2 et 3. Le groupe $S_3 = \{\mathrm{Id}, (1\,2\,3), (1\,3\,2), (1\,2), (1\,3), (2\,3)\}$ possède exactement 6 sous-groupes, en l'occurrence :

$$\{\mathrm{Id}\}, \qquad \{\mathrm{Id}, (1\,2)\}, \qquad \{\mathrm{Id}, (1\,3)\}, \qquad \{\mathrm{Id}, (2\,3)\}, \qquad \{\mathrm{Id}, (1\,2\,3), (1\,3\,2)\} \qquad \text{et} \qquad S_3.$$

Chacun de ces sous-groupes est isomorphe à un certain sous-groupe de $\mathrm{Gal}(L|\mathbb{Q})$, auquel nous le confondrons purement et simplement ci-dessous sans autre forme de procès. À quelle sous-$\mathbb{Q}$-extension de L chacun de ces sous-groupes de S_3 est-il alors associé par la correspondance de Galois ?

— Pour commencer : $L^{\{\mathrm{Id}\}} = L$ et $L^{S_3} = L^{\mathrm{Gal}(L|\mathbb{Q})} = \mathbb{Q}$.

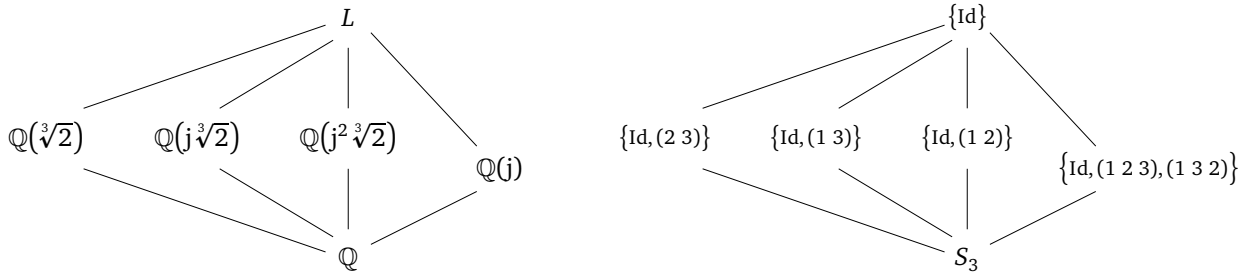
— Qu'en est-il de $L^{\{\mathrm{Id}, (1\,2)\}}$? D'après le théorème d'Artin : $\left[L : L^{\{\mathrm{Id}, (1\,2)\}}\right] = \left|\{\mathrm{Id}, (1\,2)\}\right| = 2$. On en déduit que $\left[L^{\{\mathrm{Id}, (1\,2)\}} : \mathbb{Q}\right] = 3$. Or Id et (1 2) fixent 3, donc les $\mathbb{Q}$-automorphismes correspondants fixent $\mathrm{j}^2\sqrt[3]{2}$, donc $\mathbb{Q}(\mathrm{j}^2\sqrt[3]{2}) \subset L^{\{\mathrm{Id}, (1\,2)\}}$. On tire enfin de l'égalité : $\left[\mathbb{Q}(\mathrm{j}^2\sqrt[3]{2}) : \mathbb{Q}\right] = \deg\left(\pi_{\mathrm{j}^2\sqrt[3]{2},\mathbb{Q}}\right) = \deg\left(\pi_{\sqrt[3]{2},\mathbb{Q}}\right) = \deg\left(X^3 - 2\right) = 3$ le résultat suivant : $L^{\{\mathrm{Id}, (1\,2)\}} = \mathbb{Q}(\mathrm{j}^2\sqrt[3]{2})$.

On montre de même les égalités : $L^{\{\mathrm{Id}, (1\,3)\}} = \mathbb{Q}(\mathrm{j}\sqrt[3]{2})$ et $L^{\{\mathrm{Id}, (2\,3)\}} = \mathbb{Q}(\sqrt[3]{2})$.

— Qu'en est-il enfin de $L^{\{\mathrm{Id}, (1\,2\,3), (1\,3\,2)\}}$? D'après le théorème d'Artin :

$$\left[L : L^{\{\mathrm{Id}, (1\,2\,3), (1\,3\,2)\}}\right] = \left|\{\mathrm{Id}, (1\,2\,3), (1\,3\,2)\}\right| = 3,$$

donc $\left[L^{\{\mathrm{Id}, (1\,2\,3), (1\,3\,2)\}} : \mathbb{Q}\right] = 2$. On en tire l'égalité $L^{\{\mathrm{Id}, (1\,2\,3), (1\,3\,2)\}} = \mathbb{Q}(\mathrm{j})$ en adaptant le raisonnement qui précède.



Exemple On reprend finalement l'exemple de l'extension galoisienne $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ de $\mathbb{Q}$, de groupe de Galois isomorphe à $\left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^2$. On rappelle que cet isomorphisme associe à tout $\mathbb{Q}$-automorphisme g de L l'unique couple $(\varepsilon_2, \varepsilon_3)$ défini par : $g(\sqrt{2}) = (-1)^{\varepsilon_2}\sqrt{2}$ et $g(\sqrt{3}) = (-1)^{\varepsilon_3}\sqrt{3}$. Le groupe $\left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^2$ possède exactement 5 sous-groupes, en l'occurrence :

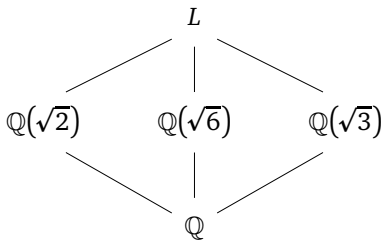
$$\{(0,0)\}, \qquad \{(0,0),(1,0)\}, \qquad \{(0,0),(0,1)\}, \qquad \{(0,0),(1,1)\} \qquad \text{et} \qquad \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^2.$$

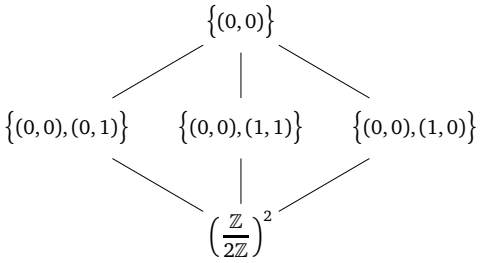
De nouveau, nous confondrons chacun de ces sous-groupes avec le sous-groupe de $\mathrm{Gal}(L|\mathbb{Q})$ auquel il est associé par isomorphisme.

— Pour commencer : $L^{\{\mathrm{Id}\}} = L$ et $L^{\left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^2} = L^{\mathrm{Gal}(L|\mathbb{Q})} = \mathbb{Q}$.

— Qu'en est-il de $L^{\{(0,0),(1,0)\}}$? D'après le théorème d'Artin : $\left[L : L^{\{(0,0),(1,0)\}}\right] = \left|\{(0,0),(1,0)\}\right| = 2$, donc $\left[L^{\{(0,0),(1,0)\}} : \mathbb{Q}\right] = 2$. Or les $\mathbb{Q}$-automorphismes associés à $(0,0)$ et $(1,0)$ fixent $\sqrt{3}$, donc : $\mathbb{Q}(\sqrt{3}) \subset L^{\{(0,0),(1,0)\}}$, mais par ailleurs : $\left[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}\right] = \deg\left(\pi_{\sqrt{3},\mathbb{Q}}\right) = \deg\left(X^2 - 3\right) = 2$, donc enfin $L^{\{(0,0),(1,0)\}} = \mathbb{Q}(\sqrt{3})$.

On montre de même que : $L^{\{(0,0),(0,1)\}} = \mathbb{Q}(\sqrt{2})$ et $L^{\{(0,0),(1,1)\}} = \mathbb{Q}(\sqrt{6})$. Pour cette dernière égalité, il faut observer que les $\mathbb{Q}$-automorphismes associés à $(0,0)$ et $(1,1)$ transforment et $\sqrt{2}$ et $\sqrt{3}$ en son opposé, donc fixent $\sqrt{6} = \sqrt{2} \times \sqrt{3}$.





Chapitre 6 Compléments de théorie des groupes

On rappelle que les groupes abstraits de ce texte sont tous considérés comme des groupes multiplicatifs d'élément neutre 1.

Toute théorie a son jargon, ses petites manies. En voici deux.

Définition 6.0.1 **(Ordre d'un groupe, groupe abélien)**

- Le cardinal d'un groupe est de préférence appelé son *ordre*.
- Pour dire qu'un groupe est commutatif, on dit plutôt généralement qu'il est *abélien*.

6.1 Sous-groupe engendré par une partie

Définition 6.1.1 **(Sous-groupe engendré par une partie)** Soit G un groupe.

- Soit X une partie de G. L'ensemble de tous les produits qu'on peut former à partir des éléments de X et de leurs inverses est un sous-groupe de G, et c'est même le plus petit sous-groupe de G contenant X. On l'appelle le *sous-groupe de G engendré par X* et on le note $\langle X \rangle$.
- On dit que G est *monogène* s'il est engendré par un seul élément, i.e. si $G = \langle x \rangle$ pour un certain $x \in G$ appelé *générateur de G*.

  On dit que G est *cyclique* s'il est à la fois fini et monogène.

Si G est monogène, disons engendré par x : $G = \langle x \rangle = \{x^k \mid k \in \mathbb{Z}\}$. En particulier, G est commutatif car pour tous $m, n \in \mathbb{Z}$: $x^m x^n = x^n x^m$.

Si X est une paire $\{x, y\}$, le sous-groupe $\langle X \rangle = \langle x, y \rangle$ contient tous les éléments x^k et y^k, k décrivant $\mathbb{Z}$, mais aussi les éléments $x^k y^l$ et $y^l x^k$, k et l décrivant $\mathbb{Z}$, mais aussi encore beaucoup de monde : $x^2 y^4 x^{-1}$, $yx^{-2}y^4x$, $xy^2x^{-3}y^{13}x^5\ldots$ À partir de deux éléments générateurs, un groupe peut donc s'avérer très compliqué.

Démonstration Par définition, $\langle X \rangle$ est l'ensemble des éléments de G de la forme $x_1^{\varepsilon_1} \ldots x_n^{\varepsilon_n}$ où $n \in \mathbb{N}$, $x_1, \ldots, x_n \in X$ et $\varepsilon_1, \ldots, \varepsilon_n \in \{1, -1\}$, avec par convention $x_1^{\varepsilon_1} \ldots x_n^{\varepsilon_n} = 1$ si $n = 0$. Il est clair que $\langle X \rangle$ est stable par produit et inversion, donc est un sous-groupe de G. Enfin, tout sous-groupe de G qui contient X contient a fortiori tous les produits qu'on peut faire à partir de ses éléments et de leurs inverses, donc contient $\langle X \rangle$, ce qui montre bien que $\langle X \rangle$ est le plus petit sous-groupe de G contenant X. ∎

Exemple $\mathbb{Z}$ est monogène, ainsi que $\mathbb{U}_n$ pour tout $n \in \mathbb{N}^*$. Plus précisément : $\mathbb{Z} = \langle 1 \rangle$ et $\mathbb{U}_n = \left\langle e^{\frac{2i\pi}{n}} \right\rangle$.

Les deux exemples qui suivent paraîtront plus lisibles si l'on remarque en amont que pour tout $\sigma \in S_n$ et pour tous $x_1, \ldots, x_k \in [\![1, n]\!]$ distincts : $\sigma\,(x_1\ x_2\ \ldots\ x_k)\,\sigma^{-1} = \big(\sigma(x_1)\ \sigma(x_2)\ \ldots\ \sigma(x_k)\big)$.

Exemple Pour tout $n \geqslant 2$, S_n est engendré par ses transpositions, et même : $S_n = \big\langle (1\ 2), (1\ 2\ 3\ \dots\ n) \big\rangle$.

Démonstration L'engendrement par les transpositions est connu. On pose $H = \big\langle (1\ 2), (1\ 2\ 3\ \dots\ n) \big\rangle$.

Pour tout $i \in [\![1, n-1]\!]$: $(1\ 2\ 3\ \dots\ n)^i\ (1\ 2)\ (1\ 2\ 3\ \dots\ n)^{-i} = (i\ \ i+1)$, donc H contient toutes les transpositions $(i\ \ i+1)$, i décrivant $[\![1, n-1]\!]$.

Ensuite, pour tous $i, j \in [\![1, n-1]\!]$ avec $i < j$: $(j\ j+1)\ (i\ j)\ (j\ j+1) = (i\ j+1)$, donc comme H contient $(1\ 2)$ et $(2\ 3)$, il contient $(1\ 3)$, et comme il contient $(1\ 3)$ et $(3\ 4)$, il contient $(1\ 4)$, etc. Ainsi, H contient $(1\ i)$ pour tout $i \in [\![2, n]\!]$.

Finalement, pour tous $i, j \in [\![2, n]\!]$ distincts : $(1\ i)\ (1\ j)\ (1\ i) = (i\ j)$, donc H contient toutes les transpositions de S_n, et comme elles engendrent S_n : $H = S_n$.

L'exemple qui suit prolonge le précédent et nous sera fort utile en temps voulu.

Exemple Soit $p \in \mathbb{P}$. Pour toute transposition τ et pour tout p-cycle σ de $[\![1, p]\!]$: $S_p = \langle \sigma, \tau \rangle$.

Démonstration

- D'abord une remarque d'intérêt général — les puissances d'un cycle ne sont pas toujours elles-mêmes des cycles. Par exemple : $(1\ 2\ 3\ 4)^2 = (1\ 3)\ (2\ 4)$. C'est parfois vrai tout de même. Ainsi, pour tout r-cycle $\rho = (x_1\ x_2\ \dots\ x_r)$ de $[\![1, n]\!]$ et pour tout $k \in \mathbb{Z}$ premier avec r, nous allons montrer que ρ^k est un r-cycle de même support, ce qui revient à dire que pour tous $i, j \in [\![1, r]\!]$ distincts : $x_j = \big(\rho^k\big)^l(x_i)$ pour un certain $l \in \mathbb{Z}$.

  Or déjà, ρ étant un r-cycle : $x_j = \rho^t(x_i)$ pour un certain $t \in \mathbb{Z}$. Ensuite, k et r étant premiers entre eux : $ku + rv = 1$ pour certains $u, v \in \mathbb{Z}$. Conclusion : $x_j = \rho^t(x_i) = \rho^{kut+rvt}(x_i) \overset{\rho^r = \mathrm{Id}}{=} \rho^{kut}(x_i) = \big(\rho^k\big)^{ut}(x_i)$.

  Par ailleurs, alors qu'il est évident que ρ^k est une puissance de ρ, remarquons que ρ est inversement une puissance de ρ^k car $\big(\rho^k\big)^u \overset{\rho^r = \mathrm{Id}}{=} \rho^{ku+rv} = \rho$.

- Mais revenons à nos moutons et écrivons $\tau = (a_1\ a_2)$ pour certains $a_1, a_2 \in [\![1, p]\!]$ distincts. Or σ étant un p-cycle : $a_2 = \sigma^k(a_1)$ pour un certain $k \in [\![1, p-1]\!]$. Et d'après le point précédent, σ^k est lui-même un p-cycle, disons $\sigma^k = (a_1\ a_2\ \dots\ a_p)$ où $i \overset{\alpha}{\longmapsto} a_i$ est une permutation de $[\![1, p]\!]$.

  À présent : $\alpha^{-1}\tau\alpha = (1\ 2)$ et $\alpha^{-1}\sigma^k\alpha = (1\ 2\ \dots\ p)$, donc $\big\langle \alpha^{-1}\sigma^k\alpha, \alpha^{-1}\tau\alpha \big\rangle = S_p$ d'après l'exemple précédent. Conclusion : $\langle \sigma, \tau \rangle = \big\langle \sigma^k, \tau \big\rangle = \alpha \big\langle \alpha^{-1}\sigma\alpha, \alpha^{-1}\tau\alpha \big\rangle \alpha^{-1} = \alpha S_p \alpha^{-1} = S_p$.

6.2 Le théorème de Lagrange

Définition-théorème 6.2.1 **(Classes à gauche modulo un sous-groupe et indice d'un sous-groupe)** Soient G un groupe et H un sous-groupe de G.

- La relation définie pour tous $x, y \in G$ par : $x^{-1}y \in H$ est une relation d'équivalence sur G.
  Pour tout $x \in G$, la classe d'équivalence de x associée est l'ensemble $xH = \big\{xh \mid\ h \in H\big\}$, qu'on appelle la *classe à gauche de x modulo H*.
- L'ensemble quotient de G associé est quant à lui noté G/H. En d'autres termes : $G/H = \big\{xH \mid\ x \in G\big\}$.
  On appelle alors *indice de H dans G* et on note $\big|G : H\big|$ le cardinal de G/H — éventuellement infini.

Démonstration Tout repose ici sur le fait que H est un sous-groupe de G. Soient $x, y, z \in G$.

— **Réflexivité :** H contient 1, donc $x^{-1}x = 1 \in H$.

— **Symétrie :** H est stable par passage à l'inverse, donc si $x^{-1}y \in H$, alors $y^{-1}x = \big(x^{-1}y\big)^{-1} \in H$.

— **Transitivité :** H est stable par produit, donc si $x^{-1}y \in H$ et $y^{-1}z \in H$, alors :

$$x^{-1}z = \big(x^{-1}y\big)\big(y^{-1}z\big) \in H.$$

— **Classes d'équivalence :** Soit $x \in G$. Pour tout $y \in G$, y appartient à la classe à gauche de x modulo H si et seulement si $x^{-1}y \in H$, i.e. si et seulement s'il existe un élément $h \in H$ pour lequel $x^{-1}y = h$, i.e. $y = xh$. Comme voulu, la classe à gauche de x modulo H est l'ensemble xH.

