THÈSE

pour l'obtention du Grade de
Docteur de l'Université de Poitiers
(Faculté des Sciences Fondamentales et Appliquées)
(Diplôme National - Arrêté du 30 Mars 1992)

Spécialité : Mathématiques

Présentée par :

Lionel DUCOS

-=-

Effectivité en théorie de Galois. Sous-résultants.

-=-

Directeur de thèse : **Claude QUITTÉ**

-=-

Soutenue le vendredi 28 novembre 1997

devant la commission d'examen

-=-

JURY

M. Raïs,	Professeur de l'Université de Poitiers	Président
J.-M. Arnaudiès,	Maître de Conférences de l'Université P. et M. Curie	Examinateur
D. Lazard,	Professeur de l'Université de Paris VI	”
C. Quitté,	Maître de Conférences de l'Université de Poitiers	”
M.-F. Roy,	Professeur de l'Université de Rennes I	”
A. Valibouze,	Professeur de l'Institut B. Pascal	”
A. C. Movahhedi,	Maître de Conférences Habilité de l'Université de Limoges	Rapporteur
M. Olivier,	Professeur de l'Université de Bordeaux I	”

Évariste Galois (1811-1832)
à l'âge de 15 ans.

Remerciements

Je tiens à témoigner toute ma gratitude aux différents responsables du Laboratoire de Mathématiques de l'Université de Poitiers qui m'ont permis de préparer cette thèse dans les meilleures conditions. Je pense également à de nombreuses personnes du Département qui m'ont aidé pendant ces trois années, notamment Patrice Naudin à qui je dois mon environnement informatique et divers conseils de "wizard" en TEX et en algorithmique.

Je souhaite remercier les membres du jury d'avoir bien voulu faire partie de la commission d'examen, en particulier Mustapha Raïs d'en être le président. Michel Olivier et A. Chazad Movahhedi ont eu la gentillesse d'accepter la tâche d'être rapporteurs. Je leur en suis reconnaissant.

Merci à Jean-Marie Arnaudiès d'avoir relu très attentivement ce document. Ses suggestions concernant entre autres la résolubilité par radicaux m'ont éclairé sur certains points sensibles.

Mes pensées vont par ailleurs aux gens du groupe de travail Projet Galois du GDR Médicis, ainsi qu'à Marie-Françoise Roy et Henri Lombardi avec qui j'ai eu de nombreuses et fructueuses conversations concernant les sous-résultants.

Je n'oublie pas mes camarades de bureau et principalement Emmanuel Hallouin : ayant la même formation doctorale que lui, je le considère comme "un frère scientifique" avec qui j'échange quotidiennement idées et remarques.

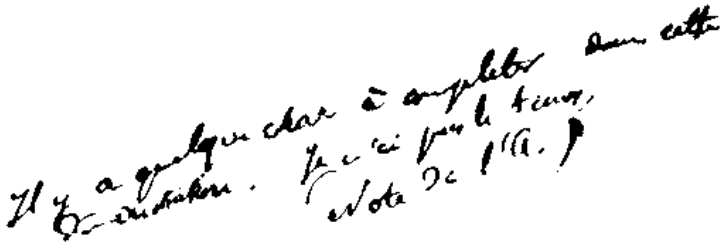
Enfin et surtout, j'adresse mes plus profonds et sincères remerciements à celui qui a guidé mes premiers pas dans la recherche en mathématiques, mon directeur de thèse, Claude Quitté. Son enthousiasme et sa générosité, qui n'ont d'égal que sa compétence, m'ont motivé à tout instant et je lui suis très redevable de m'avoir transmis une partie de son savoir.

Évariste Galois représenté
de mémoire par son frère Alfred.

A mes parents

Évariste Galois à l'âge de 17 ans.
Portrait posthume par David Johnson.

Sommaire



Introduction

[¡¡ Si maintenant] vous me donnez une équation que vous aurez choisie à votre gré et que vous désiriez connaître si elle est ou non soluble par radicaux, je n'aurai rien à y faire que de vous indiquer le moyen de répondre à votre question, sans vouloir charger ni moi ni personne de le faire. En un mot, les calculs sont impraticables.¿¿[1]

Ce célèbre paragraphe de Galois résume à la fois sa confiance en sa théorie avant-gardiste (car excessivement abstraite pour son époque) et sa lucidité vis-à-vis des calculs qu'elle engendrait. Depuis le développement des mathématiques effectives, peut-on dire que la théorie de Galois connaît un nouvel élan ? L'avènement de l'ordinateur nous donne en effet la possibilité de repousser les limites de ce qui est calculable raisonnablement. Parmi les problèmes "concrets" à résoudre en théorie de Galois, figurent au moins les trois suivants :

1. La détermination du groupe de Galois d'un polynôme ;
2. La résolubilité par radicaux des équations polynomiales ;
3. Le problème de Galois inverse effectif, c'est-à-dire la construction d'un polynôme f de $K[X]$ de groupe de Galois G où le corps K et le groupe G sont fixés à l'avance.

La première partie de cette thèse suit ces trois axes. En revanche, la seconde partie est une révision du calcul du résultant de deux polynômes à une indéterminée. Rappelons que le résultant est une fonction de base dans le calcul formel...

$\star$

Les deux premiers chapitres de ce document concernent la recherche du groupe de Galois d'un polynôme donné. Mais qu'entend-on par identifier le groupe de Galois d'un polynôme ? Plusieurs réponses peuvent être données. Adoptons les notations suivantes : K est un corps, f un polynôme unitaire (séparable) de $K[X]$, E le corps de décomposition de f sur K (à isomorphisme près).

La première manière de calculer le groupe de Galois de f, la plus répandue, est celle-ci : déterminer la représentation dans le groupe symétrique $\mathcal{S}_n$ de l'action du groupe $\mathrm{Aut}_K E$ sur les racines de f après les avoir numérotées de 1 à n. La difficulté ici est plus grande que celle de la "simple" détermination de la *classe d'isomorphie* du groupe de Galois : en effet, deux polynômes de même degré peuvent avoir des corps de décomposition identiques

[1] Citation d'Évariste Galois tirée du Discours préliminaire destiné à être placé en tête de son Mémoire sur la théorie des équations, rédigé en septembre 1830. [32] [63]

(donc le même groupe de Galois abstrait G), mais des actions de G sur leurs racines non isomorphes. Les problèmes que pose ce premier "challenge" sont déjà conséquents si l'on veut obtenir des algorithmes efficaces (voir par exemple les travaux de J.-M. Arnaudiès et A. Valibouze dans [61], ou la thèse de Y. Eichenlaub [31], ou encore [29]).

La deuxième façon d'envisager le calcul du groupe de Galois est toujours de déterminer l'action de $\mathrm{Aut}_K E$ sur les racines de f mais aussi de rendre effective l'égalité théorique

$$E^{\mathrm{Aut}_K E} = K.$$

Par rendre effective cette égalité, nous entendons qu'il faut être capable de trouver la valeur dans K d'une expression en les racines de f invariante par $\mathrm{Aut}_K E$. C'est un sujet sur lequel a choisi de travailler A. Colin dans sa thèse [18]. Cette égalité est une condition *sine qua non* pour faire du calcul relatif.

Enfin, pour nous, connaître le groupe de Galois de f, c'est discerner l'action de $\mathrm{Aut}_K E$ sur les racines de f et être capable de **calculer dans** E, autrement dit de pouvoir manipuler des expressions polynomiales en les racines de f (la première des manipulations étant le test d'égalité...). Ce problème est équivalent à trouver un idéal maximal de $K[X_1, \ldots, X_n]$ contenant les polynômes $\sigma_i - a_i$ où

$$f = X^n - a_1 X^{n-1} + a_2 X^{n-2} - \cdots + (-1)^n a_n$$

et σ_i désigne le i-ième polynôme symétrique élémentaire homogène de degré i en les indéterminées $X_1, \ldots, X_n$. Pour essayer de résoudre ce problème, notre outil mathématique (et informatique) est l'algèbre de décomposition universelle du polynôme f sur le corps K :

$$\mathbb{D}_K^f = \frac{K[X_1, \ldots, X_n]}{\langle \sigma_1 - a_1, \ldots, \sigma_n - a_n \rangle}$$

Lorsque f est séparable, cette algèbre est galoisienne sur K de groupe $\mathcal{S}_n$ (groupe symétrique). Notre but est de construire un idéal maximal $\mathfrak{m}$ de l'algèbre de décomposition universelle, en précisant un système de générateurs ou une base de Gröbner. Le quotient $\mathbb{D}_K^f/\mathfrak{m}$ est le corps de décomposition de f et le stabilisateur de $\mathfrak{m}$ dans $\mathcal{S}_n$ son groupe de Galois.

Le chapitre I est une introduction aux algèbres galoisiennes. Son rôle est d'asseoir un certain nombre de propriétés permettant d'assurer un cadre mathématique suffisant pour appréhender l'algèbre de décomposition universelle et ses sous-algèbres (étudiées dans le chapitre II). Il s'avère que la quasi-totalité des propriétés essentielles de l'algèbre de décomposition universelle provient de la théorie générale des algèbres galoisiennes.

La naissance de la théorie de Galois est due aux problèmes insolubles qu'ont rencontrés les mathématiciens pour résoudre les équations polynomiales de degré 5. Mis à part la détermination du corps de décomposition et du groupe de Galois d'un polynôme, l'algèbre de décomposition universelle permet également d'illustrer la résolubilité par radicaux : le chapitre III retrace des méthodes explicites pour calculer par radicaux les racines d'un polynôme de degré 3,4, ou 5 lorsque ceci est possible.

$\star$

Le problème inverse de la théorie de Galois est avant tout un problème théorique. La question peut être formulée ainsi : étant donné un corps K, quels sont les groupes finis pouvant être réalisés comme groupe de Galois sur K ? Pour certaines catégories de corps les réponses sont déjà connues (voir [22]) : tous les groupes finis sont réalisables sur les corps des fractions rationnelles $\mathbb{C}(t)$ (Riemann), $\mathbb{R}(t)$ (Hurwitz) et $\mathbb{Q}_p(t)$ (Harbater) ; sur les corps finis, seuls les groupes cycliques peuvent être des groupes de Galois ; un théorème (non constructif !) de Shafarevich prouve que tout groupe fini résoluble est réalisable sur $\mathbb{Q}$, mais la question reste ouverte pour la plupart des groupes sur $\mathbb{Q}$ ou $\mathbb{Q}(t)$.

Là encore, différents problèmes de difficulté croissante sont abordés dans la littérature. Le premier d'entre eux est la construction explicite d'une extension galoisienne (ou d'un polynôme) sur un corps donné dont le groupe de Galois est précisé à l'avance. La théorie de Kummer rend possible la construction sur $\mathbb{Q}$ ou $\mathbb{Q}(t)$ des produits semi-directs à noyau abélien $A \rtimes G$, si toutefois le groupe G est déjà réalisé (voir [31]).

Un deuxième obstacle dans le problème inverse consiste à **réaliser régulièrement** les groupes finis, c'est-à-dire construire, sur un corps des fractions rationnelles $k(t_1, \ldots, t_d)$, une extension galoisienne, régulière sur k (ou un polynôme régulier sur k) dont le groupe de Galois G sur $k(t_1, \ldots, t_d)$ est fixé à l'avance. Une extension $E/\mathbb{Q}$ est régulière si $E \cap \overline{\mathbb{Q}} = \mathbb{Q}$. L'existence d'extensions galoisiennes de $\mathbb{Q}(t)$ régulières sur $\mathbb{Q}$ est prouvée pour tous les groupes abéliens, les groupes symétriques $\mathcal{S}_n$ et alternés $\mathcal{A}_n$, les 26 groupes sporadiques... La théorie de la rigidité aborde ce problème en supposant que le centre du groupe G est trivial (voir [53], [54], [64]). Elle permet à cet égard de réaliser de façon régulière quelques groupes sur $\mathbb{Q}(t)$, certains groupes simples par exemple (voir [43]). Les "méthodes rigides" ont pour but de faire descendre sur $\mathbb{Q}(t)$ une réalisation d'un groupe G faite sur $\mathbb{C}(t)$.