Exemple Pour tout $n \in \mathbb{N}^*$: $\big|\mathbb{Z} : n\mathbb{Z}\big| = n$.

Démonstration Pour commencer, la relation d'équivalence que le théorème précédent associe au sous-groupe $n\mathbb{Z}$ de $\mathbb{Z}$ n'est rien d'autre que la relation de congruence classique modulo n, car pour tous $x, y \in \mathbb{Z}$:

$$x - y \in n\mathbb{Z} \iff x \equiv y \ [n].$$

Ainsi, pour tout $x \in \mathbb{Z}$, la classe à gauche de x modulo $n\mathbb{Z}$ coïncide avec l'ensemble $x + n\mathbb{Z}$ des entiers congrus à x modulo n. En d'autres termes : $\mathbb{Z}/n\mathbb{Z} = \big\{x + n\mathbb{Z} \mid x \in \mathbb{Z}\big\}$, mais cette description est pleine de redondances. Par exemple, il est équivalent d'être congru à 0 modulo n ou de l'être à n, autrement dit $0 + n\mathbb{Z} = n + n\mathbb{Z}$. Or le théorème de la division euclidienne peut être énoncé ainsi : $\forall x \in \mathbb{Z},\ \exists!\, k \in [\![0, n-1]\!],\ x \equiv k \ [n]$. Ainsi, comme voulu : $\big|\mathbb{Z} : n\mathbb{Z}\big| = \big|\mathbb{Z}/n\mathbb{Z}\big| = n$, et plus précisément : $\mathbb{Z}/n\mathbb{Z} = \big\{k + n\mathbb{Z} \mid k \in [\![0, n-1]\!]\big\}$.

Exemple $\big|\mathbb{R} : \mathbb{Z}\big| = +\infty$.

Démonstration Pour commencer : $\mathbb{R}/\mathbb{Z} = \big\{x + \mathbb{Z} \mid x \in \mathbb{R}\big\}$, mais ici encore, cette description est pleine de redondances. Or il est bien connu que : $\forall x \in \mathbb{R},\ \exists!\, \varepsilon \in [0, 1[,\ x - \varepsilon \in \mathbb{Z}$ — existence et unicité de la partie entière de x, qui vaut ici $x - \varepsilon$. Cette proposition montre à la fois que : $\mathbb{R}/\mathbb{Z} = \big\{x + \mathbb{Z} \mid x \in [0, 1[\big\}$, mais aussi qu'on ne peut pas réduire l'ensemble d'indices $[0, 1[$ à un ensemble plus petit.

Exemple $\big|\mathbb{C}^* : \mathbb{U}\big| = +\infty$.

Démonstration Pour commencer : $\mathbb{C}^*/\mathbb{U} = \big\{z\mathbb{U} \mid z \in \mathbb{C}^*\big\}$, mais : $\forall z \in \mathbb{C}^*,\ \exists!\, r > 0,\ \dfrac{z}{r} \in \mathbb{U}$ — avec bien sûr $r = |z|$. Par exemple : $(1+\mathrm{i})\mathbb{U} = \sqrt{2}\mathrm{e}^{\frac{\mathrm{i}\pi}{4}}\mathbb{U} = \sqrt{2}\mathbb{U}$. On en tire à la fois que : $\mathbb{C}^*/\mathbb{U} = \big\{r\mathbb{U} \mid r > 0\big\}$, mais aussi qu'on ne peut pas réduire l'ensemble d'indices $\mathbb{R}_+^*$ à un ensemble plus petit. Géométriquement, pour tout $r > 0$, $r\mathbb{U}$ est le cercle de centre 0 et de rayon r. L'ensemble $\mathbb{C}^*/\mathbb{U}$ n'est ainsi rien d'autre que l'ensemble des cercles de $\mathbb{C}$ de centre 0 et de rayon strictement positif — lesquels forment bien une partition de $\mathbb{C}^*$.

Exemple Si on note H le sous-groupe $\big\langle(1\ 2)\big\rangle = \big\{\mathrm{Id}, (1\ 2)\big\}$ de S_3 : $\big|S_3 : H\big| = 3$.

Démonstration Un calcul direct montre que :

$$\mathrm{Id}\, H = H\,(1\ 2) = H, \qquad (1\ 2\ 3)\, H = (1\ 3)\, H = \big\{(1\ 2\ 3), (1\ 3)\big\} \qquad \text{et} \qquad (1\ 3\ 2)\, H = (2\ 3)\, H = \big\{(1\ 3\ 2), (2\ 3)\big\}.$$

Le théorème qui suit est l'un des théorèmes les plus importants de la théorie des groupes finis, mais « important » ne veut dire ni « difficile » ni « profond ». Simplement, le *théorème de Lagrange* traverse la théorie de part en part.

Théorème 6.2.2 (Théorème de Lagrange) Soient G un groupe fini et H un sous-groupe de G. Alors d'une part $|H|$ divise $|G|$, et d'autre part : $\big|G : H\big| = \dfrac{|G|}{|H|}$.

Démonstration Pour tout $x \in G$, l'application $h \longmapsto xh$ est bijective de H sur xH de réciproque $t \longmapsto x^{-1}t$, donc : $|xH| = |H|$. En résumé, les classes à gauche de G modulo H sont toutes de cardinal $|H|$. Pour conclure, il reste à remarquer que G est la réunion disjointe de ces classes, qui sont au nombre de $\big|G : H\big|$ par définition de l'indice, donc en effet : $G = \big|G : H\big| \times |H|$.

Entre autres conséquences du théorème de Lagrange, l'énoncé qui suit complète naturellement celui du théorème **4.6.1**.

Théorème 6.2.3 (Conditions de divisibilité sur l'ordre d'un groupe de Galois) Soient K un sous-corps de $\mathbb{C}$ et L une extension galoisienne de K.

(i) Si on note P un polynôme de $K[X]$ dont L est le corps de décomposition sur K, alors $\big|\mathrm{Gal}(L|K)\big|$ divise $\big(\deg(P)\big)\,!$.

(ii) Pour tout $x \in L$, $\big|\mathrm{Gal}(L|K)\big|$ est divisible par $\deg\big(\pi_{x,K}\big)$.

Démonstration

(i) Simple conséquence du théorème de Lagrange, car d'après **4.6.1**, si nous notons $x_1, \dots, x_n$ les racines disctinctes de P dans L, l'application $g \longmapsto g|_{\{x_1,\dots,x_n\}}$ est un isomorphisme de groupes de $\mathrm{Gal}(L|K)$ sur son image, qui est un sous-groupe de $S_{\{x_1,\dots,x_n\}}$. Ainsi, $\big|\mathrm{Gal}(L|K)\big|$ divise $\big|S_{\{x_1,\dots,x_n\}}\big| = n!$, qui divise $\big(\deg(P)\big)\,!$.

(ii) Pour tout $x \in L$, L étant galoisienne sur K : $\big|\mathrm{Gal}(L|K)\big| = \big[L : K\big] = \big[L : K(x)\big] \times \big[K(x) : K\big]$, donc $\big|\mathrm{Gal}(L|K)\big|$ est divisible par $\big[K(x) : K\big] = \deg\big(\pi_{x,K}\big)$ d'après **3.3.1**.

Si l'exemple qui suit ne nous apprend rien de nouveau, il illustre tout de même bien l'usage qu'on peut faire des relations de divisibilité précédentes.

Exemple Le groupe de Galois de $L = \mathbb{Q}\big(\mathrm{j}, \sqrt[3]{2}\big)$ sur $\mathbb{Q}$ est d'ordre 6.

Démonstration Pour commencer, $\big|\mathrm{Gal}(L|\mathbb{Q})\big|$ divise $3! = 6$ car L est le corps de décomposition de $X^3 - 2$ sur $\mathbb{Q}$. Ensuite, $\big|\mathrm{Gal}(L|\mathbb{Q})\big|$ est divisible par $\deg\big(\pi_{\mathrm{j},\mathbb{Q}}\big) = \deg\big(X^2 + X + 1\big) = 2$ ainsi que par $\deg\big(\pi_{\sqrt[3]{2},\mathbb{Q}}\big) = \deg\big(X^3 - 2\big) = 3$.

6.3 Sous-groupes distingués et groupes quotients

Définition-théorème 6.3.1 **(Conjugaison et sous-groupe distingué)** Soient G un groupe et H un sous-groupe de G.

- Soit $x \in G$. L'application $g \longmapsto xgx^{-1}$ est un automorphisme de groupe de G appelé *conjugaison par* x, et l'ensemble $xHx^{-1} = \big\{xhx^{-1} \mid h \in H\big\}$ est un sous-groupe de G appelé le *conjugué de* H *par* x.
- On dit que H est *distingué dans* G s'il est *stable par conjugaison*, i.e. si pour tout $x \in G$: $xHx^{-1} = H$, ce qui revient aussi à dire que pour tous $x \in G$ et $h \in H$: $xhx^{-1} \in H$.

Le sous-groupe H est distingué dans G s'il « commute globalement » avec tout élément de G. À défaut de pouvoir affirmer que pour tous $h \in H$ et $x \in G$: $xhx^{-1} = h$, on dispose au moins d'une relation de « commutation globale » : $xHx^{-1} = H$.

Démonstration Soit $x \in G$. L'application $g \longmapsto xgx^{-1}$ est un morphisme de groupes car pour tous $g, g' \in G$: $x(gg')x^{-1} = \big(xgx^{-1}\big)\big(xg'x^{-1}\big)$, et sa réciproque est l'application $g \longmapsto x^{-1}gx$. Enfin, xHx^{-1} est un sous-groupe de G comme image de H par $g \longmapsto xgx^{-1}$ d'après **4.5.2**.

Exemple Soit G un groupe.

- Les sous-groupes $\big\{1\big\}$ et G sont distingués dans G.
- Si G est abélien, tout sous-groupe de G y est distingué. Dans ce cas, en effet, le seul automorphisme de conjugaison est l'identité car pour tous $x, g \in G$: $xgx^{-1} = g$.

En particulier, déterminer les sous-groupes distingués du groupe abélien $\mathbb{Z}$ revient à déterminer ses sous-groupes tout court.

Exemple Les sous-groupes de $\mathbb{Z}$ sont les ensembles $n\mathbb{Z}$, n décrivant $\mathbb{N}$.

Démonstration Nous avons déjà admis implicitement que $n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$ pour tout $n \in \mathbb{N}$. Pour la réciproque, soit G un sous-groupe de $\mathbb{Z}$. Si $G = \big\{0\big\}$, alors $G = 0\mathbb{Z}$. Supposons désormais $G \neq \big\{0\big\}$. Comme G est stable par passage à l'opposé, $G \cap \mathbb{N}^*$ est alors une partie non vide de $\mathbb{N}$, donc possède un plus petit élément n. A fortiori : $n\mathbb{Z} = \langle n\rangle \subset G$. Inversement, soit $x \in G$. La division euclidienne de x par n peut être écrite $x = nq + r$ pour certains $q \in \mathbb{Z}$ et $r \in [\![0, n-1]\!]$. Aussitôt, G étant stable par addition et passage à l'opposé : $r = x - nq \in G$, mais n est par définition le plus petit élément de $G \cap \mathbb{N}^*$, donc forcément $r = 0$, i.e. $x = nq \in n\mathbb{Z}$. Conclusion : $G = n\mathbb{Z}$.

Exemple Dans un groupe quelconque, tout sous-groupe d'indice 2 est distingué.

Démonstration Soient G un groupe et H un sous-groupe de G d'indice 2. Soient $x \in G$ et $h \in H$.

— Si $x \in H$, évidemment $xhx^{-1} \in H$.

— Supposons désormais que $x = 1^{-1}x \notin H$. Dans ce cas, x et 1 ne sont pas dans la même classe à gauche modulo H, autrement dit $xH \neq H$. Comme $\big|G : H\big| = 2$, il en découle que $G/H = \big\{H, xH\big\}$, de sorte que G est la réunion disjointe des classes H et xH. Or $xhx^{-1} \notin xH$ — sans quoi x serait élément de H — donc $xhx^{-1} \in H$.

Dans tous les cas : $xhx^{-1} \in H$, donc comme voulu, H est distingué dans G.

Exemple D'après l'exemple précédent, $\big\langle (1\ 2\ 3) \big\rangle$ est un sous-groupe distingué de S_3. Le sous-groupe $\big\langle (1\ 2) \big\rangle$, en revanche, ne l'est pas car : $(1\ 3) \big\langle (1\ 2) \big\rangle (1\ 3)^{-1} = \big\langle (1\ 3)\ (1\ 2)\ (1\ 3) \big\rangle = \big\langle (2\ 3) \big\rangle \neq \big\langle (1\ 2) \big\rangle$.

Exemple $K = \Big\{ \mathrm{Id}\ ,\ (1\ 2)\ (3\ 4)\ ,\ (1\ 3)\ (2\ 4)\ ,\ (1\ 4)\ (2\ 3) \Big\}$ est un sous-groupe distingué dans S_4.

Démonstration Le fait que K soit un sous-groupe de S_4 se vérifie à la main. Outre l'identité, les éléments de K sont exactement tous les produits de deux transpositions disjointes qu'on peut former dans S_4. Or n'oublions pas que pour tout $\sigma \in S_4$ et pour tous $a, b, c, d \in [\![1, 4]\!]$ distincts : $\sigma\ (a\ b)\ (c\ d)\ \sigma^{-1} = \big(\sigma(a)\ \ \sigma(b)\big)\big(\sigma(c)\ \ \sigma(d)\big)$. D'après ce principe, l'ensemble des produits de deux transpositions disjointes est stable par conjugaison, donc K est distingué dans S_4.

On généralise à présent la construction classique des groupes additifs $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$. Ces groupes modulo n ont tout l'air d'un miracle arithmétique à première vue, mais l'algèbre est en réalité pleine de ce genre de groupes modulo quelque chose. Modulo quoi ? Modulo un sous-groupe distingué comme nous allons le voir.

On pose pour tout groupe G et pour toutes parties X et Y de G : $XY = \Big\{ xy \mid \quad x \in X, \quad y \in Y \Big\}$.

Définition-théorème 6.3.2 **(Quotient d'un groupe par un sous-groupe distingué)** Soient G un groupe et H un sous-groupe distingué de G.

(i) Pour tous $x, y \in G$: $(xH)(yH) = (xy)H$. Cette identité définit une loi interne sur l'ensemble G/H des classes à gauche de G modulo H.

(ii) Muni de cette loi, G/H est un groupe d'élément neutre $H = 1\,H$ appelé le *groupe quotient de G par H* et noté $\dfrac{G}{H}$. Dans ce groupe, pour tout $x \in G$: $(xH)^{-1} = x^{-1}H$.

S'il est toujours possible de définir l'ensemble G/H, celui-ci ne peut être un groupe pour la loi de l'assertion (i) que si H est distingué dans G, i.e. que si H « commute globalement » avec tout élément de G. Sans cela, la relation $(xH)(yH) = (xy)H$ est fausse en général.

La notion de groupe quotient est l'une des plus fondamentales de l'algèbre. Le groupe $\dfrac{G}{H}$ doit être vu comme un avatar de G dans lequel on raisonne modulo H, autrement dit dans lequel les éléments de H sont invisibles. En ce sens, comme avec les groupes additifs $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$, quotienter c'est oublier.

Quand on connaît le groupe G — i.e. quand on sait y mener tous les calculs qu'on veut — on connaît les groupes H et $\dfrac{G}{H}$ qui en sont comme deux composantes. On peut considérer d'ailleurs que G est le résultat d'un certain empilement du groupe $\dfrac{G}{H}$ sur le sous-groupe H. Dans le cas d'un groupe inconnu G, la connaissance d'un sous-groupe distingué H et du quotient associé $\dfrac{G}{H}$ fournit ainsi de précieuses informations sur G. Il est hélas faux en général que H et $\dfrac{G}{H}$ caractérisent à eux seuls entièrement G, car la structure de G dépend aussi fortement de la manière dont $\dfrac{G}{H}$ est empilé sur H.

Démonstration

(i) Soient $x, y \in G$. Alors $(xy)H \subset (xH)(yH)$, car pour tout $h \in H$: $(xy)h = x(yh) \in (xH)(yH)$.

Réciproquement, montrons que $(xH)(yH) \subset (xy)H$. Soient $h, h' \in H$. Or comme H est distingué dans G : $y^{-1}hy \in y^{-1}Hy = H$, donc $(xh)(yh') = (xy)\underbrace{\big(y^{-1}hy\big)}_{\in H}h' \in (xy)H$.

(ii) Le magma G/H est associatif car pour tous $x, y, z \in G$:

$$\big((xH)(yH)\big)(zH) \overset{\text{(i)}}{=} \big((xy)H\big)(zH) \overset{\text{(i)}}{=} \big((xy)z\big)H = \big(x(yz)\big)H \overset{\text{(i)}}{=} (xH)\big((yz)H\big) \overset{\text{(i)}}{=} (xH)\big((yH)(zH)\big).$$

Ce magma admet ensuite $1\,H = H$ pour élément neutre car : $(1\,H)(xH) \overset{\text{(i)}}{=} (1\,x)\,H = xH$ pour tout $x \in G$ et de même $(xH)(1\,H) = xH$. Enfin, xH est inversible d'inverse $x^{-1}H$ pour tout $x \in G$ car $(xH)\big(x^{-1}H\big) = \big(xx^{-1}\big)H = H$ et de même $\big(x^{-1}H\big)(xH) = H$.