Nous nous pencherons sur un tout petit aspect du problème inverse de Galois. Dans le chapitre IV, nous verrons comment la théorie de Kummer et la ramification dans les corps de fonctions sur $\mathbb{Q}(t)$ permettent de réaliser régulièrement tout produit semi-direct à noyau abélien $A \rtimes G$, si toutefois G est déjà réalisé régulièrement sur $\mathbb{Q}(t)$. Par ailleurs, nous conjuguerons les méthodes de Dentzer et de Volklein (voir [24], et [64] pages 236-237) avec la théorie de Kummer afin de réaliser régulièrement, dans le corps des séries formelles $k((t))$, tous les groupes abéliens d'exposant étranger à la caractéristique du corps k.

La difficulté "suprême" dans le problème de Galois inverse est la réalisation générique ou universelle des groupes finis (voir [50] ou [55]). Sans donner la définition précise d'un polynôme universel (voir [35]), en voici un réalisant le groupe alterné $\mathcal{A}_3$ sur $\mathbb{Q}(t)$:

$$f_t(X) = X^3 - tX^2 - (3+t)X - 1$$

L'une des propriétés de f_t est celle-ci : si E/K est une extension galoisienne de groupe $\mathcal{A}_3$ de caractéristique distincte de 2, alors il existe $t_0 \in K$ tel que E est le corps de décomposition de f_{t_0}. En clair, avec ce polynôme, nous "possédons" toutes les extensions galoisiennes de groupe $\mathcal{A}_3$ de caractéristique distincte de 2... D'autre part, il y est démontré que certains groupes, comme le groupe cyclique d'ordre 8 (H. Lenstra), ne sont malheureusement pas réalisables génériquement sur $\mathbb{Q}$.

$\star$

La deuxième partie de ce travail (i.e. les chapitres A et B), totalement indépendante de la théorie de Galois, aborde l'élimination "à la Bareiss" et les polynômes sous-résultants. Les quelques pages du chapitre A ont pour objectif de donner naissance de façon assez naturelle à un certain formalisme provenant de l'algèbre extérieure. Celui-ci permet de redémontrer les identités de Sylvester et l'algorithme de Bareiss. Son but est également de faire le lien entre les algorithmes de Bareiss et des sous-résultants, bien que les objets manipulés par ces deux algorithmes soient totalement différents.

Le chapitre B est consacré à l'étude des polynômes sous-résultants. Le formalisme très particulier développé dans le chapitre A apporte de nouvelles relations de divisibilité euclidienne entre les sous-résultants et des polynômes quelconques de $R[X]$ (R est un anneau commutatif intègre). L'énorme avantage de ce formalisme est de pouvoir démontrer quasiment toutes les formules existantes dans la littérature classique, et ce de **manière systématique** : un ou deux théorèmes abstraits (mais élémentaires) d'algèbre extérieure suffisent pour donner lieu à toute une panoplie de relations de similarité ou de divisibilité (voir [27] ou [28]). Cette recherche sur de nouvelles relations est motivée par l'espoir de pouvoir appliquer la "philosophie" de l'algorithme de Bareiss à celui des sous-résultants. Réaliser cet espoir donnerait-il lieu à une méthode de calcul des sous-résultants plus efficace que l'algorithme des sous-résultants lui-même ? L'algorithme auquel nous conduisent ces nouvelles relations de divisibilité du chapitre B laisse à penser que la réponse est oui.

$\star$

Chapitre I

Algèbres galoisiennes

C'est à partir de 1960 que sont apparus les premiers travaux traitant la théorie de Galois sur les anneaux commutatifs (voir [6]). Dans cette théorie, il est parfois utile de supposer que l'algèbre galoisienne ne contient pas d'idempotent autre que 0 et 1. C'est ce que font F. DeMeyer et E. Ingraham dans [23] pour généraliser, par exemple, le théorème de la correspondance galoisienne. Il est tout de même possible de se passer d'une telle hypothèse (voir [16]), mais malheureusement les énoncés des résultats se compliquent.

Dans ce chapitre, il n'est pas question de généraliser un résultat déjà établi. Il s'agit plutôt d'une introduction aux algèbres galoisiennes, notre but étant de "préparer le terrain" pour l'étude de l'algèbre de décomposition universelle d'un polynôme séparable (chapitre II). Dans un premier temps, le discours restera très général et très simple, sans hypothèse particulière. Puis nous nous intéresserons aux algèbres galoisiennes dont l'anneau de base est intégralement clos, voire un corps. En revanche, nous ne supposerons jamais que les seuls idempotents de l'algèbre galoisienne sont 0 et 1 : en effet, si l'algèbre de décomposition universelle d'un polynôme séparable sur un corps vérifie cette hypothèse, elle est obligatoirement un corps (galoisien au sens classique), ce qui atténue sensiblement l'intérêt d'une étude préliminaire des algèbres galoisiennes.

I.1 Définitions

I.1.a Une première définition

Théorème I.1.1 (voir [10], pages 40-44) *Soit A un anneau commutatif, G un groupe fini opérant sur A, R l'anneau des invariants sous l'action de G. Alors*

1. *A est entier sur R.*
2. *G opère transitivement sur les idéaux premiers de A au-dessus d'un même idéal premier de R. Autrement dit, si $\mathfrak{p}'$ et $\mathfrak{q}'$ sont deux idéaux premiers de A tel que $\mathfrak{p}' \cap R = \mathfrak{q}' \cap R$, alors $G.\mathfrak{p}' = G.\mathfrak{q}'$.*
3. *Soit $\mathfrak{p}'$ un idéal premier de A, $\mathfrak{p} = R \cap \mathfrak{p}'$ idéal premier de R, k le corps des fractions de $R/\mathfrak{p}$ et k' celui de $A/\mathfrak{p}'$. Alors k' est une extension normale de k et le morphisme*

canonique de $D(\mathfrak{p}') = \mathrm{Stab}_G \mathfrak{p}' = \{g \in G \mid g\mathfrak{p}' = \mathfrak{p}'\}$ *dans le groupe* $\mathrm{Aut}_k k'$ *est surjectif* [...]