Exemple $\mathbb{Z}$ est un sous-groupe de $\mathbb{R}$, distingué car $\mathbb{R}$ est abélien, et nous avons déjà vu que $\dfrac{\mathbb{R}}{\mathbb{Z}} = \Big\{ x + \mathbb{Z} \mid \quad x \in [0, 1[\Big\}$. Ce quotient est un groupe tout à fait analogue à $\mathbb{R}$ à ceci près qu'on y raisonne modulo $\mathbb{Z}$, i.e. modulo 1. On peut se le représenter comme une version circulaire de l'intervalle $[0, 1[$ dont les extrémités ont été en quelque sorte réunies par la congruence : $1 \equiv 0\ [1]$.

Exemple $\mathbb{U}$ est un sous-groupe de $\mathbb{C}^*$, distingué car $\mathbb{C}^*$ est abélien, et nous avons déjà vu que $\dfrac{\mathbb{C}^*}{\mathbb{U}} = \big\{r\mathbb{U} \mid \ r > 0\big\}$. Ce quotient est un groupe tout à fait analogue à $\mathbb{C}^*$ à ceci près qu'on y néglige complètement les nombres complexes de module 1, ce qui revient à ne percevoir des nombres complexes que leur module.

Dans les exemples précédents, on est parti d'un groupe abélien G et on l'a quotienté par l'un de ses sous-groupes H. Le résultat $\dfrac{G}{H}$ est alors toujours un groupe abélien car pour tous $x, y \in G$: $\quad (xH)(yH) = (xy)H = (yx)H = (yH)(xH)$. L'exemple qui suit montre qu'en général, H et $\dfrac{G}{H}$ peuvent être abéliens sans que G le soit.

Exemple Il n'est pas dur de vérifier que les matrices : $\quad \pm I_2, \quad \pm\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \pm\begin{pmatrix} 0 & \mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix} \quad$ et $\quad \pm\begin{pmatrix} -\mathrm{i} & 0 \\ 0 & \mathrm{i} \end{pmatrix}$ forment un sous-groupe de $\mathrm{GL}_2(\mathbb{C})$, le *groupe des quaternions*, noté Q_8. Encore que cela puisse paraître un peu confus, on pose classiquement :

$$1 = I_2, \qquad \mathrm{i} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \qquad \mathrm{j} = \begin{pmatrix} 0 & \mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix} \qquad \text{et} \qquad \mathrm{k} = \begin{pmatrix} -\mathrm{i} & 0 \\ 0 & \mathrm{i} \end{pmatrix}, \qquad \text{de sorte que } Q_8 = \big\{\pm 1, \pm \mathrm{i}, \pm \mathrm{j}, \pm \mathrm{k}\big\}.$$

La loi de ce groupe non abélien est entièrement définie par les relations qui suivent :

$$\bigstar \qquad \mathrm{i}^2 = \mathrm{j}^2 = \mathrm{k}^2 = -1, \qquad \mathrm{ij} = \mathrm{k}, \qquad \mathrm{jk} = \mathrm{i}, \qquad \mathrm{ki} = \mathrm{j} \qquad \text{et} \qquad \mathrm{ji} = -\mathrm{k}, \qquad \mathrm{kj} = -\mathrm{i}, \qquad \mathrm{ik} = -\mathrm{j}.$$

On en déduit facilement que le sous-groupe $\langle -1 \rangle = \big\{\pm 1\big\}$ est distingué dans Q_8 — et abélien. En outre :

$$\frac{Q_8}{\langle -1 \rangle} = \Big\{ \big\{\pm 1\big\}, \big\{\pm \mathrm{i}\big\}, \big\{\pm \mathrm{j}\big\}, \big\{\pm \mathrm{k}\big\} \Big\} = \Big\{\overline{1}, \overline{\mathrm{i}}, \overline{\mathrm{j}}, \overline{\mathrm{k}}\Big\} \qquad \text{si on pose :} \quad \overline{1} = \big\{\pm 1\big\}, \quad \overline{\mathrm{i}} = \big\{\pm \mathrm{i}\big\}, \quad \overline{\mathrm{j}} = \big\{\pm \mathrm{j}\big\} \quad \text{et} \quad \overline{k} = \big\{\pm \mathrm{k}\big\}.$$

Les relations $\bigstar$ deviennent dans ce quotient : $\quad \overline{\mathrm{i}}^2 = \overline{\mathrm{j}}^2 = \overline{\mathrm{k}}^2 = \overline{1}, \quad \overline{\mathrm{i}}\,\overline{\mathrm{j}} = \overline{\mathrm{k}}, \quad \overline{\mathrm{j}}\,\overline{\mathrm{k}} = \overline{\mathrm{i}} \quad$ et $\quad \overline{\mathrm{k}}\,\overline{\mathrm{i}} = \overline{\mathrm{j}}$. Or ces relations sont les mêmes que celles qui définissent le groupe additif $\left(\dfrac{\mathbb{Z}}{2\mathbb{Z}}\right)^2$:

$$(1,0)^2 = (0,1)^2 = (1,1)^2, \qquad (1,0) + (0,1) = (1,1), \qquad (0,1) + (1,1) = (1,0) \qquad \text{et} \qquad (1,1) + (1,0) = (0,1).$$

Les lois des groupes $\dfrac{Q_8}{\langle -1 \rangle}$ et $\left(\dfrac{\mathbb{Z}}{2\mathbb{Z}}\right)^2$ sont ainsi décrites par les mêmes tables au nom près des objets, ce qui suffit à montrer que ces groupes sont isomorphes. Comme annoncé, $\langle -1 \rangle$ et $\dfrac{Q_8}{\langle -1 \rangle}$ sont abéliens, mais pas Q_8 lui-même.

$\times$	$\overline{1}$	$\overline{\mathrm{i}}$	$\overline{\mathrm{j}}$	$\overline{\mathrm{k}}$
$\overline{1}$	$\overline{1}$	$\overline{\mathrm{i}}$	$\overline{\mathrm{j}}$	$\overline{\mathrm{k}}$
$\overline{\mathrm{i}}$	$\overline{\mathrm{i}}$	$\overline{1}$	$\overline{\mathrm{k}}$	$\overline{\mathrm{j}}$
$\overline{\mathrm{j}}$	$\overline{\mathrm{j}}$	$\overline{\mathrm{k}}$	$\overline{1}$	$\overline{\mathrm{i}}$
$\overline{\mathrm{k}}$	$\overline{\mathrm{k}}$	$\overline{\mathrm{j}}$	$\overline{\mathrm{i}}$	$\overline{1}$

$+$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(0,0)$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(1,0)$	$(1,0)$	$(0,0)$	$(1,1)$	$(0,1)$
$(0,1)$	$(0,1)$	$(1,1)$	$(0,0)$	$(1,0)$
$(1,1)$	$(1,1)$	$(0,1)$	$(1,0)$	$(0,0)$

Exemple On note K le sous-groupe distingué $\Big\{\mathrm{Id}\,,\ (1\ 2)\,(3\ 4)\,,\ (1\ 3)\,(2\ 4)\,,\ (1\ 4)\,(2\ 3)\Big\}$ de S_4. Les groupes $\dfrac{S_4}{K}$ et S_3 sont alors isomorphes.

Démonstration Comme K est distingué dans S_4, l'application $\sigma \longmapsto K\sigma$ est un morphisme de groupes de S_4 dans $\dfrac{S_4}{K}$ de noyau K. Nous nous intéreserons à sa seule restriction φ à S_3, où l'on voit S_3 comme l'ensemble des permutations de $[\![1,4]\!]$ qui fixent 4. Le noyau de φ vaut $\mathrm{Ker}\,\varphi = K \cap S_3 = \big\{\mathrm{Id}\big\}$, donc φ est injective. Or d'après le théorème de Lagrange : $\quad \big|S_4 : K\big| = \dfrac{|S_4|}{|K|} = \dfrac{24}{4} = 6 = |S_3|, \quad$ donc φ est en fait bijective de S_3 sur $\dfrac{S_4}{K}$.

Théorème 6.3.3 **(Sous-groupes d'un quotient)** Soient G un groupe et H un sous-groupe distingué de G.

(i) L'application $K \longmapsto \dfrac{K}{H}$ est une bijection croissante de l'ensemble des sous-groupes de G contenant H sur l'ensemble des sous-groupes de $\dfrac{G}{H}$.

(ii) Pour tout sous-groupe K de G contenant H, $\dfrac{K}{H}$ est distingué dans $\dfrac{G}{H}$ si et seulement si K l'est dans G.

Démonstration Pour toute partie $\big\{x_i H \mid \ i \in I\big\}$ de $\dfrac{G}{H}$, $\displaystyle\bigcup_{i\in I} x_i H$ est une partie de G stable par produit à droite par tout élément de H. Inversement, toute partie de G stable par produit à droite par tout élément de H est

une réunion de classes à gauche de G modulo H. Plus précisément, l'application $\{x_iH \mid \ i \in I\} \overset{\theta}{\longmapsto} \bigcup_{i\in I} x_iH$ est bijective de l'ensemble des parties de $\frac{G}{H}$ sur l'ensemble des parties de G stable par produit à droite par tout élément de H.

(i) Pour tout sous-groupe K de G contenant H : $\frac{K}{H} = \{kH \mid \ k \in K\}$ et pour tous $k, k' \in K$: $k^{-1}k' \in K$ donc $(kH)^{-1}(k'H) = (k^{-1}k')H \in \frac{K}{H}$. Ainsi, $\frac{K}{H}$ est un sous-groupe de $\frac{G}{H}$.

Réciproquement, soit $\{x_iH \mid \ i \in I\}$ un sous-groupe de $\frac{G}{H}$. Posons $K = \bigcup_{i\in I} x_iH$. Cet ensemble K contient l'élément neutre H de $\frac{G}{H}$, mais il reste à montrer que c'est un sous-groupe de G. Soient $x, y \in K$, disons $x \in x_iH$ et $y \in x_jH$ pour certains $i, j \in I$. Comme $\{x_iH \mid \ i \in I\}$ est un sous-groupe de $\frac{G}{H}$, alors pour un certain $k \in I$: $x^{-1}y \in (xH)^{-1}(yH) = (x_iH)^{-1}(x_jH) = x_kH \subset K$.

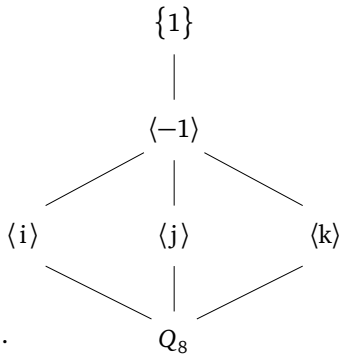
(ii) Soit K un sous-groupe de G. Si K est distingué dans G, alors pour tous $g \in G$ et $k \in K$: $gkg^{-1} \in K$ donc $(gH)(kH)(gH)^{-1} = (gkg^{-1})H \in \frac{K}{H}$, autrement dit $\frac{K}{H}$ est distingué dans $\frac{G}{H}$. Réciproquement, si $\frac{K}{H}$ est distingué dans $\frac{G}{H}$, alors pour tous $g \in G$ et $k \in K$: $(gkg^{-1})H = (gH)(kH)(gH)^{-1} \in \frac{K}{H}$, donc pour un certain $k' \in K$: $gkg^{-1} \in k'H \subset K$, autrement dit K est distingué dans G. ∎

Exemple Le groupe des quaternions Q_8 n'est pas abélien, mais reprenant un exemple récent, nous allons voir que ses sous-groupes sont tous distingués dans Q_8 — cette situation est assez rare. Tout sous-groupe de $Q_8 = \{\pm 1, \pm\mathrm{i}, \pm\mathrm{j}, \pm\mathrm{k}\}$ autre que $\{1\}$ contient -1 — donc $\langle -1\rangle$ — car $(\pm\mathrm{i})^2 = (\pm\mathrm{j})^2 = (\pm\mathrm{k})^2 = -1$. Or le quotient $\frac{Q_8}{\langle -1\rangle}$ est abélien, donc tous ses sous-groupes sont distingués. Il en découle d'après **6.3.3** que tout sous-groupe de Q_8 contenant $\langle -1\rangle$ est distingué dans Q_8, mais donc finalement que tout sous-groupe de Q_8 y est distingué.

Qui sont exactement les sous-groupes de Q_8 ? Hormis $\{1\}$, tous proviennent d'un unique sous-groupe de $\frac{Q_8}{\langle -1\rangle}$ d'après **6.3.3**, lequel est isomorphe à $\left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^2$ d'après un exemple précédent et possède 5 sous-groupes comme nous l'avons déjà vu en étudiant le groupe de Galois de l'extension galoisienne $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ de $\mathbb{Q}$:

$$\{(0,0)\}, \quad \{(0,0),(1,0)\}, \quad \{(0,0),(0,1)\}, \quad \{(0,0),(1,1)\} \quad \text{et} \quad \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^2.$$

À ces 5 sous-groupes de $\left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^2$ correspondent 5 sous-groupes de Q_8, à savoir respectivement : $\langle -1\rangle$, $\langle \mathrm{i}\rangle$, $\langle \mathrm{j}\rangle$, $\langle \mathrm{k}\rangle$ et Q_8, auxquels il convient d'inclure pour finir le sous-groupe $\{1\}$.



6.4 Le théorème d'isomorphisme

Définition-théorème 6.4.1 **(Noyau d'un morphisme de groupes)** Soient G et G' deux groupes et $\varphi : G \longrightarrow G'$ un morphisme de groupes. On appelle *noyau de* φ et on note $\operatorname{Ker}\varphi$ l'ensemble : $\operatorname{Ker}\varphi = \{x \in G \mid \ \varphi(x) = 1\}$.

Il s'agit là d'un sous-groupe distingué de G. En outre, φ est injective si et seulement si $\operatorname{Ker}\varphi = \{1\}$.

Pour tous $x \in G$ et $k \in \operatorname{Ker}\varphi$: $\varphi(xk) = \varphi(x)\varphi(k) = \varphi(x)1 = \varphi(x)$. Ce calcul montre que deux éléments de G qui ne diffèrent que d'un élément de $\operatorname{Ker}\varphi$ sont indiscernables dans G' quand on les observe à travers φ.

Tout ceci n'est pas sans rappeler la définition du noyau en algèbre linéaire et son lien avec l'injectivité, mais il ne faut pas oublier que les applications linéaires sont des morphismes de groupes additifs. L'élément neutre additif des espaces vectoriels étant noté 0 plutôt que 1, la définition du noyau de l'algèbre linéaire n'est finalement qu'un cas particulier de sa définition en théorie des groupes.

Démonstration Le noyau $\operatorname{Ker}\varphi$ est un sous-groupe de G car d'une part : $\varphi(1) = 1$ donc $1 \in \operatorname{Ker}\varphi$, et d'autre part, pour tous $x, y \in \operatorname{Ker}\varphi$: $\varphi(x^{-1}y) = \varphi(x)^{-1}\varphi(y) = 1^{-1}1 = 1$ donc $x^{-1}y \in \operatorname{Ker}\varphi$.

Ensuite, $\operatorname{Ker}\varphi$ est distingué dans G car pour tous $x \in \operatorname{Ker}\varphi$ et $g \in G$:

$$\varphi(gxg^{-1}) = \varphi(g)\varphi(x)\varphi(g)^{-1} = \varphi(g)\varphi(g)^{-1} = 1, \qquad \text{donc comme voulu } gxg^{-1} \in \operatorname{Ker}\varphi.$$

Supposons enfin φ injective. Aussitôt, pour tout $x \in \operatorname{Ker}\varphi$: $\varphi(x) = 1 = \varphi(1)$ donc $x = 1$, donc $\operatorname{Ker}\varphi = \{1\}$. Pour la réciproque, faisons l'hypothèse que $\operatorname{Ker}\varphi = \{1\}$. Alors pour tous $x, x' \in G$:

$$\varphi(x) = \varphi(x') \iff \varphi\left(x^{-1}x'\right) = 1 \iff x^{-1}x' \in \operatorname{Ker}\varphi \iff x^{-1}x' = 1 \iff x = x',$$

donc φ est injective. ∎

Le théorème qui suit, dit *théorème d'isomorphisme*, est un analogue du théorème du rang adapté à la théorie des groupes. Théorème majeur s'il en est !

Théorème 6.4.2 (Théorème d'isomorphisme) Soient G et G' deux groupes et $\varphi : G \longrightarrow G'$ un morphisme de groupes. On note $\overline{x}$ la classe à gauche de x dans $\dfrac{G}{\operatorname{Ker}\varphi}$ pour tout $x \in G$.

Il existe un et un seul morphisme de groupes $\overline{\varphi} : \dfrac{G}{\operatorname{Ker}\varphi} \longrightarrow G'$ pour lequel pour tout $x \in G$: $\overline{\varphi}\left(\overline{x}\right) = \varphi(x)$, et ce morphisme est en fait un isomorphisme de groupes de $\dfrac{G}{\operatorname{Ker}\varphi}$ sur $\operatorname{Im}\varphi$.

Le noyau de φ est l'ensemble des éléments de G que φ rend invisibles dans G', donc en quotientant par $\operatorname{Ker}\varphi$, on oublie les invisibles et on fait coïncider tous les éléments de G que φ ne parvenait pas à discerner. Une nouvelle application $\overline{\varphi}$ est ainsi créée de $\dfrac{G}{\operatorname{Ker}\varphi}$ dans G', et cette application est injective puisqu'il n'y a plus d'indiscernables pour φ dans $\dfrac{G}{\operatorname{Ker}\varphi}$.

Démonstration On aimerait pouvoir poser $\overline{\varphi}\left(\overline{x}\right) = \varphi(x)$ pour tout $x \in G$, mais cette définition pose problème a priori car x n'est qu'un élément parmi d'autres de la classe $\overline{x} = x(\operatorname{Ker}\varphi)$. Pour lever toute ambiguïté, nous devons garantir que pour tous $x, x' \in G$: $\varphi(x) = \varphi(x')$ dès que x et x' définissent la même classe à gauche modulo $\operatorname{Ker}\varphi$. Or c'est assez clair, car :

$$\varphi(x) = \varphi(x') \iff \varphi\left(x^{-1}x'\right) = 1 \iff x^{-1}x' \in \operatorname{Ker}\varphi \iff \overline{x} = \overline{x}'.$$

Pour être précis, l'implication : $\overline{x} = \overline{x}' \implies \varphi(x) = \varphi(x')$ justifie la bonne définition de $\overline{\varphi}$, mais la réciproque : $\varphi(x) = \varphi(x') \implies \overline{x} = \overline{x}'$ nous intéresse aussi beaucoup, elle signifie que $\overline{\varphi}$ est injective.

L'unicité de $\overline{\varphi}$ découle de sa définition car la relation $\overline{\varphi}\left(\overline{x}\right) = \varphi(x)$ pour tout $x \in G$ ne nous laisse guère de choix, mais la surjectivité en découle aussi :

$$\operatorname{Im}\overline{\varphi} = \left\{\overline{\varphi}(t) \,\middle|\, t \in \frac{G}{\operatorname{Ker}\varphi}\right\} = \left\{\overline{\varphi}\left(\overline{x}\right) \mid x \in G\right\} = \left\{\varphi(x) \mid x \in G\right\} = \operatorname{Im}\varphi.$$

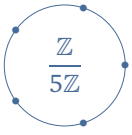
Il nous reste donc à montrer que $\overline{\varphi}$ est un morphisme de groupes. Or pour tous $x, y \in G$:

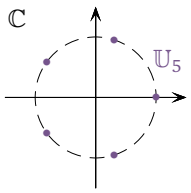
$$\overline{\varphi}\left(\overline{x}\,\overline{y}\right) = \overline{\varphi}\left(\overline{xy}\right) = \varphi(xy) = \varphi(x)\varphi(y) = \overline{\varphi}\left(\overline{x}\right)\overline{\varphi}\left(\overline{y}\right).$$

∎

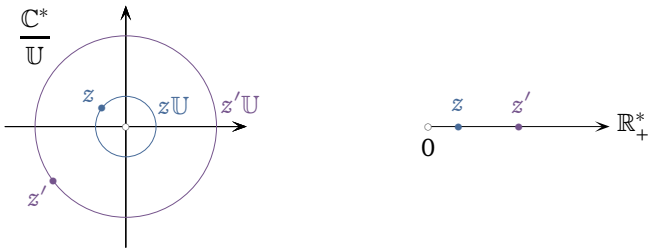
Exemple La fonction $x \longmapsto |x|$ est un morphisme de groupes de $\mathbb{R}^*$ dans lui-même de noyau $\mathbb{U}_2 = \{\pm 1\}$ et d'image $\mathbb{R}_+^*$. D'après le théorème d'isomorphisme, les groupes $\dfrac{\mathbb{R}^*}{\mathbb{U}_2}$ et $\mathbb{R}_+^*$ sont donc isomorphes. Est-ce étonnant ? Non, car oublier le signe d'un réel, c'est ne garder que sa valeur absolue.

Exemple Pour tout $n \in \mathbb{N}^*$, la fonction $k \longmapsto \mathrm{e}^{\frac{2ik\pi}{n}}$ est un morphisme de groupes surjectif de $\mathbb{Z}$ sur $\mathbb{U}_n$ de noyau $n\mathbb{Z}$. D'après le théorème d'isomorphisme, les groupes $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ et $\mathbb{U}_n$ sont donc isomorphes. Cet isomorphisme n'est pas étonnant, nous le retrouvons en nous à titre d'intuition en nous représentant ces deux groupes comme deux « boucles qui tournent » de taille n. En particulier, pour $n = 2$, la fonction $k \longmapsto (-1)^k$ de $\mathbb{Z}$ dans $\{\pm 1\}$ induit par quotient un isomorphisme de $\dfrac{\mathbb{Z}}{2\mathbb{Z}}$ sur $\{\pm 1\}$.





Exemple La fonction $z \longmapsto |z|$ est un morphisme de groupes de $\mathbb{C}^*$ dans $\mathbb{R}^*$ de noyau $\mathbb{U}$ et d'image $\mathbb{R}_+^*$. D'après le théorème d'isomorphisme, les groupes $\dfrac{\mathbb{C}^*}{\mathbb{U}}$ et $\mathbb{R}_+^*$ sont donc isomorphes. Nous avons déjà vu que $\dfrac{\mathbb{C}^*}{\mathbb{U}}$ est l'ensemble des cercles de $\mathbb{C}$ de centre 0 et de rayon strictement positif. La fonction $z \longmapsto |z|$ ramène chacun de ces cercles à son seul rayon.



Exemple La fonction $\theta \longmapsto e^{i\theta}$ est un morphisme de groupes de $\mathbb{R}$ dans $\mathbb{C}^*$ de noyau $2\pi\mathbb{Z}$ et d'image $\mathbb{U}$. D'après le théorème d'isomorphisme, les groupes $\dfrac{\mathbb{R}}{2\pi\mathbb{Z}}$ et $\mathbb{U}$ sont donc isomorphes. Géométriquement, $\dfrac{\mathbb{R}}{2\pi\mathbb{Z}}$ est le monde qu'on obtient quand on tient pour égaux les réels modulo 2π. Cela revient à considérer le fil $\mathbb{R}$ non plus comme un fil déroulé en ligne droite comme on se le représente couramment, mais comme un fil enroulé sur une bobine de diamètre 2π — la bobine $\mathbb{U}$.

Définition-théorème 6.4.3 **(Groupe alterné)** Soit $n \geqslant 2$. Le noyau de la signature ε sur S_n est un sous-groupe distingué de S_n appelé le *groupe alterné de degré n* et noté A_n. En d'autres termes, A_n est l'ensemble des permutations paires de S_n.

Le quotient $\dfrac{S_n}{A_n}$ est isomorphe à $\dfrac{\mathbb{Z}}{2\mathbb{Z}}$. En particulier : $|A_n| = \dfrac{n!}{2}$.

Démonstration D'après le théorème d'isomorphisme, le morphisme de groupes ε, surjectif de S_n sur $\{\pm 1\}$, induit un isomorphisme de $\dfrac{S_n}{A_n}$ sur $\{\pm 1\}$. Comme $\{\pm 1\}$ sont isomorphes, $\dfrac{S_n}{A_n}$ est donc isomorphe à $\dfrac{\mathbb{Z}}{2\mathbb{Z}}$. En particulier, d'après le théorème de Lagrange : $\dfrac{|S_n|}{|A_n|} = |S_n : A_n| = 2$, donc $|A_n| = \dfrac{|S_n|}{2} = \dfrac{n!}{2}$.

Exemple $A_2 = \{\mathrm{Id}\}$, $A_3 = \{\mathrm{Id}, (1\,2\,3), (1\,3\,2)\} = \langle (1\,2\,3)\rangle$ et :

$$A_4 = \{\mathrm{Id}\,,\ \underbrace{(1\,2)\,(3\,4)\,,\ (1\,3)\,(2\,4)\,,\ (1\,4)\,(2\,3)}_{\text{Doubles transpositions}}\,,\ \underbrace{(1\,2\,3)\,,\ (1\,3\,2)\,,\ (1\,2\,4)\,,\ (1\,4\,2)\,,\ (1\,3\,4)\,,\ (1\,4\,3)\,,\ (2\,3\,4)\,,\ (4\,3\,2)}_{\text{3-cycles}}\}$$

6.5 Ordre d'un élément et théorème de Cauchy

Le théorème suivant offre une classification complète à isomorphisme près de tous les groupes monogènes. Nous aurions pu l'établir avant, mais le théorème d'isomorphisme l'éclaire d'une lumière telle qu'il était préférable d'attendre un peu.

Théorème 6.5.1 **(Classification des groupes monogènes)** Soit G un groupe monogène.

- Si G est infini, G est isomorphe à $\mathbb{Z}$.
- Si G est cyclique d'ordre n, G est isomorphe à $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$. Par ailleurs, si on note x un générateur de G :
$$G = \{1, x, x^2, \dots, x^{n-1}\}, \qquad \text{et pour tous } i, j \in \mathbb{Z} : \quad x^i = x^j \iff i \equiv j\ [n].$$

Démonstration L'application $k \overset{\varphi}{\longmapsto} x^k$ est un morphisme de groupes de $\mathbb{Z}$ dans G, surjectif par définition de x. Son noyau est un sous-groupe de $\mathbb{Z}$, donc est de la forme $\operatorname{Ker}\varphi = m\mathbb{Z}$ pour un certain $m \in \mathbb{N}$ unique.

Si $m = 0$, φ est injective, donc c'est un isomorphisme de $\mathbb{Z}$ sur G et en particulier G est infini. Si $m \neq 0$, φ induit par quotient un isomorphisme de $\dfrac{\mathbb{Z}}{m\mathbb{Z}}$ sur G d'après le théorème d'isomorphisme. En particulier, dans ce cas : $m = |\mathbb{Z} : m\mathbb{Z}| = |G| = n$, et pour tous $i, j \in \mathbb{Z}$:

$$x^i = x^j \iff x^{i-j} = 1 \iff i - j \in \operatorname{Ker}\varphi = n\mathbb{Z} \iff i \equiv j\ [n].$$

Il en découle comme voulu que $G = \langle x\rangle = \{x^k \mid k \in \mathbb{Z}\} = \{1, x, x^2, \dots, x^{n-1}\}$.

Théorème 6.5.2 **(Classification des groupes d'ordre premier)** Soit $p \in \mathbb{P}$. Tout groupe d'ordre p est isomorphe à $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$.

Démonstration Soit G un groupe d'ordre p. Donnons-nous un élément x de $G \setminus \{1\}$. D'après le théorème de Lagrange, $\big|\langle x\rangle\big|$ divise $|G| = p$ — sans valoir 1 pour autant — donc $\big|\langle x\rangle\big| = p$, ou encore $G = \langle x\rangle$. Cyclique d'ordre p, G est finalement isomorphe à $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$ d'après **6.5.1**.

Définition-théorème **(Ordre d'un élément dans un groupe)** Soient G un groupe et $x \in G$.

- On appelle *ordre de* x et on note $|x|$ l'ordre du sous-groupe $\langle x\rangle$ — éventuellement $+\infty$.
- Si x est d'ordre fini, $|x|$ est le plus petit entier $k \in \mathbb{N}^*$ pour lequel $x^k = 1$.

  En outre, si G est fini, $|x|$ divise $|G|$.

Démonstration Le fait que $|x| = \big|\langle x\rangle\big|$ divise $|G|$ lorsque G est fini découle simplement du théorème de Lagrange. Ensuite, d'après **6.5.1**, pour tout $k \in \mathbb{N}^*$:

$$x^k = 1 \iff x^k = x^0 \iff k \equiv 0\,\big[|x|\big] \iff |x| \text{ divise } k,$$

donc en effet, $|x|$ est le plus petit entier $k \in \mathbb{N}^*$ pour lequel $x^k = 1$.

Exemple

- Dans $\mathbb{R}$, 1 est d'ordre infini car $\langle 1\rangle = \mathbb{Z}$ est infini.
- Dans $\mathbb{C}^*$, $e^{\frac{2i\pi}{n}}$ est d'ordre n pour tout $n \in \mathbb{N}^*$ car $\left\langle e^{\frac{2i\pi}{n}}\right\rangle = \mathbb{U}_n$ est d'ordre n.
- Dans $\dfrac{\mathbb{Z}}{12\mathbb{Z}}$, 1 est d'ordre 12, 2 d'ordre 6, 3 d'ordre 4, 4 d'ordre 3 et 5 d'ordre 12.
- Dans S_n, pour tous $x_1, \dots, x_p \in [\![1, n]\!]$ distincts, le p-cycle $(x_1\ x_2\ \dots\ x_p)$ est d'ordre p.

Comme on vient de le voir, l'ordre d'un élément divise toujours l'ordre du groupe dans un groupe fini d'après le théorème de Lagrange. La réciproque est-elle vraie ? Autrement dit, un groupe fini G et un diviseur d de $|G|$ étant donnés, G contient-il un élément d'ordre d ? La réponse est non. Par exemple, le groupe S_3 est d'ordre 6, mais ne contient aucun élément d'ordre 6 — sans quoi il serait cyclique, ce qui est faux. Le *théorème de Cauchy* montre qu'à défaut d'un telle réciproque, on peut quand même compter sur l'existence de certains éléments d'ordre prescrit.

Théorème 6.5.3 **(Théorème de Cauchy)** Soient G un groupe fini et p un diviseur premier de $|G|$. Alors G contient un élément d'ordre p.

Démonstration Notons E l'ensemble des applications $f : \mathbb{F}_p \longrightarrow G$ pour lesquelles : $f(0)f(1)\dots f(p-1) = 1$. Construire une telle application revient à choisir arbitrairement les valeurs de $f(1), \dots, f(p-1)$ et à poser : $f(0) = \big(f(1)\dots f(p-1)\big)^{-1}$. Ainsi $|E| = |G|^{p-1}$.

On définit sur E une relation binaire $\sim$ de la façon suivante — pour toutes $f, f' \in E$:

$$f \sim f' \iff \exists k \in \mathbb{F}_p,\quad \forall x \in \mathbb{F}_p,\quad f'(x) = f(x+k).$$

Il n'est pas difficile de vérifier qu'il s'agit là d'une relation d'équivalence sur E. Quelles en sont les classes d'équivalence ? Soit $f \in E$. La classe d'équivalence de f pour $\sim$ est l'ensemble des applications $x \longmapsto f(x+k)$, k décrivant $\mathbb{F}_p$. Se peut-il que deux d'entre elles soient égales ? Soient $k, k' \in \mathbb{F}_p$ distincts pour lesquels pour tout $x \in \mathbb{F}_p$: $f(x+k) = f(x+k')$, ou encore $f(x+k'-k) = f(x)$. Or $k'-k$ est non nul donc inversible dans $\mathbb{F}_p$, donc pour tout $x \in \mathbb{F}_p$: $f(x+1) = f\Big(x + \underbrace{(k'-k) + \dots + (k'-k)}_{(k'-k)^{-1} \text{ fois}}\Big) = f(x)$. Dans ces conditions, f est constante.

En résumé, soit f n'est pas constante et sa classe d'équivalence est de cardinal p, soit f est constante et sa classe d'équivalence est un singleton. En notant a le nombre de classes d'équivalence de cardinal p et b le nombre de classes d'équivalence ponctuelles, on obtient ainsi : $|G|^{p-1} = ap + b$, donc $b \equiv 0\,[p]$. Or $b \geqslant 1$ car la fonction $x \longmapsto 1$ est constante, donc en fait $b \geqslant p$ et E contient une fonction constante $x \longmapsto g$ pour un certain $g \in G \setminus \{1\}$. Finalement, par définition de E : $g^p = 1$, donc $|g|$ divise p, et comme $g \neq 1$, forcément $|g| = p$.

6.6 Groupes résolubles

Les groupes abéliens constituent sans doute la catégorie de groupes les plus simples qu'on puisse imaginer. Un groupe non abélien est toujours un peu plus compliqué à comprendre. Par exemple, un groupe abélien engendré par deux éléments x et y est facile à décrire, ses éléments sont tous de la forme $x^i y^j$, i et j décrivant $\mathbb{Z}$. Sans la commutativité, on ne pourrait pas dire a priori que $x^3y^2xy^5 = x^4y^7$, ces deux éléments seraient potentiellement distincts, et distincts aussi de xy^7x^3 ou $y^3x^4y^4$.

Si tous les groupes ne sont pas abéliens, un groupe peut par chance l'être presque à défaut de l'être tout à fait. En quel sens ? On peut donner de nombreuses significations à cette assertion, dont chacune a ses mérites et démérites. On peut par exemple considérer qu'un groupe G n'est pas loin d'être abélien quand il possède un sous-groupe abélien distingué H pour lequel le quotient $\frac{G}{H}$ est lui-même abélien. Pour le comprendre, plaçons-nous dans le cas simple d'un quotient $\frac{G}{H}$ monogène, disons $\frac{G}{H} = \langle xH \rangle$ pour un certain $x \in G$. Pour tout $g \in G$, gH peut alors être écrit $gH = (xH)^k$ pour un certain $k \in \mathbb{Z}$, ou encore $gH = x^kH$ car H et x « commutent globalement ». Ainsi, g est de la forme x^kh pour certains $h \in H$ et $k \in \mathbb{Z}$, et c'est valable pour un élément g quelconque. Même un élément un peu compliqué comme $x^2hx^{-1}h'xh''x^5$ avec $h, h', h'' \in H$ peut donc être ramené à la forme simple $x^{2-1+1+5}h''' = x^7h'''$ pour un certain $h''' \in H$. Que s'est-il passé finalement ? Même si G n'est pas abélien, le fait que $\frac{G}{H}$ le soit — il est ici monogène — a permis qu'on regroupe les puissances de x entre elles, du moins modulo H.