Rappel. Une extension algébrique normale est une extension k' d'un corps k qui vérifie la propriété suivante : si un polynôme irréductible à coefficients dans k possède une racine dans k', alors celui-ci se décompose totalement dans k'.

On voit alors qu'à elle seule l'hypothèse $R = A^G$ implique beaucoup d'autres propriétés : conjugaison des idéaux premiers, normalité de l'extension k' sur k, surjectivité du morphisme canonique $D(\mathfrak{p}') \to \mathrm{Aut}_k k'$...

Dans le cas où A est déjà un corps (i.e. $A = k'$), nous obtenons la propriété suivante, laquelle peut être démontrée simplement.

Propriété I.1.1 *Soit k' un corps, G un groupe fini opérant fidèlement sur k', k le corps des invariants sous l'action de G. Alors k' est une extension normale séparable de k.*

De plus, on a nécessairement $G \simeq \mathrm{Aut}_k k'$ et $\dim_k k' = |G|$. Autrement dit, k' est une extension galoisienne de k.

Rappel. Une extension d'un corps k est séparable si celle-ci est algébrique sur k et le polynôme minimal de chacun de ses éléments est à racines simples (polynôme minimal séparable).

Nous ne donnons pas ici une preuve complète de cette proposition classique mais seulement une trame pour la démontrer. La première partie du résultat vient grâce au polynôme $P = \prod_{y \in G.x}(T - y)$ où $x \in k'$. Ce polynôme (à coefficients dans k) est très particulier : il est appelé **résolvante** de l'élément x (voir page 32).

La deuxième moitié du résultat peut être vue comme une conséquence du théorème de l'élément primitif et du fait que les éléments de k' sont de degré moindre que $|G|$. On peut aussi démontrer cela grâce à un raisonnement plus galoisien introduit par Artin (voir [5] pages 41-43).

Ainsi les extensions galoisiennes de corps se "résument" à la situation suivante :

$$k = k'^G \xrightarrow{G} k'$$

où $G = \mathrm{Aut}_k k'$ est un groupe fini.

Ceci nous amène à une généralisation des extensions galoisiennes :

Définition I.1.1 *Soit A un anneau commutatif, G un groupe fini opérant sur A, et R le sous-anneau des points fixes. On dira que A est une R-**algèbre galoisienne de groupe** G si quel que soit l'idéal maximal $\mathfrak{p}'$ de A, $\mathfrak{p} = R \cap \mathfrak{p}'$ sa trace sur A, $k = R/\mathfrak{p}$ et $k' = A/\mathfrak{p}'$ les corps résiduels, le morphisme canonique de*

$$D(\mathfrak{p}') = \mathrm{Stab}_G \mathfrak{p}' = \{g \in G \mid g\mathfrak{p}' = \mathfrak{p}'\}$$

dans le groupe $\mathrm{Aut}_k k'$ est bijectif.

*Le groupe $D(\mathfrak{p}')$ est appelé **groupe de décomposition** de l'idéal $\mathfrak{p}'$.*

Remarque. Il est absolument indispensable de spécifier le groupe G pour lequel une algèbre est galoisienne. En effet, plusieurs groupes peuvent convenir, si bien qu'il y a un certain flou si l'on ne précise pas G. Par exemple, si k est un corps, k^n est une algèbre galoisienne sur k pour tout sous-groupe transitif de $\mathcal{S}_n$ d'ordre n (voir la section I.2). Ces groupes opèrent sur k^n par permutations des coordonnées et s'injectent ainsi dans $\mathrm{Aut}_k\, k^n$.

Dans la théorie des extensions galoisiennes classique, on ne précise pas le groupe G, car, comme nous l'avons vu, il s'agit obligatoirement du groupe des automorphismes ($G = \mathrm{Aut}_k\, k'$).

Nous verrons page 19 que si une algèbre galoisienne de groupe G est libre (comme k^n sur k), nécessairement le groupe G est de cardinal le rang de l'algèbre (dans notre exemple, $|G| = n$). Ceci rend par exemple impossible que k^n soit une k-algèbre de groupe $\mathrm{Aut}_k\, k^n$, car ce dernier est isomorphe à $\mathcal{S}_n$ de cardinal $n!$.

Propriété I.1.2 *Si A est une R-algèbre galoisienne de groupe G, alors G opère fidèlement sur A. Autrement dit, G s'injecte dans $\mathrm{Aut}_R\, A$.*

Démonstration Si G n'opère pas fidèlement sur A alors, quel que soit l'idéal maximal $\mathfrak{p}'$, le morphisme canonique $D(\mathfrak{p}') \twoheadrightarrow \mathrm{Aut}_k\, k'$ est non injectif :

$$\forall\, x \in A \quad g.x = x \qquad \text{implique} \qquad \forall\, x \in A \quad g.x \equiv x \mod \mathfrak{p}'. \qquad \square$$

Propriété I.1.3 *En reprenant les notations de la définition I.1.1, quel que soit l'idéal maximal $\mathfrak{p}'$ de A, le corps $k' = A/\mathfrak{p}'$ est une extension galoisienne de $k = R/(\mathfrak{p}' \cap R)$ de groupe de Galois $D(\mathfrak{p}')$.*

Remarque. Nous verrons que cette propriété est également vraie si $\mathfrak{p}'$ est seulement un idéal premier de A, en posant $k' = \mathrm{Frac}(A/\mathfrak{p}')$ et $k = \mathrm{Frac}(R/\mathfrak{p}' \cap R)$ (corollaire I.4.2, page 26).