Ce qu'il faut retenir de cette situation, c'est qu'un groupe G est facile à décrire quand il est l'empilement d'un quotient $\frac{G}{H}$ abélien sur un sous-groupe distingué H lui-même abélien. La définition qui suit est plus difficile à apprécier, mais elle formalise la même intuition.

Définition 6.6.1 **(Groupe résoluble)** Soit G un groupe. On dit que G est *résoluble* s'il possède des sous-groupes $H_0, \dots, H_n$ pour lesquels :

- $\{1\} = H_0 \subset H_1 \subset \dots \subset H_n = G$,
- H_k est distingué dans H_{k+1} pour tout $k \in [\![0, n-1]\!]$,
- le quotient $\frac{H_{k+1}}{H_k}$ est abélien pour tout $k \in [\![0, n-1]\!]$.

Une telle famille $(H_0, \dots, H_n)$ est appelée une *suite de résolubilité de G*.

Quotienter par $H_0 = \{1\}$ revient à ne pas vraiment quotienter car : $\frac{H_1}{H_0} = \{xH_0 \mid x \in H_1\} = \big\{\{x\} \mid x \in H_1\big\}$. Quitte à identifier x et $\{x\}$ pour tout $x \in H_1$, on peut considérer que le quotient $\frac{H_1}{H_0}$ coïncide avec le groupe H_1 lui-même.

Exemple Tout groupe abélien est résoluble.

Démonstration Pour tout groupe abélien G, la famille $\big(\{1\}, G\big)$ est clairement une suite de résolubilité de G.

On rappelle pour les exemples qui suivent que tout groupe d'ordre premier est cyclique — donc abélien — d'après **6.5.2**.

Exemple S_3 et S_4 sont non abéliens mais résolubles.

Démonstration Pour S_3, le sous-groupe $A_3 = \big\langle (1\ 2\ 3) \big\rangle$ est distingué dans G et d'ordre 3 donc abélien, et le quotient associé est d'ordre 2 donc abélien. La famille $\big(\{\mathrm{Id}\}, A_3, S_3\big)$ est ainsi une suite de résolubilité de S_3.

Pour S_4, on peut poser : $H_0 = \{\mathrm{Id}\}$, $H_1 = \big\{\mathrm{Id}\ ,\ (1\ 2)\ (3\ 4)\ ,\ (1\ 3)\ (2\ 4)\ ,\ (1\ 4)\ (2\ 3)\big\}$, $H_2 = A_4$ et $H_3 = S_4$. Clairement, H_1 est abélien, mais $\frac{H_2}{H_1}$ l'est aussi car il est d'ordre 3, ainsi que $\frac{H_3}{H_2}$ qui est d'ordre 2. La famille (H_0, H_1, H_2, H_3) est ainsi une suite de résolubilité de S_4.

Exemple Le groupe des quaternions Q_8 est résoluble.

Démonstration Avec les notations classiques : $Q_8 = \{\pm 1, \pm \mathrm{i}, \pm \mathrm{j}, \pm \mathrm{k}\}$, nous avons déjà vu que le quotient $\frac{Q_8}{\langle -1 \rangle}$ est abélien. La famille $\big(\{1\}, \langle -1 \rangle, Q_8\big)$ est donc une suite de résolubilité de Q_8.

Le théorème qui suit montre que la classe des groupes résolubles est assez stable, elle se comporte bien vis-à-vis des sous-groupes et des quotients. Nous nous servirons beaucoup de cette stabilité au moment de conclure ce texte.

Théorème 6.6.2 **(Sous-groupes et quotients d'un groupe résoluble)** Soient G un groupe et H un sous-groupe de G.

(i) Si G est résoluble, H l'est est aussi.

(ii) Si G est résoluble et si H est distingué dans G, $\dfrac{G}{H}$ est aussi résoluble.

(iii) Si H est distingué dans G et si H et $\dfrac{G}{H}$ sont résolubles, G lui-même est résoluble.

Démonstration

(i) Soit $(H_0,\dots,H_n)$ une suite de résolubilité de G. Nous allons montrer que la famille $(H\cap H_0,\dots,H\cap H_n)$ est une suite de résolubilité de H. Pour commencer : $\quad H\cap H_0 = H\cap\{1\} = \{1\} \quad$ et $\quad H\cap H_n = H\cap G = H$.
Ensuite, pour tout $i\in[\![0,n-1]\!]$, le fait que $H\cap H_i$ soit distingué dans $H\cap H_{i+1}$ ne pose aucune difficulté, mais il reste à montrer que le quotient $\dfrac{H\cap H_{i+1}}{H\cap H_i}$ est abélien. Or l'application $x\longmapsto H_i x$ est un morphisme de groupes de H_{i+1} dans $\dfrac{H_{i+1}}{H_i}$ de noyau H_i, donc sa restriction à $H\cap H_{i+1}$ est un morphisme de groupes de $H\cap H_{i+1}$ dans $\dfrac{H_{i+1}}{H_i}$ de noyau $H\cap H_i$. D'après le théorème d'isomorphisme, ce morphisme induit par quotient un isomorphisme de $\dfrac{H\cap H_{i+1}}{H\cap H_i}$ sur un sous-groupe de $\dfrac{H_{i+1}}{H_i}$. Or $\dfrac{H_{i+1}}{H_i}$ est abélien par hypothèse, donc $\dfrac{H\cap H_{i+1}}{H\cap H_i}$ aussi.

(ii) Soit $(H_0,\dots,H_n)$ une suite de résolubilité de G. Pour tout $i\in[\![0,n]\!]$, notons Q_i le sous-groupe $\dfrac{H_iH}{H}$ de $\dfrac{G}{H}$ et montrons que la famille $(Q_0,\dots,Q_n)$ est une suite de résolubilité de $\dfrac{G}{H}$.
Pour commencer : $\quad Q_0 = \dfrac{H_0H}{H} = \dfrac{H}{H} = \{H\} \quad$ et $\quad Q_n = \dfrac{H_nH}{H} = \dfrac{G}{H}$.
Pour le reste, fixons $i\in[\![0,n-1]\!]$. Le sous-groupe H_i est distingué dans H_{i+1} et H l'est dans G, donc aisément, H_iH est distingué dans $H_{i+1}H$, donc Q_i l'est dans Q_{i+1}. Il reste à montrer que le quotient $\dfrac{Q_{i+1}}{Q_i}$ est abélien. Notons pour cela π_i le morphisme de groupes $xH\longmapsto (xH)\,Q_i$ de Q_{i+1} sur $\dfrac{Q_{i+1}}{Q_i}$. Ce morphisme est surjectif, donc tout élément de $\dfrac{Q_{i+1}}{Q_i}$ peut être écrit sous la forme $\pi_i(xH)$ pour un certain $x\in H_{i+1}$.
Donnons-nous finalement $x,y\in H_{i+1}$ et montrons que : $\quad \pi_i(xH)\,\pi_i(yH) = \pi_i(yH)\,\pi_i(xH)$. Le quotient $\dfrac{H_{i+1}}{H_i}$ étant abélien : $\quad xy = yxh_i \quad$ pour un certain $h_i\in H_i$. En particulier : $\quad h_iH\in\dfrac{H_iH}{H} = Q_i = \operatorname{Ker}\pi_i$,
donc comme voulu : $\quad \pi_i(xH)\,\pi_i(yH) = \pi_i\big((xH)(yH)\big) = \pi_i\big((xy)H\big) = \pi_i\big((yxh_i)H\big)$
$= \pi_i(yH)\,\pi_i(xH)\,\pi_i(h_iH) = \pi_i(yH)\,\pi_i(xH)$.

(iii) Soient $(H_0,\dots,H_m)$ une suite de résolubilité de H et, grâce à **6.3.3**, $\left(\dfrac{K_0}{H},\dots,\dfrac{K_n}{H}\right)$ une suite de résolubilité de $\dfrac{G}{H}$ où $K_0,\dots,K_n$ sont des sous-groupes de G contenant H. La famille $(H_0,\dots,H_m=K_0,\dots,K_n)$ est assez clairement une suite de résolubilité de G, donc G est résoluble. ∎

Définition-théorème 6.6.3 **(Sous-groupe dérivé)** Soit G un groupe. Pour tous $x,y\in G$, on appelle *commutateur de x et y* et on note $\big[x,y\big]$ l'élément $\big[x,y\big] = xyx^{-1}y^{-1}$ de G. Le sous-groupe de G qu'engendrent tous ces éléments est appelé le *sous-groupe dérivé de G* et noté $\mathrm{D}(G)$.

(i) $\mathrm{D}(G)$ est distingué dans G.

(ii) $\dfrac{G}{\mathrm{D}(G)}$ est abélien.

Plus généralement, pour tout sous-groupe distingué H de G, $\dfrac{G}{H}$ est abélien si et seulement si $\mathrm{D}(G)\subset H$.

En résumé, $\mathrm{D}(G)$ est le plus petit sous-groupe distingué de G par le quotient duquel on obtient un groupe abélien. En particulier, G est abélien si et seulement si $\mathrm{D}(G)=1$. Quotienter par $\mathrm{D}(G)$ revient à rendre invisibles les éléments de la forme $xyx^{-1}y^{-1}$ avec $x,y\in G$, et donc à considérer que x et y commutent dans le groupe quotient associé.

Démonstration

(i) Il n'est pas difficile de vérifier que pour tous $x,y,g\in G$: $\quad g\big[x,y\big]g^{-1} = \big[gxg^{-1},gyg^{-1}\big]$. L'ensemble des commutateurs de G est ainsi stable par conjugaison, mais donc aussi le sous-groupe qu'ils engendrent.

(ii) Soit H un sous-groupe distingué de G.

$$\begin{aligned} \mathrm{D}(G) \subset H &\iff \forall x,y \in G,\ \big[x,y\big] \in H &&\iff \forall x,y \in G,\ \big[x^{-1},y^{-1}\big] \in H \\ &\iff \forall x,y \in G,\ x^{-1}y^{-1}xyH = H &&\iff \forall x,y \in G,\ (xH)(yH) = (yH)(xH) \\ &\iff \frac{G}{H} \text{ est abélien.} \end{aligned}$$

Exemple Pour tout $n \geqslant 2$: $\mathrm{D}(S_n) \subset A_n$. Nous verrons que cette inclusion est en fait une égalité au prochain paragraphe.

Démonstration Le quotient $\dfrac{S_n}{A_n}$ est isomorphe à $\dfrac{\mathbb{Z}}{2\mathbb{Z}}$ pour tout $n \geqslant 2$, donc est abélien, donc : $\mathrm{D}(S_n) \subset A_n$ d'après **6.6.3**.

On définit par récurrence, pour tout groupe G, ses sous-groupes dérivés successifs en posant $\mathrm{D}^0(G) = G$ et pour tout $n \in \mathbb{N}$: $\mathrm{D}^{n+1}(G) = \mathrm{D}\big(\mathrm{D}^n(G)\big)$.

Théorème 6.6.4 **(Caractérisation des groupes résolubles par leurs sous-groupes dérivés successifs)** Soit G un groupe. Les assertions suivantes sont équivalentes :

(i) G est résoluble.

(ii) Pour un certain $n \in \mathbb{N}$: $\mathrm{D}^n(G) = \big\{1\big\}$.

Démonstration

(i) $\Longrightarrow$ (ii) Supposons G résoluble. Il existe des sous-groupes $H_0 = \big\{1\big\}, \dots, H_n = G$ de G pour lesquels pour tout $k \in [\![0, n-1]\!]$, H_k est distingué dans H_{k+1} et $\dfrac{H_{k+1}}{H_k}$ est abélien. Ainsi, d'après **6.6.3** : $\mathrm{D}(H_{k+1}) \subset H_k$ pour tout $k \in [\![0, n-1]\!]$, donc : $\mathrm{D}^n(G) = \mathrm{D}^n(H_n) \subset \dots \subset \mathrm{D}^2(H_2) \subset \mathrm{D}(H_1) \subset H_0 = \big\{1\big\}$.

(ii) $\Longrightarrow$ (i) Faisons l'hypothèse que : $\mathrm{D}^n(G) = \big\{1\big\}$ pour un certain $n \in \mathbb{N}$. Le groupe G est alors aussitôt résoluble car : $\big\{1\big\} = \mathrm{D}^n(G) \subset \mathrm{D}^{n-1}(G) \subset \dots \subset \mathrm{D}(G) \subset G$ et pour tout $k \in [\![0, n-1]\!]$, $\mathrm{D}^{k+1}(G)$ est distingué dans $\mathrm{D}^k(G)$ et $\dfrac{\mathrm{D}^k(G)}{\mathrm{D}^{k+1}(G)}$ est abélien d'après **6.6.3**.

6.7 Non-résolubilité du groupe symétrique S_n pour $n \geqslant 5$

Définition 6.7.1 **(Groupe alterné)** Soit $n \geqslant 2$. Le noyau de la signature ε sur S_n est appelé le *groupe alterné de degré n* et noté A_n. En d'autres termes, A_n est l'ensemble des permutations paires de S_n.

Appliqué à la signature $\varepsilon : S_n \longrightarrow \big\{\pm 1\big\}$, le théorème d'isomorphisme montre que les groupes $\dfrac{S_n}{A_n}$ et $\big\{\pm 1\big\}$ sont isomorphes. Le quotient $\dfrac{S_n}{A_n}$ est en particulier abélien, donc d'après le théorème **6.6.3** : $\mathrm{D}(S_n) \subset A_n$. Le même isomorphisme montre aussi que $|A_n| = \dfrac{|S_n|}{2} = \dfrac{n!}{2}$.

Théorème 6.7.2 **(Groupe alterné et 3-cycles)**

(i) Pour tout $n \geqslant 3$, A_n est engendré par les 3-cycles de $[\![1, n]\!]$.

(ii) Pour tout $n \geqslant 5$, les 3-cycles de $[\![1, n]\!]$ sont *conjugués dans A_n*, ce qui veut dire que si σ et σ' sont deux tels 3-cycles : $\sigma' = \alpha\sigma\alpha^{-1}$ pour un certain $\alpha \in A_n$.

Démonstration

(i) Si le groupe S_n est engendré par les transpositions de $[\![1,n]\!]$, A_n l'est quant à lui par les doubles transpositions, i.e. par les permutations de la forme $(a\ b)\,(c\ d)$ avec $a,b,c,d \in [\![1,n]\!]$. Il nous suffit dès lors de montrer que toute double transposition est un produit de 3-cycles. Or :

— si deux des nombres a, b, c et d sont égaux, par exemple $a=c$: $\quad (a\ b)\,(c\ d)=(a\ b)\,(a\ d)=(a\ b\ d)$,

— si a, b, c et d sont distincts : $\quad (a\ b)\,(c\ d)=(a\ b)\,(b\ c)\,(b\ c)\,(c\ d)=(a\ b\ c)\,(b\ c\ d)$.

(ii) Soient $(a\ b\ c)$ et $(a'\ b'\ c')$ deux 3-cycles de $[\![1,n]\!]$. Donnons-nous φ une permutation quelconque de $[\![1,n]\!]$ pour laquelle : $\quad \varphi(a)=a', \quad \varphi(b)=b' \quad$ et $\quad \varphi(c)=c'$. Aussitôt :

$$\varphi(a\ b\ c)\,\varphi^{-1}=\big(\varphi(a)\ \ \varphi(b)\ \ \varphi(c)\big)=(a'\ b'\ c').$$

Si $\varphi \in A_n$, c'est fini. Sinon, nous pouvons nous donner deux éléments d' et e' de $[\![1,n]\!]\setminus\{a',b',c'\}$ car $n\geqslant 5$. Il se trouve alors que $(d'\ e')\,(a'\ b'\ c')\,(d'\ e')=(a'\ b'\ c')$, donc : $\quad \big((d'e')\varphi\big)(a\ b\ c)\big((d'\ e')\varphi\big)^{-1}=(a'\ b'\ c')$. Or : $\quad \varepsilon\big((d'\ e')\,\varphi\big)=(-1)^2=1, \quad$ donc $(d'\ e')\varphi \in A_n$. ■

Théorème 6.7.3 **(Non-résolubilité du groupe symétrique S_n pour $n\geqslant 5$)** Soit $n\geqslant 5$.

(i) $\quad \mathrm{D}(S_n)=\mathrm{D}(A_n)=A_n$.

(ii) S_n n'est pas résoluble.

Démonstration

(i) Évidemment : $\quad \mathrm{D}(A_n)\subset \mathrm{D}(S_n)\subset A_n$. Il nous reste à montrer l'inclusion $A_n\subset \mathrm{D}(A_n)$, et d'après **6.7.2**, il nous suffit pour cela de montrer que $\mathrm{D}(A_n)$ contient tous les 3-cycles de $[\![1,n]\!]$. Soit σ un tel 3-cycle. Alors σ^{-1} est aussi un 3-cycle, donc est conjugué à σ dans A_n d'après **6.7.2** : $\quad \sigma^{-1}=\alpha\sigma\alpha^{-1}$ pour un certain $\alpha\in A_n$. Aussitôt : $\quad \sigma=\sigma^{-2}=\big[\alpha,\sigma\big]\in \mathrm{D}(A_n)$.

(ii) D'après (i) : $\quad \mathrm{D}^2(S_n)=\mathrm{D}(A_n)=A_n=\mathrm{D}(S_n), \quad$ donc pour tout $k\in\mathbb{N}^*$: $\quad \mathrm{D}^k(S_n)=A_n\neq\big\{\mathrm{Id}\big\}$. ■

CHAPITRE 7 LA CORRESPONDANCE DE GALOIS 2

La correspondance de Galois, nous l'avons vu, énonce un lien bijectif entre les sous-groupes du groupe de Galois d'une extension donnée et ses extensions intermédiaires. Soit K un sous-corps de $\mathbb{C}$, L une extension galoisienne de K et E une sous-K-extension de L. Il est alors vrai que L est galoisienne sur E, mais nous avons vu qu'en général E n'est pas galoisienne sur K. Par exemple, $\mathbb{Q}\big(\mathrm{j}, \sqrt[3]{2}\big)$ est galoisienne sur $\mathbb{Q}$ mais $\mathbb{Q}\big(\sqrt[3]{2}\big)$ ne l'est pas. À quelle condition sur $\mathrm{Gal}(L|K)$ peut-on dire que E est galoisienne sur K ? Le travail de Galois répond aussi à cette question, je parlerai à ce sujet de la *correspondance de Galois 2*.

Théorème 7.0.1 **(Conjugaison dans un groupe de Galois)** Soient K un sous-corps de $\mathbb{C}$, L une extension galoisienne de K et E une sous-K-extension de L. Pour tout $g \in \mathrm{Gal}(L|K)$: $\quad g\mathrm{Gal}(L|E)g^{-1} = \mathrm{Gal}\big(L\big|g(E)\big)$.

Démonstration Soit $\varphi \in \mathrm{Gal}(L|E)$. Pour tout $x = g(t) \in g(E)$ avec $t \in E$: $\quad g\varphi g^{-1}(x) = g\varphi(t) = g(t) = x$, donc $g\varphi g^{-1} \in \mathrm{Gal}\big(L\big|g(E)\big)$.

Inversement, soit $\psi \in \mathrm{Gal}\big(L\big|g(E)\big)$. Pour tout $x \in E$: $\quad g(x) \in g(E)$, $\quad$ donc $g^{-1}\psi g(x) = g^{-1}g(x) = x$, donc $g^{-1}\psi g \in \mathrm{Gal}(L|E)$, ou encore $\psi \in g\mathrm{Gal}(L|E)g^{-1}$. ∎

Théorème 7.0.2 **(Correspondance de Galois 2)** Soient K un sous-corps de $\mathbb{C}$, L une extension galoisienne de K et E une sous-K-extension de L. Les assertions suivantes sont équivalentes :

(i) E est galoisienne sur K.

(ii) $\mathrm{Gal}(L|E)$ est distingué dans $\mathrm{Gal}(L|K)$.

Dans ce cas, les groupes $\dfrac{\mathrm{Gal}(L|K)}{\mathrm{Gal}(L|E)}$ et $\mathrm{Gal}(E|K)$ sont isomorphes.

Démonstration D'après **7.0.1** et la correspondance de Galois 1 : $\quad L^{g\mathrm{Gal}(L|E)g^{-1}} = L^{\mathrm{Gal}(L|g(E))} = g(E)$ $\quad$ pour tout $g \in \mathrm{Gal}(L|K)$. Il en découle que $\mathrm{Gal}(L|E)$ est distingué dans $\mathrm{Gal}(L|K)$ si et seulement si pour tout $g \in \mathrm{Gal}(L|K)$: $g(E) = L^{g\mathrm{Gal}(L|E)g^{-1}} = L^{\mathrm{Gal}(L|E)} = E$.

- Supposons E galoisienne sur K, corps de décomposition sur K d'un certain polynôme $P \in K[X]$ de racines distinctes $x_1, \dots, x_n \in E$. Pour tout $g \in \mathrm{Gal}(L|K)$ et pour tout racine x_i de P dans $\mathbb{C}$, $g(x_i)$ est aussi racine de P d'après **4.1.2**, donc appartient à $E = K(x_1, \dots, x_n)$. A fortiori $g(E) \subset E$. Or E étant un corps, $g_{|_E}$ est injectif d'après **4.1.3**, et comme E est de dimension finie sur K : $\quad g(E) = E$. $\quad$ Comme voulu, $\mathrm{Gal}(L|E)$ est distingué dans $\mathrm{Gal}(L|K)$.

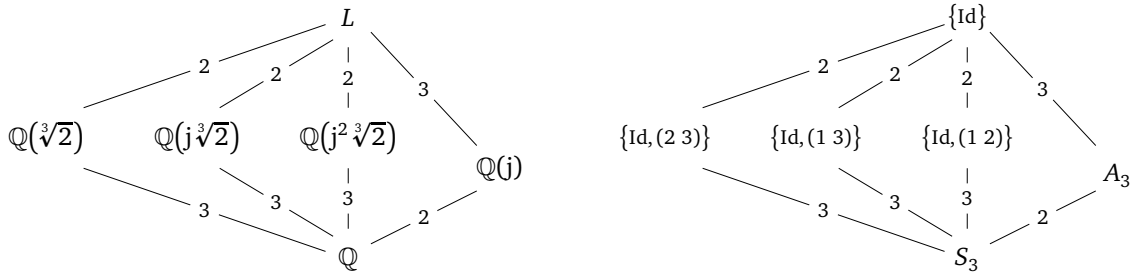
- Réciproquement, supposons $\mathrm{Gal}(L|E)$ distingué dans $\mathrm{Gal}(L|K)$. Pour tout $g \in \mathrm{Gal}(L|K)$: $\quad g_{|_E} \in \mathrm{Gal}(E|K)$ d'après l'introduction de cette preuve, et l'application $g \overset{\rho}{\longmapsto} g_{|_E}$ ainsi définie est un morphisme de groupes de $\mathrm{Gal}(L|K)$ dans $\mathrm{Gal}(E|K)$. D'après le théorème d'Artin appliqué au sous-groupe $\mathrm{Im}\,\rho$ de $\mathrm{Gal}(E|K)$: $\mathrm{Im}\,\rho = \mathrm{Gal}\big(E\big|E^{\mathrm{Im}\,\rho}\big)$ $\quad$ avec :

$$E^{\mathrm{Im}\,\rho} = \Big\{x \in E \mid \quad \forall g \in \mathrm{Gal}(L|K), \quad \rho(g)(x) = x\Big\} = \Big\{x \in E \mid \quad \forall g \in \mathrm{Gal}(L|K), \quad g(x) = x\Big\}$$
$$= E \cap L^{\mathrm{Gal}(L|K)} = E \cap K = K. \qquad \text{Conclusion : } \rho \text{ est surjective.}$$

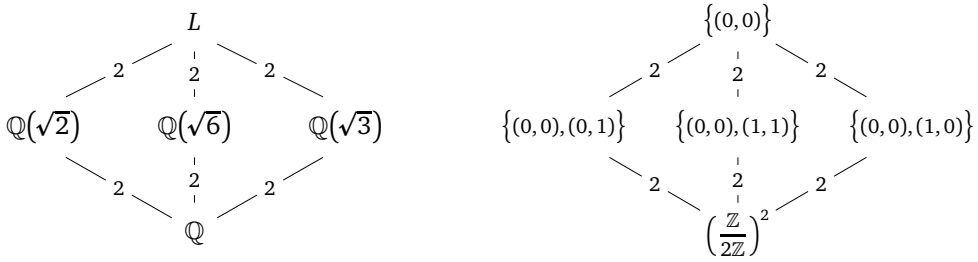
  Par ailleurs : $\quad \mathrm{Ker}\,\rho = \Big\{g \in \mathrm{Gal}(L|K) \mid \quad g_{|_E} = \mathrm{Id}\Big\} = \mathrm{Gal}(L|E)$, $\quad$ donc d'après le théorème d'isomorphisme, ρ induit par quotient un isomorphisme de $\dfrac{\mathrm{Gal}(L|K)}{\mathrm{Gal}(L|E)}$ sur $\mathrm{Gal}(E|K)$. En particulier, d'après le théorème de Lagrange, L étant galoisienne sur K et E : $\quad \big|\mathrm{Gal}(E|K)\big| = \dfrac{\big|\mathrm{Gal}(L|K)\big|}{\big|\mathrm{Gal}(L|E)\big|} = \dfrac{\big|L : K\big|}{\big|L : E\big|} = \big|E : K\big|$, $\quad$ donc E est galoisienne sur K. ∎

Exemple On reprend l'exemple de l'extension galoisienne $L = \mathbb{Q}\big(\mathrm{j}, \sqrt[3]{2}\big)$ de $\mathbb{Q}$, de groupe de Galois isomorphe à S_3 si on numérote $\sqrt[3]{2}$, $\mathrm{j}\sqrt[3]{2}$ et $\mathrm{j}^2\sqrt[3]{2}$ respectivement 1, 2 et 3. Les diagrammes ci-dessous ont déjà été justifiés en temps voulu. On ajuste indiqué en plus sur chaque branche le degré de l'extension ou l'indice du sous-groupe concernés.

Le groupe S_3 possède exactement 3 sous-groupes distingués, à savoir : $\big\{\mathrm{Id}\big\}$, A_3 et S_3. Quant à la sous-$\mathbb{Q}$-extension galoisienne de $\mathbb{Q}\big(\mathrm{j}, \sqrt[3]{2}\big)$ de $\mathbb{Q}$, il n'y en a que 3 aussi : $\mathbb{Q}\big(\mathrm{j}, \sqrt[3]{2}\big)$, $\mathbb{Q}(\mathrm{j})$ qui est le corps de décomposition de X^2+X+1 sur $\mathbb{Q}$, et $\mathbb{Q}$ lui-même. Les extensions $\mathbb{Q}\big(\sqrt[3]{2}\big)$, $\mathbb{Q}\big(\mathrm{j}\sqrt[3]{2}\big)$ et $\mathbb{Q}\big(\mathrm{j}^2\sqrt[3]{2}\big)$ ne le sont pas car $\pi_{\sqrt[3]{2},\mathbb{Q}} = \pi_{\mathrm{j}\sqrt[3]{2},\mathbb{Q}} = \pi_{\mathrm{j}^2\sqrt[3]{2},\mathbb{Q}} = X^3-2$ admet $\mathbb{Q}\big(\mathrm{j}, \sqrt[3]{2}\big)$ tout entier pour corps de décomposition sur $\mathbb{Q}$.



Exemple On reprend maintenant l'exemple de l'extension galoisienne $\mathbb{Q}\big(\sqrt{2}, \sqrt{3}\big)$ de $\mathbb{Q}$, de groupe de Galois isomorphe à $\left(\dfrac{\mathbb{Z}}{2\mathbb{Z}}\right)^2$. On rappelle que cet isomorphisme associe à tout $\mathbb{Q}$-automorphisme g de L l'unique couple $(\varepsilon_2, \varepsilon_3)$ défini par : $g\big(\sqrt{2}\big) = (-1)^{\varepsilon_2}\sqrt{2}$ et $g\big(\sqrt{3}\big) = (-1)^{\varepsilon_3}\sqrt{3}$. Le groupe $\left(\dfrac{\mathbb{Z}}{2\mathbb{Z}}\right)^2$ est abélien, donc ses sous-groupes sont tous distingués. Côté extensions, il est clair que $\mathbb{Q}$, $\mathbb{Q}\big(\sqrt{2}\big)$, $\mathbb{Q}\big(\sqrt{3}\big)$, $\mathbb{Q}\big(\sqrt{6}\big)$ et L sont toutes galoisiennes sur $\mathbb{Q}$, corps de décomposition sur $\mathbb{Q}$ des polynômes respectifs : X, X^2-2, X^2-3, X^2-6 et X^4-10X^2+1.



Exemple Posant : $\theta = \sqrt{\big(2+\sqrt{2}\big)\big(3+\sqrt{3}\big)}$, nous allons montrer que l'extension $\mathbb{Q}(\theta)$ est galoisienne sur $\mathbb{Q}$ et calculer son groupe de Galois.

- Comme : $\theta^2 = 6+3\sqrt{2}+2\sqrt{3}+\sqrt{6}$, $\mathbb{Q}\big(\theta^2\big)$ est l'une des 5 sous-$\mathbb{Q}$-extensions de $\mathbb{Q}\big(\sqrt{2}, \sqrt{3}\big)$ de l'exemple précédent, de $\mathbb{Q}$-bases respectives : (1), $\big(1, \sqrt{2}\big)$, $\big(1, \sqrt{3}\big)$, $\big(1, \sqrt{6}\big)$ et $\big(1, \sqrt{2}, \sqrt{3}, \sqrt{6}\big)$. Or les coordonnées de θ^2 dans cette dernière base étant toutes non nulles : $\mathbb{Q}\big(\theta^2\big) = \mathbb{Q}\big(\sqrt{2}, \sqrt{3}\big)$. En particulier, $\mathbb{Q}(\theta)$ contient $\mathbb{Q}\big(\sqrt{2}, \sqrt{3}\big)$.
- Notons g_{i} (resp. g_{j}) l'unique $\mathbb{Q}$-automorphisme de $\mathbb{Q}\big(\sqrt{2}, \sqrt{3}\big)$ pour lequel : $g_{\mathrm{i}}\big(\sqrt{2}\big) = -\sqrt{2}$ et $g_{\mathrm{i}}\big(\sqrt{3}\big) = \sqrt{3}$ (resp. : $g_{\mathrm{j}}\big(\sqrt{2}\big) = \sqrt{2}$ et $g_{\mathrm{j}}\big(\sqrt{3}\big) = -\sqrt{3}$). Aussitôt :
$$g_{\mathrm{i}}\big(\theta^2\big) = g_{\mathrm{i}}\Big(\big(2+\sqrt{2}\big)\big(3+\sqrt{3}\big)\Big) = \big(2-\sqrt{2}\big)\big(3+\sqrt{3}\big) = \frac{2-\sqrt{2}}{2+\sqrt{2}}\,\theta^2 = \frac{\big(2-\sqrt{2}\big)^2}{2}\,\theta^2 = \Big(\big(\sqrt{2}-1\big)\,\theta\Big)^2$$
et : $g_{\mathrm{j}}\big(\theta^2\big) = g_{\mathrm{j}}\Big(\big(2+\sqrt{2}\big)\big(3+\sqrt{3}\big)\Big) = \big(2+\sqrt{2}\big)\big(3-\sqrt{3}\big) = \dfrac{3-\sqrt{3}}{3+\sqrt{3}}\,\theta^2 = \dfrac{\big(3-\sqrt{3}\big)^2}{6}\,\theta^2 = \left(\dfrac{\sqrt{3}-1}{\sqrt{2}}\,\theta\right)^2$.
- Si jamais $\theta \in \mathbb{Q}\big(\sqrt{2}, \sqrt{3}\big)$: $g_{\mathrm{i}}\big(\theta^2\big) = g_{\mathrm{i}}(\theta)^2$, donc $g_{\mathrm{i}}(\theta) = \varepsilon\big(\sqrt{2}-1\big)\,\theta$ pour un certain $\varepsilon \in \big\{\pm 1\big\}$, donc : $g_{\mathrm{i}}^2(\theta) = g_{\mathrm{i}}\Big(\varepsilon\big(\sqrt{2}-1\big)\,\theta\Big) = \varepsilon\big(-\sqrt{2}-1\big) \times \varepsilon\big(\sqrt{2}-1\big)\,\theta = -\theta$, alors que $g_{\mathrm{i}}^2 = \mathrm{Id}$. Conclusion : $\theta \notin \mathbb{Q}\big(\sqrt{2}, \sqrt{3}\big)$, et comme $X^2-\theta^2$ admet θ pour racine : $\pi_{\theta,\mathbb{Q}(\theta^2)} = X^2-\theta^2$. D'après **4.2.2**, nous pouvons ainsi introduire l'unique $\mathbb{Q}$-automorphisme g_{-1} de $\mathbb{Q}(\theta)$ pour lequel $g_{-1}(\theta) = -\theta$. En particulier $g_{-1} \neq \mathrm{Id}$, mais $g_{-1}^2 = \mathrm{Id}$ d'après **4.1.4** car $g_{-1}^2(\theta) = -(-\theta) = \theta$.
- Nous allons maintenant exploiter le théorème **4.2.3** pour prolonger g_{i} et g_{j} en des $\mathbb{Q}$-automorphismes de $\mathbb{Q}(\theta)$. Or :
$$(g_{\mathrm{i}})_X\big(\pi_{\theta,\mathbb{Q}(\theta^2)}\big) = X^2 - g_{\mathrm{i}}\big(\theta^2\big) = X^2 - \Big(\big(\sqrt{2}-1\big)\,\theta\Big)^2 \qquad \text{et} \qquad (g_{\mathrm{j}})_X\big(\pi_{\theta,\mathbb{Q}(\theta^2)}\big) = X^2 - g_{\mathrm{j}}\big(\theta^2\big) = X^2 - \left(\frac{\sqrt{3}-1}{\sqrt{2}}\,\theta\right)^2,$$
donc les relations $g_{\mathrm{i}}(\theta) = \big(\sqrt{2}-1\big)\,\theta$ et $g_{\mathrm{j}}(\theta) = \dfrac{\sqrt{3}-1}{\sqrt{2}}\,\theta$ prolongent g_{i} et g_{j} en des $\mathbb{Q}$-morphismes de $\mathbb{Q}(\theta)$ dans $\mathbb{C}$, qui sont en fait des $\mathbb{Q}$-automorphismes de $\mathbb{Q}(\theta)$ car $\mathbb{Q}(\theta)$ contient $\sqrt{2}$ et $\sqrt{3}$. Aussitôt :

$g_{\mathrm{i}}^2(\theta) = g_{\mathrm{i}}\Big(\big(\sqrt{2}-1\big)\theta\Big) = \big(-\sqrt{2}-1\big)\times\big(\sqrt{2}-1\big)\theta = -\theta$ et $g_{\mathrm{j}}^2(\theta) = g_{\mathrm{j}}\left(\dfrac{\sqrt{3}-1}{\sqrt{2}}\,\theta\right) = \dfrac{-\sqrt{3}-1}{\sqrt{2}}\times\dfrac{\sqrt{3}-1}{\sqrt{2}}\theta = -\theta,$

donc d'après **4.1.4** : $g_{\mathrm{i}}^2 = g_{\mathrm{j}}^2 = g_{-1}$. En particulier $g_{\mathrm{i}}^4 = g_{\mathrm{j}}^4 = \mathrm{Id}$, mais aussi $g_{-1}\big(\sqrt{2}\big) = \sqrt{2}$ et $g_{-1}\big(\sqrt{3}\big) = \sqrt{3}$.