Démonstration Il suffit de montrer que ${k'}^{\Gamma} = k$ où nous posons $\Gamma = \mathrm{Aut}_k\, k'$ pour alléger les notations. Comme les automorphismes de k' sont linéairement indépendants sur k' (théorème de Dedekind, voir [14] page 27), leur somme $\sum_{\overline{g}\in\Gamma} \overline{g}$ n'est pas identiquement nulle. Il existe par conséquent un élément $\overline{c} \in k'$ tel que

$$\sum_{\overline{g}\in\Gamma} \overline{g}(\overline{c}) = 1$$

A présent, considérons un élément $\overline{x} \in {k'}^{\Gamma}$ et montrons qu'il appartient en fait à k. Choisissons de remonter $\overline{x}$ en un élément $x \in A$ qui appartient à tous les conjugués de $\mathfrak{p}'$ sauf peut-être $\mathfrak{p}'$: ceci est possible en vertu du théorème chinois $\prod_{\mathfrak{q}'\in G.\mathfrak{p}'} A/\mathfrak{q}' \simeq A/\cap G.\mathfrak{p}'$. Nous obtenons ainsi un élément $x \in A$ vérifiant

$$\begin{array}{cc} \forall\, g \in G \setminus D(\mathfrak{p}') & g(x) \in \mathfrak{p}' \\ \forall\, g \in D(\mathfrak{p}') & g(x) - x \in \mathfrak{p}' \end{array}$$

En multipliant chaque ligne par $g(c)$ et en les sommant toutes, on obtient finalement

$$\sum_{g\in G} g(x)g(c) - x. \sum_{g\in D(\mathfrak{p}')} g(c) \in \mathfrak{p}'$$

Or $\sum_{g\in G} g(x)g(c)$ est invariant par G, appartient donc à R. Par hypothèse sur c, la quantité $\sum_{g\in D(\mathfrak{p}')} g(c)$ est congrue à 1 modulo $\mathfrak{p}'$ car

$$\sum_{g\in D(\mathfrak{p}')} \overline{g(c)} = \frac{|D(\mathfrak{p}')|}{|\Gamma|} \sum_{\overline{g}\in\Gamma} \overline{g}(\overline{c}) = \sum_{\overline{g}\in\Gamma} \overline{g}(\overline{c})$$

Ainsi nous avons prouvé que x est congru à un élément de R modulo $\mathfrak{p}'$, ce qui prouve bien que $\overline{x}$ appartient à k. □

Remarque. Cette démonstration reste valable même dans le cas où le morphisme canonique $D(\mathfrak{p}') \twoheadrightarrow \mathrm{Aut}_k\, k'$ est non injectif, à condition que le cardinal de son noyau (portant le nom de **groupe d'inertie**) soit inversible dans k, c'est-à-dire premier avec la caractéristique de k.

Dans [10] (pages 48-49), Bourbaki démontre un résultat beaucoup plus général : on suppose seulement $A^G = R$ (cadre du théorème I.1.1), pour un idéal maximal (voire premier) $\mathfrak{p}' \subset A$ fixé, on note I le noyau du morphisme canonique $D(\mathfrak{p}') \twoheadrightarrow \mathrm{Aut}_k\, k'$. Alors $\mathrm{Frac}\left(A^I/(\mathfrak{p}' \cap A^I)\right)$ est la plus grande extension séparable de k' dans k.

I.1.b Autres définitions équivalentes

On peut reformuler la définition I.1.1 ci-dessus par :

Définition I.1.2 *Soit A un anneau commutatif, G un groupe fini opérant sur A, et R le sous-anneau des points fixes. On dira que A est une R-**algèbre galoisienne de groupe** G si quel que soit $\mathfrak{p}'$ idéal maximal de A et quel que soit $g \in G$, $g \neq 1_G$, il existe au moins un $x \in A$ tel que $g(x) - x \notin \mathfrak{p}'$.*

Remarquer qu'il suffit de considérer les éléments $g \in D(\mathfrak{p}') = \mathrm{Stab}_G(\mathfrak{p}')$.

Il apparaît une propriété importante, toujours dans le cas où $A = k'$ est une extension (de corps) galoisienne de $R = k$. En effet, posons $G = \mathrm{Aut}_k\, k'$ et considérons le morphisme de k'-algèbres

$$\begin{array}{rccc} l & : & k' \otimes_k k' & \longrightarrow & \prod_G k' \\ & & a \otimes b & \longmapsto & (a.g(b))_{g\in G} \end{array}$$

Ce morphisme est en fait bijectif : il suffit pour le prouver de montrer qu'il est surjectif car les dimensions des k'-algèbres $k' \otimes_k k'$ et $\prod_G k'$ sont toutes les deux égales à la dimension de l'extension k'/k, c'est-à-dire $|G|$.

Démonstration Soit x un élément primitif de k' sur k (théorème de l'élément primitif). Alors $1 \otimes x$ est un élément primitif de $k' \otimes_k k'$ sur k' et son image par le morphisme l est un vecteur dont toutes les composantes sont distinctes : $(g(x))_{g\in G}$ (x est un élément primitif de k'/k donc tous ses conjugués sont distincts). Or un vecteur de $\prod_G k'$ dont toutes les coordonnées sont distinctes est un élément primitif. Ainsi l est un morphisme d'algèbres surjectif, et par suite bijectif. □

Considérons maintenant un anneau A sur lequel opère un groupe fini G. Soit R le sous-anneau des points fixes. Supposons que le morphisme de A-algèbres

$$\begin{array}{rccc} l & : & A \otimes_R A & \longrightarrow & \prod_G A \\ & & a \otimes b & \longmapsto & (a.g(b))_{g\in G} \end{array}$$

soit en fait un isomorphisme. Montrons alors que A est une algèbre galoisienne de R de groupe G, c'est-à-dire que le morphisme canonique $D(\mathfrak{p}') = \{g \in G \mid g\mathfrak{p}' = \mathfrak{p}'\} \twoheadrightarrow \mathrm{Aut}_k\, k'$ est injectif (il est toujours surjectif car $R = A^G$, voir théorème I.1.1).