- On pose enfin : $g_1 = \mathrm{Id}$, $g_{-\mathrm{i}} = g_{-1}g_{\mathrm{i}}$, $g_{-\mathrm{j}} = g_{-1}g_{\mathrm{j}}$, $g_{\mathrm{k}} = g_{\mathrm{i}}g_{\mathrm{j}}$ et $g_{-\mathrm{k}} = g_{-1}g_{\mathrm{i}}g_{\mathrm{j}}$. Le tableau ci-dessous résume la manière dont les 8 $\mathbb{Q}$-automorphismes en présence agissent sur $\sqrt{2}$ et $\sqrt{3}$. Comme $g_{-1} \neq \mathrm{Id}$, on y voit bien qu'ils sont distincts. Or par ailleurs :

$$\Big|\mathrm{Gal}\big(\mathbb{Q}(\theta)\big|\mathbb{Q}\big)\Big| \leqslant \big[\mathbb{Q}(\theta):\mathbb{Q}\big] = \big[\mathbb{Q}(\theta):\mathbb{Q}\big(\sqrt{2},\sqrt{3}\big)\big] \times \big[\mathbb{Q}\big(\sqrt{2},\sqrt{3}\big):\mathbb{Q}\big] = \deg\big(\pi_{\theta,\mathbb{Q}(\theta^2)}\big) \times 4 = 8,$$

donc $\mathbb{Q}(\theta)$ est galoisienne sur $\mathbb{Q}$ et : $\mathrm{Gal}\big(\mathbb{Q}(\theta)\big|\mathbb{Q}\big) = \Big\{g_1, g_{-1}, g_{\mathrm{i}}, g_{-\mathrm{i}}, g_{\mathrm{j}}, g_{-\mathrm{j}}, g_{\mathrm{k}}, g_{-\mathrm{k}}\Big\}$.

	g_1 / g_{-1}	g_{i} / $g_{-\mathrm{i}}$	g_{j} / $g_{-\mathrm{j}}$	g_{k} / $g_{-\mathrm{k}}$
$\sqrt{2}$	$\sqrt{2}$	$-\sqrt{2}$	$\sqrt{2}$	$-\sqrt{2}$
$\sqrt{3}$	$\sqrt{3}$	$\sqrt{3}$	$-\sqrt{3}$	$-\sqrt{3}$

- Évidemment, les notations choisies suggèrent que le groupe de Galois étudié est isomorphe au groupe des quaternions Q_8. C'est ce que nous allons prouver. Or : $g_{\mathrm{j}}g_{\mathrm{i}}(\theta) = g_j\Big(\big(\sqrt{2}-1\big)\theta\Big) = \big(\sqrt{2}-1\big)\times\dfrac{\sqrt{3}-1}{\sqrt{2}}\,\theta$ et :

$$g_{-\mathrm{k}}(\theta) = g_{-1}g_{\mathrm{i}}g_{\mathrm{j}}(\theta) = g_{-1}g_{\mathrm{i}}\left(\frac{\sqrt{3}-1}{\sqrt{2}}\,\theta\right) = g_{-1}\left(\frac{\sqrt{3}-1}{-\sqrt{2}}\times\big(\sqrt{2}-1\big)\theta\right) = \frac{\sqrt{3}-1}{-\sqrt{2}}\times\big(\sqrt{2}-1\big)(-\theta) = g_{\mathrm{j}}g_{\mathrm{i}}(\theta),$$

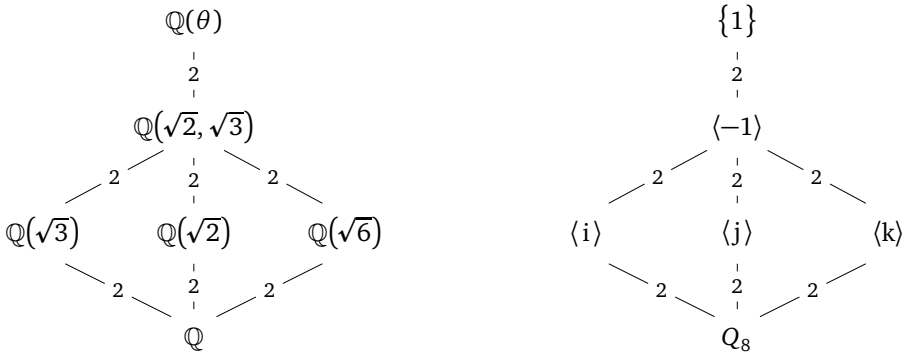
donc d'après **4.1.4** : $g_{\mathrm{j}}g_{\mathrm{i}} = g_{-\mathrm{k}}$. C'en est assez pour tout savoir du groupe étudié. Par exemple :

$$g_{\mathrm{k}}^2 = (g_{\mathrm{i}}g_{\mathrm{j}})^2 = g_{\mathrm{i}}(g_{\mathrm{j}}g_{\mathrm{i}})g_{\mathrm{j}} = g_{\mathrm{i}}(g_{-1}g_{\mathrm{i}}g_{\mathrm{j}})g_{\mathrm{j}} = g_{\mathrm{i}}\big(g_{\mathrm{i}}^2g_{\mathrm{i}}g_{\mathrm{j}}\big)g_{\mathrm{j}} = g_{\mathrm{i}}^4g_{\mathrm{j}}^2 = \mathrm{Id}\,g_{-1} = g_{-1}$$

et $g_{\mathrm{k}}g_{\mathrm{i}} = (g_{\mathrm{i}}g_{\mathrm{j}})g_{\mathrm{i}} = g_{\mathrm{i}}(g_{\mathrm{j}}g_{\mathrm{i}}) = g_{\mathrm{i}}(g_{-1}g_{\mathrm{i}}g_{\mathrm{j}}) = g_{\mathrm{i}}\big(g_{\mathrm{i}}^2g_{\mathrm{i}}g_{\mathrm{j}}\big) = g_{\mathrm{i}}^4g_{\mathrm{j}} = \mathrm{Id}\,g_{\mathrm{j}} = g_{\mathrm{j}}$.

L'application $x \longmapsto g_x$ est ainsi clairement un isomorphisme de Q_8 sur $\mathrm{Gal}\big(\mathbb{Q}(\theta)\big|\mathbb{Q}\big)$.

- Il ne nous reste plus qu'à exploiter la correspondance de Galois pour comprendre $\mathbb{Q}(\theta)$ en profondeur. Et comme Q_8 n'a que 6 sous-groupes, $\mathbb{Q}(\theta)$ n'a que 6 sous-$\mathbb{Q}$-extensions. Or nous en connaissons déjà 6, il suffit de les placer au bon endroit en s'aidant du tableau ci-dessus. Enfin, les sous-groupes de Q_8 sont tous distingués, donc d'après la correspondance de Galois 2, les sous-$\mathbb{Q}$-extensions de $\mathbb{Q}(\theta)$ sont toutes galoisiennes sur $\mathbb{Q}$.



Il reste peut-être à se demander quel corps de décomposition sur $\mathbb{Q}$ se cache derrière $\mathbb{Q}(\theta)$. Il nous suffit pour cela de trouver un polynôme unitaire de $\mathbb{Q}[X]$ de degré 8 dont θ est racine. Or après calcul : $\theta^2 = 6 + 3\sqrt{2} + 2\sqrt{3} + \sqrt{6}$,

$$\theta^4 = 72 + 48\sqrt{2} + 36\sqrt{3} + 24\sqrt{6}, \qquad \theta^6 = 1080 + 756\sqrt{2} + 600\sqrt{3} + 420\sqrt{6}$$

et : $\theta^8 = 17136 + 12096\sqrt{2} + 9792\sqrt{3} + 6912\sqrt{6}$, donc pour tous $a, b, c \in \mathbb{Q}$:

$$\theta^8 + a\theta^6 + b\theta^4 + c\theta^2 = \big(17136 + 1080a + 72b + 6c\big) + \big(12096 + 756a + 48b + 3c\big)\sqrt{2} + \big(9792 + 600a + 36b + 2c\big)\sqrt{3} + \big(6912 + 420a + 24b + c\big)\sqrt{6}.$$

Demandons-nous à présent pour quelles valeurs de a, b et c les coordonnées de cette quantité selon $\sqrt{2}$, $\sqrt{3}$ et $\sqrt{6}$ sont nulles. Après résolution d'un système linéaire, on obtient : $a = -24$, $b = 144$ et $c = -288$. En retour : $\theta^8 - 24\theta^6 + 144\theta^4 - 288\theta^2 = -144$. Conclusion : $\pi_{\theta,\mathbb{Q}} = X^8 - 24X^6 + 144X^4 - 288X^2 + 144$.

CHAPITRE 8 RÉSOLUBILITÉ PAR RADICAUX

Nous attaquons enfin la dernière partie de ce texte, sa conclusion. La notion de polynôme résoluble par radicaux a été définie à la fin du chapitre **2**. Nous allons montrer dans cet ultime chapitre qu'un polynôme est résoluble par radicaux si et seulement si le groupe de Galois de son corps de décomposition est résoluble. On comprend mieux en passant pourquoi les groupes résolubles portent ce nom. Il nous restera encore à exhiber un polynôme dont le groupe de Galois n'est pas résoluble, et nous aurons ainsi démontré que certaines équations polynomiales ne sont pas résolubles par radicaux.

8.1 RÉSOLUBILITÉ PAR RADICAUX ET GROUPE DE GALOIS

Théorème 8.1.1 **(Une famille de groupes de Galois abéliens)** Soient K un sous-corps de $\mathbb{C}$ et $n \in \mathbb{N}^*$. L'extension $K\left(e^{\frac{2i\pi}{n}}\right)$ est galoisienne sur K et son groupe de Galois est abélien.

Démonstration Posons $\omega = e^{\frac{2i\pi}{n}}$. Alors ω est racine de $X^n - 1$ et : $K(\omega) = K\left(1, \omega, \omega^2, \dots, \omega^{n-1}\right)$, donc $K(\omega)$ est le corps de décomposition de $X^n - 1$ sur K, et de ce fait est galoisienne sur K.

Ensuite, soient $g, g' \in \mathrm{Gal}(L|K)$. D'après **4.3.2**, $g(\omega)$ et $g'(\omega)$ sont deux racines de $\pi_{\omega,K}$, donc de $X^n - 1$, disons $g(\omega) = \omega^i$ et $g'(\omega) = \omega^j$ pour certains $i, j \in [\![0, n-1]\!]$. Aussitôt : $g \circ g'(\omega) = \left(\omega^j\right)^i = \left(\omega^i\right)^j = g' \circ g(\omega)$, et par ailleurs, $g \circ g'$ et $g' \circ g$ sont deux K-automorphismes de $K(\omega)$, donc $g \circ g' = g' \circ g$ d'après **4.2.2**. Comme voulu, $\mathrm{Gal}(L|K)$ est abélien.

Théorème 8.1.2 **(Un famille de groupes de Galois résolubles)** Soient K un sous-corps de $\mathbb{C}$, $n \in \mathbb{N}^*$ et $a \in K$. Si on note L le corps de décomposition de $X^n - a$ sur K, le groupe $\mathrm{Gal}(L|K)$ est résoluble.

Démonstration Posons $\omega = e^{\frac{2i\pi}{n}}$. L'extension $K(\omega)$ est galoisienne sur K et $\mathrm{Gal}\left(K(\omega)\middle|K\right)$ est abélien d'après **8.1.1**. La correspondance de Galois 2 affirme en retour que $\mathrm{Gal}\left(L\middle|K(\omega)\right)$ est un sous-groupe distingué de $\mathrm{Gal}(L|K)$ et que le quotient $\dfrac{\mathrm{Gal}(L|K)}{\mathrm{Gal}\left(L\middle|K(\omega)\right)}$ est isomorphe au groupe $\mathrm{Gal}\left(K(\omega)\middle|K\right)$, donc est abélien.

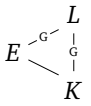
Pour montrer que $\mathrm{Gal}(L|K)$ est résoluble, il nous suffirait donc de savoir que $\mathrm{Gal}\left(L\middle|K(\omega)\right)$ est lui-même abélien. Donnons-nous pour cela une racine quelconque α de $X^n - a$ dans $\mathbb{C}$. Les racines de $X^n - a$ sont tous les nombres $\alpha\omega^i$, i décrivant $[\![0, n-1]\!]$, donc $L = K\left(\alpha, \alpha\omega, \alpha\omega^2, \dots, \alpha\omega^{n-1}\right) = K(\omega)(\alpha)$.

Soient $g, g' \in \mathrm{Gal}\left(L\middle|K(\omega)\right)$. D'après **4.3.2**, $g(\alpha)$ et $g'(\alpha)$ sont deux racines de $\pi_{\alpha,K}$, donc de $X^n - a$, disons $g(\alpha) = \alpha\omega^i$ et $g'(\alpha) = \alpha\omega^j$ pour certains $i, j \in [\![0, n-1]\!]$. Aussitôt, sachant que g et g' fixent ω :

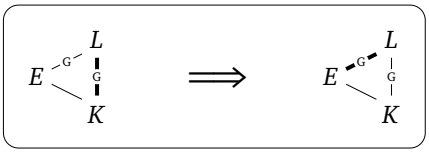
$$g \circ g'(\alpha) = g\left(\alpha\omega^j\right) = g(\alpha)\,\omega^j = \alpha\omega^{i+j} = g'(\alpha)\,\omega^i = g'\left(\alpha\omega^i\right) = g' \circ g(\alpha),$$

et par ailleurs, $g \circ g'$ et $g' \circ g$ sont deux K-automorphismes de $L = K(\omega)(\alpha)$, donc $g \circ g' = g' \circ g$ d'après **4.2.2**. Comme voulu, $\mathrm{Gal}\left(L\middle|K(\omega)\right)$ est abélien.

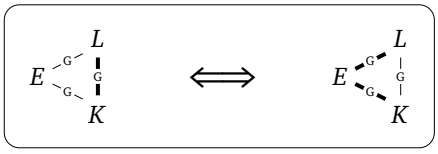
Avant de poursuivre, nous allons tâcher de représenter graphiquement les enseignements majeurs de la correspondance de Galois dans ses versions 1 et 2 et de l'important théorème **6.6.2** relatif aux sous-groupes et quotients d'un groupe résoluble. Cette représentation graphique m'est tout à fait personnelle et n'a vraiment rien d'universel. Donnons-nous un sous-corps K de $\mathbb{C}$ et une extension galoisienne L de K, ainsi qu'une sous-K-extension E de L — pas forcément galoisienne sur K. Nous indiquerons qu'une extension est galoisienne en apposant la lettre « G » sur le segment qui la représente. Par exemple, à ce stade :



Par ailleurs, on peut associer à chaque segment « galoisien » d'un tel graphe son groupe de Galois. Un segment plus épais indiquera désormais que ce groupe de Galois est résoluble. Par exemple, d'après **6.6.2**, si le groupe $\mathrm{Gal}(L|K)$ est résoluble, le sous-groupe $\mathrm{Gal}(L|E)$ l'est aussi. Cet énoncé est résumé dans le cartouche qui suit :



Grâce à la correspondance de Galois 2, nous savons aussi que si E est galoisienne sur K, les groupes $\dfrac{\mathrm{Gal}(L|K)}{\mathrm{Gal}(L|E)}$ et $\mathrm{Gal}(E|K)$ sont isomorphes. A fortiori, d'après **6.6.2**, le groupe $\mathrm{Gal}(L|K)$ est résoluble si et seulement si les groupes $\mathrm{Gal}(L|E)$ et $\mathrm{Gal}(E|K)$ le sont, équivalence que l'on peut aussi résumer dans un cartouche :



Théorème 8.1.3 **(Un dernier lemme avant l'apothéose)** Soient K un sous-corps de $\mathbb{C}$ et $P \in K[X]$, ainsi que $x \in \mathbb{C}$ et $r \in \mathbb{N}^*$ pour lesquels : $x^r \in K$. On note L le corps de décomposition de P sur K. Les assertions suivantes sont équivalentes :

(i) $\mathrm{Gal}(L|K)$ est résoluble.