Démonstration Montrons que le noyau du morphisme canonique $D(\mathfrak{p}') \twoheadrightarrow \mathrm{Aut}_k\, k'$ est réduit à $\{1\}$. Soit $\sigma \in D(\mathfrak{p}')$ tel que $\sigma(z) - z \in \mathfrak{p}'$ quel que soit $z \in A$.

Soit $v \in \prod_G A$ dont toutes les composantes sont nulles sauf celle en 1_G qui vaut 1. Notons $\sum_i x_i \otimes y_i$ son antécédent par l. Ceci revient simplement à dire que

$$v = l(\sum_i x_i \otimes y_i) = \left(\sum_i x_i g(y_i)\right)_{g\in G}$$

ou encore $\sum_i x_i y_i = 1$ et $\sum_i x_i g(y_i) = 0$ pour $g \neq 1_G$.

Ainsi, par hypothèse sur σ,

$$\mathfrak{p}' \ni \sum x_i(\sigma(y_i) - y_i) = \sum x_i\sigma(y_i) - 1$$

Comme -1 n'appartient pas à $\mathfrak{p}'$, la somme $\sum x_i\sigma(y_i)$ ne peut pas être nulle. La seule possibilité restante est $\sum_i x_i\sigma(y_i)$=1, i.e. $\sigma = 1_G$. Le morphisme canonique est bien injectif. Par suite, A est galoisienne. □

En fait, il est prouvé dans [16] et [23] (pages 81-84) la réciproque du résultat que l'on vient d'établir, à savoir :

Théorème I.1.2 *Soit un anneau commutatif A sur lequel opère un groupe fini G. Soit R le sous-anneau des points fixes. Alors il y a équivalence entre les assertions suivantes :*

1. *Le morphisme $A\otimes_R A \to \prod_G A$ défini par $a\otimes b \mapsto (a.g(b))_{g\in G}$ est un G-isomorphisme de A-algèbres.*

2. *Il existe des éléments $x_1, \ldots, x_n, y_1, \ldots, y_n$ dans A tels que*

$$\forall\ g \in G \qquad \sum_i x_i g(y_i) = \delta_{g,1_G}$$

   Remarque. Dans ces conditions, nous avons aussi $\sum_i h(x_i)y_i = \delta_{h,1_G}$ pour tout $h \in G$ en posant $h = g^{-1}$. Autrement dit, les familles $\{x_i\}_i$ et $\{y_i\}_i$ ont des rôles identiques dans cette propriété.

3. *A est une algèbre galoisienne sur R de groupe G.*

Corollaire I.1.1 *Une algèbre galoisienne est un module projectif de type fini de rang constant $|G|$ sur son sous-anneau des points fixes.*

Démonstration En reprenant l'assertion *2* du théorème précédent, on remarque que l'on a

$$\sum_i \big(\sum_{g\in G} g(zy_i)\big)x_i = \sum_{g\in G}\sum_i g(y_i)x_i\ g(z) = \sum_{g\in G} g(z)\delta_{g,1_G} = z$$

et ce quel que soit $z \in A$. Comme $\sum_g g(zy_i)$ appartient à R car invariant par G, on en déduit que $A = \sum_i Rx_i$.

Cette relation $z = \sum_i \big(\sum_g g(zy_i)\big)x_i$ montre en outre que A est un module projectif car les formes linéaires $z \mapsto \sum_g g(zy_i)$ et les éléments x_i forment un "système de coordonnées" pour A sur R.

De plus, grâce à l'assertion *1* du théorème précédent, nous avons $A \otimes_R A \simeq \prod_G A$. Soit $\mathfrak{m}$ un idéal maximal de R et S la partie multiplicative $R \setminus \mathfrak{m}$. On note $R_\mathfrak{m}$ le localisé de R par S, $A_\mathfrak{m}$ le localisé de A par S. Nous obtenons toujours un isomorphisme

$$A_\mathfrak{m} \otimes_{R_\mathfrak{m}} A_\mathfrak{m} \simeq \prod_G A_\mathfrak{m}$$

(Nous verrons page 26 que $A_\mathfrak{m}$ est galoisienne sur $R_\mathfrak{m}$ de groupe G.) Or $A_\mathfrak{m}$ est un module projectif de type fini sur un anneau local, donc $A_\mathfrak{m}$ est libre : son rang est nécessairement $|G|$ car $(\dim_{R_\mathfrak{m}} A_\mathfrak{m})^2 = |G|.\dim_{R_\mathfrak{m}} A_\mathfrak{m}$. C'est en quoi A est un R-module projectif de type fini et de rang constant égal à $|G|$. □

Corollaire I.1.2 *Par exemple, une algèbre galoisienne sur un anneau principal, ou local (voire semi-local, dans [8], page 143), ou sur un anneau de polynôme $k[X_1, \ldots, X_n]$ (où k est un corps) est libre.*

Propriété I.1.4 *Soit A une algèbre galoisienne de groupe G sur un anneau R. Quel que soit le système de générateurs $\{b_i\}_{i\in I}$ du R-module A, il existe une famille $\{a_i\}_{i\in I}$ telle que $\sum_i g(a_i)b_i = \delta_{1,g}$ pour tout $g \in G$.*

Démonstration On sait qu'il existe $x_1, \ldots, x_n, y_1, \ldots, y_n$ tel que $\sum_j g(y_j)x_j = \delta_{1,g}$ pour tout $g \in G$. Par hypothèse les x_j s'exprime en fonction des b_i par $x_j = \sum_i r_{i,j}b_i$. On obtient alors

$$\sum_i g\big(\sum_j r_{i,j}y_j\big)b_i = \sum_i\sum_j r_{i,j}g(y_j)\ b_i = \sum_j\sum_i r_{i,j}b_i\ g(y_j) = \sum_j x_j g(y_j) = \delta_{1,g}$$

ce qui prouve le résultat : $a_i = \sum_j r_{i,j}y_j$. □

I.2 Exemples

• Voici un exemple on ne peut plus classique d'une algèbre galoisienne pour plusieurs groupes. Soit R un anneau commutatif, $n \in \mathbb{N}^*$ et G un sous-groupe transitif de $\mathcal{S}_n$ d'ordre n. Si l'on fait opérer G par permutation des coordonnées, $A = R^n$ est une algèbre galoisienne sur R de groupe G.

En effet, l'action de G sur la base canonique de A est transitive par le choix de G, donc A^G est l'ensemble des vecteurs dont les coordonnées sont identiques (i.e. la diagonale de R^n), que l'on identifie à R.

Enfin, un idéal maximal $\mathfrak{p}'$ de A se décompose en $n-1$ copies de R et un idéal maximal $\mathfrak{p}$ de R : par exemple $\mathfrak{p} \times R^{n-1}$, ou $R \times \mathfrak{p} \times R^{n-2}$... Alors le quotient $k' = A/\mathfrak{p}'$ est isomorphe au quotient $k = R/\mathfrak{p}$. Ainsi $\mathrm{Aut}_k\, k' = \{1\}$. Or $D(\mathfrak{p}') = \mathrm{Stab}_G\, \mathfrak{p}'$ est de cardinal $\frac{|G|}{|G.\mathfrak{p}'|} = 1$ car $\mathfrak{p}'$ possède n conjugués (G opère transitivement sur les coordonnées). Nous venons de prouver que le morphisme canonique $D(\mathfrak{p}') \twoheadrightarrow \mathrm{Aut}_k\, k'$ est bijectif, et finalement que A est une algèbre galoisienne sur R de groupe G.

On peut aussi prouver ce résultat grâce aux assertions *1* et *2* du théorème I.1.2. En effet, si l'on pose toujours $A = R^n$, $A \otimes_R A \simeq A^n \simeq \prod_G A$ où les isomorphismes et les actions canoniques de G sont compatibles. On peut également donner explicitement des éléments x_i et y_i : poser $x_i = y_i = (\delta_{i,j})_{j=1..n}$. Remarquer que ces éléments forment une base normale de A sur R.

• Soit $f \in \mathbb{Z}[T]$ un polynôme unitaire séparable de degré n, dont les racines dans $\mathbb{C}$ sont $x_1, \ldots, x_n$. On note G le groupe de Galois de f, d le discriminant de f, enfin les anneaux $R = \mathbb{Z}[d^{-1}]$ et $A = R[x_1, \ldots, x_n]$. Alors A est une R-algèbre galoisienne de groupe G.

Premièrement $A^G = R$ car les éléments de A invariants par G, appartenant donc à $\mathbb{Q}$, sont entiers sur R qui est intégralement clos.

D'autre part, soit $\mathfrak{p}'$ un idéal maximal de A, $\mathfrak{p}$ sa trace sur R, k et k' les corps finis $R/\mathfrak{p}$ et $A/\mathfrak{p}'$ respectivement. Comme le discriminant de f est inversible dans R, $\overline{f}$ reste séparable dans k', et ses racines sont $\overline{x_1}, \ldots, \overline{x_n}$. Si $g \in D(\mathfrak{p}')$ vérifie $\overline{g}(\overline{y}) = \overline{y}$ pour tout $\overline{y} \in k'$, alors $\overline{g(x_i)} = \overline{x_i}$ pour tout i. Comme $\overline{f}$ est séparable et que $g(x_i) = x_j$, nécessairement $g(x_i) = x_i$ pour tout i, et $g = \mathrm{Id}$: le morphisme $D(\mathfrak{p}') \twoheadrightarrow \mathrm{Aut}_k\, k'$ est bien injectif (et par suite bijectif).

• Soit K un corps de nombres galoisien sur $\mathbb{Q}$, $\mathcal{O}$ la fermeture intégrale de $\mathbb{Z}$ dans K, d le discriminant de $\mathcal{O}$ sur $\mathbb{Z}$, i.e. le discriminant d'une base quelconque du $\mathbb{Z}$-module $\mathcal{O}$ (seul 1 est le carré d'un inversible de $\mathbb{Z}$). Alors l'algèbre $A = \mathcal{O}[d^{-1}]$ est galoisienne sur $R = \mathbb{Z}[d^{-1}]$ de groupe $G = \mathrm{Aut}_{\mathbb{Q}}\, K$.

En effet, $A^G = \mathcal{O}[d^{-1}]^G = \mathbb{Z}[d^{-1}] = R$ car les éléments de A invariants par G, appartenant donc à $\mathbb{Q}$, sont entiers sur $\mathbb{Z}[d^{-1}]$ qui est intégralement clos.

Soit $\mathfrak{p}'$ un idéal maximal de A, $\mathfrak{p}$ sa trace sur R, k et k' les corps finis $R/\mathfrak{p}$ et $A/\mathfrak{p}'$ respectivement. Comme A est un anneau de Dedekind, $\mathfrak{p}$ se factorise dans A en produit d'idéaux premiers. Or $\mathfrak{p}$ n'est pas ramifié dans A car il ne divise pas le discriminant de A sur R (celui-ci est inversible dans R !). Ainsi le morphisme canonique $D(\mathfrak{p}') \twoheadrightarrow \mathrm{Aut}_k\, k'$ est bijectif.

> Rappel. Tout anneau d'entiers $\mathcal{O}$ d'un corps de nombres est un anneau de Dedekind. Dans un anneau de Dedekind, tout idéal non trivial se factorise en un produit fini d'idéaux premiers (maximaux) de façon unique à l'ordre près des facteurs.