(ii) $\mathrm{Gal}\big(L(x)\big|K(x)\big)$ est résoluble.

Démonstration Posant : $\omega = \mathrm{e}^{\frac{2\mathrm{i}\pi}{r}}$, nous allons commencer par dresser une liste d'extensions galoisiennes.

— L est galoisienne sur K par hypothèse.

— $L(x)$ est galoisienne sur $K(x)$ comme corps de décomposition de P sur $K(x)$.

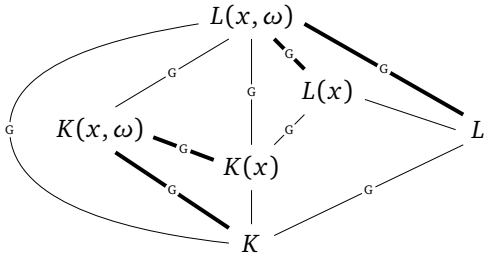
— $K(x,\omega)$ est galoisienne sur K comme corps de décomposition de $X^r - x^r$ sur K car les racines de $X^r - x^r$ sont $x, x\omega, x\omega^2, \dots, x\omega^{r-1}$, et par hypothèse $x^r \in K$. En outre, d'après **8.1.2**, $\mathrm{Gal}\big(K(x,\omega)\big|K\big)$ est résoluble.

— $L(x,\omega)$ est galoisienne sur L comme corps de décomposition de $X^r - x^r$ sur L, et d'après **8.1.2**, $\mathrm{Gal}\big(L(x,\omega)\big|L\big)$ est résoluble.

— $K(x,\omega)$ est galoisienne sur $K(x)$ d'après **8.1.1** et $\mathrm{Gal}\big(K(x,\omega)\big|K(x)\big)$ est abélien, donc résoluble.

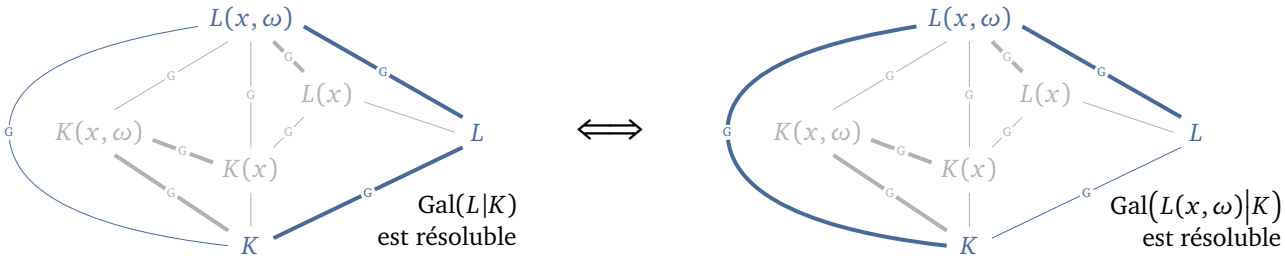
— $L(x,\omega)$ est galoisienne sur $L(x)$ d'après **8.1.1** et $\mathrm{Gal}\big(L(x,\omega)\big|L(x)\big)$ est abélien, donc résoluble.

Pour finir, l'extension $L(x,\omega)$ est galoisienne sur K comme corps de décomposition de $\big(X^r - x^r\big)P$ sur K et c'est dans cette extension ambiante que nous allons travailler. La figure suivante résume la situation.

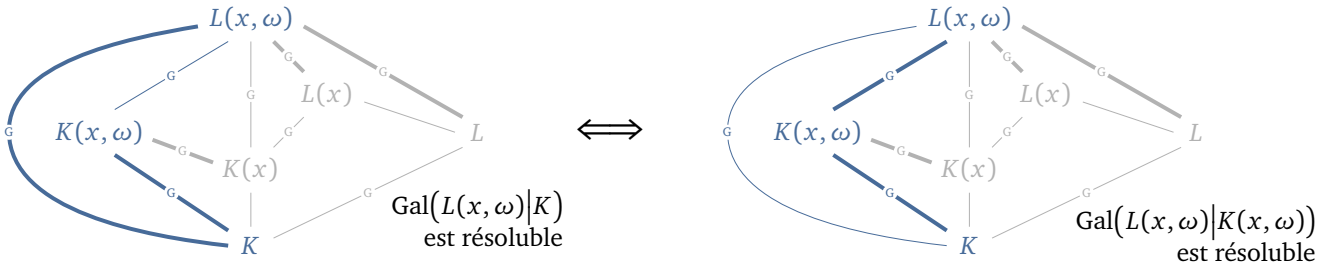


Nous allons maintenant prouver l'équivalence des assertions (i) et (ii) graphiquement en exploitant les cartouches introduits un peu plus haut, seulement le deuxième d'ailleurs. On a représenté en bleu le « triangle » d'extensions dans lequel chaque équivalence est obtenue.

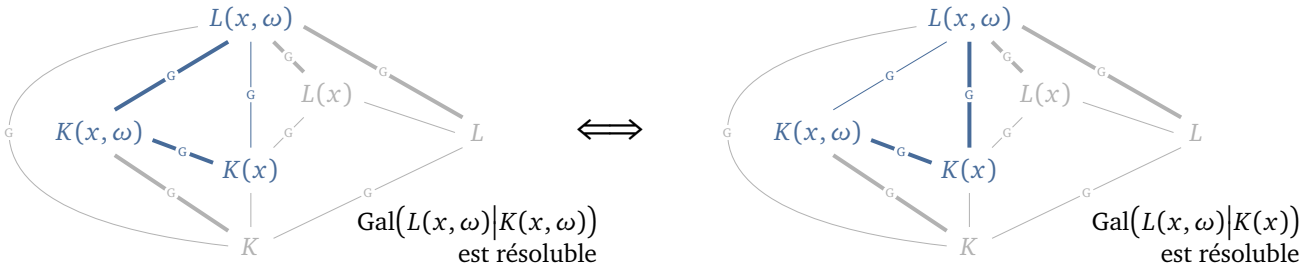
- **Première équivalence :**



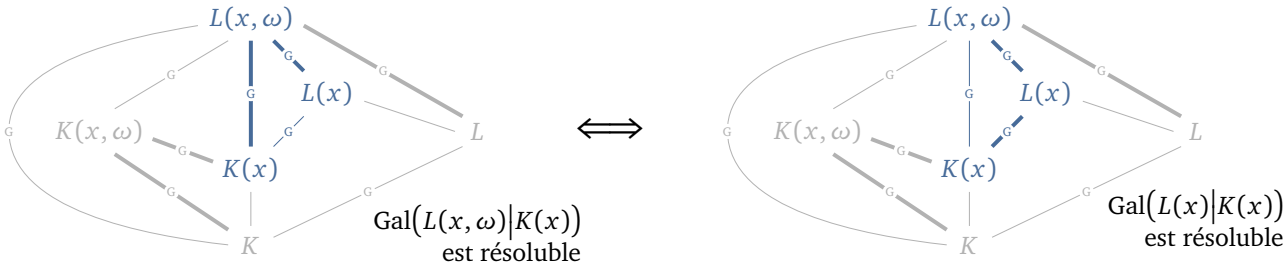
- **Deuxième équivalence :**



- **Troisième équivalence :**



- **Quatrième équivalence :**



On conclut en emboîtant simplement ces quatre équivalences. ∎

Le théorème qui suit est l'aboutissement théorique de ce texte, mais nous n'en prouverons que l'implication (i) $\Longrightarrow$ (ii). Il ne serait pas trop long de démontrer la réciproque, mais l'objectif auquel nous nous sommes astreints ne la rend pas nécessaire. Nous cherchons en effet seulement des exemples de polynômes non résolubles par radicaux et n'aurons donc besoin que de l'implication (i) $\Longrightarrow$ (ii).

Théorème 8.1.4 **(Groupe de Galois d'un polynôme résoluble par radicaux)** Soient K un sous-corps de $\mathbb{C}$ et $P \in K[X]$. On note L le corps de décomposition de P sur K. Les assertions suivantes sont équivalentes :

(i) P est résoluble par radicaux.

(ii) $\mathrm{Gal}(L|K)$ est résoluble.

Démonstration On suppose P résoluble par radicaux. Il existe alors des éléments $x_1, \dots, x_n \in \mathbb{C}$ et des entiers $r_1, \dots, r_n \in \mathbb{N}^*$ pour lesquels $L \subset K(x_1, \dots, x_n)$ et pour tout $i \in [\![1, n]\!]$: $\quad x_i^{r_i} \in K(x_1, \dots, x_{i-1})$.

Soit $i \in [\![1, n]\!]$ fixé. Clairement, $L(x_1, \dots, x_{i-1})$ est le corps de décomposition de P sur $K(x_1, \dots, x_{i-1})$, y compris pour $i = 1$ avec la convention usuelle. En outre : $\quad x_i^{r_i} \in K(x_1, \dots, x_{i-1})$, $\quad$ donc d'après **8.1.3** :

$\mathrm{Gal}\big(L(x_1,\dots,x_{i-1})\big|K(x_1,\dots,x_{i-1})\big)$ est résoluble si et seulement si $\mathrm{Gal}\big(L(x_1,\dots,x_i)\big|K(x_1,\dots,x_i)\big)$ l'est.

Or ici $L(x_1,\dots,x_n)=K(x_1,\dots,x_n)$, donc $\mathrm{Gal}\big(L(x_1,\dots,x_n)\big|K(x_1,\dots,x_n)\big)$ est réduit au singleton $\{\mathrm{Id}\}$, donc est résoluble. À l'autre bout de la chaîne, pour $i=1$, le groupe $\mathrm{Gal}(L|K)$ est ainsi résoluble. ∎

Théorème 8.1.5 **(Une condition suffisante de non-résolubilité par radicaux sur $\mathbb{Q}$)** Soit $P\in\mathbb{Q}[X]$. Si P est irréductible sur $\mathbb{Q}$, de degré un nombre premier supérieur ou égal à 5, et possède exactement deux racines non réelles, alors il n'est pas résoluble par radicaux sur $\mathbb{Q}$.

Ce théorème n'énonce qu'une condition suffisante, mais il a pour lui l'avantage de la simplicité et nous n'irons pas au-delà.

Démonstration Notons p le degré de P et L le corps de décomposition de P sur $\mathbb{Q}$. Irréductible sur $\mathbb{Q}$, P est à racines simples dans $\mathbb{C}$ d'après **1.1.2**. Nous noterons ses racines $x_1,\dots,x_p$ où, par exemple, x_1 et x_2 sont les deux racines complexes non réelles conjuguées de P.

Le théorème **4.6.1** en tête, nous identifierons $\mathrm{Gal}(L|\mathbb{Q})$ à un sous-groupe de S_p via le morphisme de groupes injectif $g\longmapsto g|_{\{x_1,\dots,x_p\}}$ et l'identification de la racine x_i et de l'entier i pour tout $i\in[\![1,p]\!]$. Nous allons montrer en fait que $\mathrm{Gal}(L|\mathbb{Q})=S_p$. Comme $p\geqslant 5$, il en découlera que $\mathrm{Gal}(L|\mathbb{Q})$ n'est pas résoluble d'après **6.7.3**, puis que P n'est pas résoluble par radicaux sur $\mathbb{Q}$ d'après d'après **8.1.4**.

À présent, pour montrer l'égalité $\mathrm{Gal}(L|\mathbb{Q})=S_p$, il nous suffit de montrer que $\mathrm{Gal}(L|\mathbb{Q})$ contient à la fois une transposition et un p-cycle d'après un exemple du chapitre **6**, et ce parce que p est premier.

— Le polynôme P est à coefficients réels, l'ensemble $\{x_1,\dots,x_p\}$ de ses racines est stable par conjugaison et $L=\mathbb{Q}(x_1,\dots,x_p)$ l'est a fortiori. Il est équivalent de dire que l'application $z\longmapsto\overline{z}$ est un $\mathbb{Q}$-automorphisme de L. Or, considéré dans S_p comme une permutation de $\{x_1,\dots,x_p\}$, ce $\mathbb{Q}$-automorphisme n'est autre que la transposition $(1\ 2)$ car $\overline{x_1}=x_2$ et pour tout $k\in[\![3,p]\!]$: $\overline{x_k}=x_k$. Conclusion : $\mathrm{Gal}(L|\mathbb{Q})$ contient la transposition $(1\ 2)$.

— Comme P est irréductible sur $\mathbb{Q}$: $P=\pi_{x_1,\mathbb{Q}}$. Il en découle d'après **6.2.3** que $\deg\big(\pi_{x_1,\mathbb{Q}}\big)=p$ divise $\big|\mathrm{Gal}(L|\mathbb{Q})\big|$, puis que $\mathrm{Gal}(L|\mathbb{Q})$ contient un élément d'ordre p d'après le théorème de Cauchy. Or dans S_p, les seuls éléments d'ordre p sont les p-cycles, donc $\mathrm{Gal}(L|\mathbb{Q})$ contient un p-cycle. ∎

8.2 Exemples de polynômes non résolubles par radicaux sur $\mathbb{Q}$

Exemple Les polynômes $P=X^5-5X-1$ et $Q=X^5-10X+5$ ne sont pas résolubles par radicaux.

Démonstration Grâce à **8.1.5**, il nous suffit de montrer que P et Q sont irréductibles sur $\mathbb{Q}$ et possèdent exactement deux racines non réelles. Leur irréductibilité a déjà été prouvée grâce au critère d'Eisenstein et on tire aisément des tableaux de variations qui suivent leur nombre de racines réelles.

x	$-\infty$		-1		1		$+\infty$
$P'(x)$		$+$	0	$-$	0	$+$	
$P(x)$	$-\infty$	↗	3	↘	-5	↗	$+\infty$

x	$-\infty$		$-\sqrt[4]{2}$		$\sqrt[4]{2}$		$+\infty$
$Q'(x)$		$+$	0	$-$	0	$+$	
$Q(x)$	$-\infty$	↗	$5+8\sqrt[4]{2}$	↘	$5-8\sqrt[4]{2}$	↗	$+\infty$

Exemple Le polynôme $P=3X^7-7X^6-7X^3+21X^2-7$ n'est pas résoluble par radicaux.

Démonstration On suit la piste de l'exemple précédent. Après calcul : $P'=21(X+1)X(X-1)(X-2)\big(X^2+1\big)$.

x	$-\infty$		-1		0		1		2		$+\infty$
$P'(x)$		$+$	0	$-$	0	$+$	0	$-$	0	$+$	
$P(x)$	$-\infty$	↗	11	↘	-7	↗	3	↘	-43	↗	$+\infty$

Exemple Le polynôme $P = X^7 - 3X^5 - X^2 + 3X + 1$ n'est pas résoluble par radicaux.

Démonstration

- Le critère d'Eisenstein, cette fois, n'apporte rien, mais nous allons raisonner modulo 2 et montrer que la réduction de P dans $\mathbb{F}_2[X]$, à savoir $X^7+X^5+X^2+X+1$, est irréductible sur $\mathbb{F}_2$. Cela montrera bien d'après **1.2.6** que P est irréductible sur $\mathbb{Q}$. Pour commencer, $X^7+X^5+X^2+X+1$ n'a pas de racine dans $\mathbb{F}_2$. Si ce polynôme est réductible sur $\mathbb{F}_2$, il possède donc un diviseur irréductible de degré 2 ou 3, i.e. un diviseur de degré 2 ou 3 sans racine d'après **1.1.1**.

  — Or qui sont les polynômes de degré 2 de $\mathbb{F}_2[X]$? Ce sont : X^2, X^2+1, X^2+X et X^2+X+1, et seul le dernier n'a pas de racine dans $\mathbb{F}_2$, i.e. est irréductible sur $\mathbb{F}_2$.

  — Quant aux polynômes de degré 3, ce sont : X^3, X^3+1, X^3+X, X^3+X+1, X^3+X^2, X^3+X^2+1, X^3+X^2+X et X^3+X^2+X+1, dont deux seulement sont irréductibles : X^3+X+1 et X^3+X^2+1.

  Il reste à remarquer qu'aucun des trois polynômes irréductibles trouvés ne divise $X^7+X^5+X^2+X+1$. Or un simple calcul de divisions euclidiennes montre que :

$$X^7+X^5+X^2+X+1 = \big(X^2+X+1\big)\big(X^5+X^4+X^3+X\big)+1 = \big(X^3+X+1\big)\big(X^4+X\big)+1 = \big(X^3+X^2+1\big)\big(X^4+X^3+X\big)+X^2+1.$$

- Irréductible sur $\mathbb{Q}$, P est racines simples dans $\mathbb{C}$ d'après **1.1.2**. Grâce à **8.1.5**, il nous reste donc à montrer que P possède exactement 5 racines réelles. Or :

$$P' = 7X^6 - 15X^4 - 2X + 3, \qquad P'' = 42X^5 - 60X^3 - 2 \qquad \text{et} \qquad P''' = 210X^4 - 180 = 30\big(7X^4 - 6\big),$$

  donc P''' possède exactement 2 racines réelles. D'après le théorème de Rolle, P'' en possède donc au plus 3, puis P' au plus 4, et enfin P au plus 5.
  On observe alors que : $P(-2) = -41$, $P\left(-\frac{4}{3}\right) = \frac{815}{2187}$, $P(-1) = -1$, $P(0) = 1$, $P\left(\frac{3}{2}\right) = -\frac{313}{128}$ et $P(2) = 35$. D'après le théorème des valeurs intermédiaires, P possède donc au moins 5 racines réelles — bref, exactement 5.