Lorsqu'un nombre premier p de $\mathbb{Z}$ se factorise en produit d'idéaux premiers $\mathfrak{p}_1 \dots \mathfrak{p}_n$ dans $\mathcal{O}$, on dit qu'il est ramifié lorsqu'au moins deux idéaux $\mathfrak{p}_i$ sont égaux.

On démontre qu'un premier p de $\mathbb{Z}$ n'est pas ramifié dans $\mathcal{O}$ si et seulement si le morphisme canonique $D(\mathfrak{p}') \twoheadrightarrow \mathrm{Aut}_k\, k'$ est bijectif quel que soit l'idéal premier $\mathfrak{p}'$ de $\mathcal{O}$ au-dessus de p. (voir [51] pages 101-107).

• Soit R un anneau commutatif, $f = T^2 - sT + p \in R[T]$ un polynôme dont le discriminant $s^2 - 4p$ est inversible dans R. Considérons la R-algèbre

$$A = R[X_1, X_2]/(X_1 + X_2 - s, X_1X_2 - p)$$

Notons x_i les classes des X_i : $x_i = \overline{X_i}$. Il est facile de voir que $\{1, x_1\}$ forme une base de A sur R. Soit l'automorphisme σ de A échangeant x_1 et x_2. Cet automorphisme est d'ordre 2 car x_1 et x_2 sont distincts ($\mathrm{dis}(f) = (x_1 - x_2)^2$ est inversible).

Alors A est une algèbre galoisienne sur R de groupe $G = \{\mathrm{Id}, \sigma\}$.

En effet, $A^G = R : \sigma(ax_1 + b) = ax_1 + b$ équivaut à $2a = 0$ et $as = 0$ (utiliser les égalités $\sigma(x_1) = x_2 = s - x_1$). Mais ces deux égalités induisent à leur tour $a(s^2 - 4p) = 0$, c'est-à-dire $a = 0$ puisque $\mathrm{dis}(f) = s^2 - 4p$ est inversible.

D'autre part, si $\mathfrak{p}'$ est un idéal maximal de A et l'on suppose $\sigma(x) - x \in \mathfrak{p}'$ pour tout $x \in A$, il vient $(x_2 - x_1)^2 = (\sigma(x_1) - x_1)^2 \in \mathfrak{p}'$, ce qui est absurde car $\mathrm{dis}(f) = (x_2 - x_1)^2$ est inversible... Ainsi le morphisme canonique $D(\mathfrak{p}') \twoheadrightarrow \mathrm{Aut}_{R/R\cap\mathfrak{p}'}\, A/\mathfrak{p}'$ est obligatoirement injectif.

Remarque. L'algèbre A en question est en fait l'algèbre de décomposition universelle du polynôme f. Cette algèbre sera traitée de façon plus détaillée dans le chapitre II : par exemple, nous verrons que si le discriminant d'un polynôme unitaire f est inversible, alors son algèbre de décomposition universelle est une algèbre galoisienne libre de groupe $\mathcal{S}_n$.

I.3 La forme linéaire trace

Le corollaire I.1.1 montre qu'une R-algèbre galoisienne A de groupe G est un R-module de type fini ($A = \sum_i Rx_i$). En effet, dans sa démonstration, nous avons vu que tout élément $z \in A$ s'écrit $\sum_i r_i x_i$, où $r_i = \sum_g g(zy_i)$.

Rappel. Les x_i et les y_i ont été choisis pour la propriété suivante :

$$\forall\ g \in G, \qquad \sum_i x_i g(y_i) = \delta_{g,1}$$

Définition I.3.1 *Soit A une algèbre galoisienne sur R de groupe G. On appelle* ***trace****, et on note* tr*, la forme linéaire suivante*

$$\begin{array}{rccc} \mathrm{tr} : & A & \longrightarrow & R \\ & z & \longmapsto & \sum_{g\in G} g(z) \end{array}$$

Ainsi, on obtient de façon plus compacte :

Lemme I.3.1 *Soit A une algèbre galoisienne sur R de groupe G et $x_1, \ldots, x_n, y_1, \ldots, y_n$ des éléments de A tels que $\sum_i x_i g(y_i) = \delta_{g,1}$ pour tout $g \in G$. Alors, quel que soit $z \in A$, on a $z = \sum_i \mathrm{tr}(zy_i)x_i$.*

Propriété I.3.1 *Soit A une algèbre galoisienne sur R de groupe G. Alors $\mathrm{tr}(A) = R$.*

Démonstration L'image de tr est un idéal I de R. Comme $1 = \sum_i \mathrm{tr}(1y_i)x_i$, on voit que 1 appartient à IA : nous avons donc $IA = A$. Comme A est une algèbre entière sur R, I est nécessairement égal à R tout entier (utiliser le relèvement des idéaux premiers dans une algèbre entière). □

Corollaire I.3.1 *Soit A une algèbre galoisienne sur R de groupe G. Alors R est un facteur direct de A.*

Démonstration Soit $c \in A$ tel que $\mathrm{tr}(c) = 1$. Considérons la forme linéaire $c^* : A \to R$ définie par $c^*(z) = \mathrm{tr}(cz)$. Par exemple, $c^*(1) = 1$, $c^* \circ c^* = c^*$: en clair, c^* est un projecteur de A sur R. Alors tout élément $z \in A$ peut se décomposer de façon unique en $z = c^*(z) \oplus z - c^*(z)$. En conclusion, $A = R \oplus \ker c^*$. □

Mais on peut aller plus loin : si h est une forme linéaire, $h \in A^*$, on établit pour tout $z \in A$:

$$\mathrm{tr}\big(\sum h(x_i)y_i\ z\big) = \sum h(x_i)\,\mathrm{tr}(y_i z) = h\Big(\sum \mathrm{tr}(y_i z)x_i\Big) = h(z)$$

On voit alors qu'il existe $a \in A$ (à savoir $\sum_i h(x_i)y_i$) tel que $h(z) = \mathrm{tr}(az)$ pour tout $z \in A$.

Théorème I.3.1 *Soit A une algèbre galoisienne sur R de groupe G, $(x_i)_{i=1..n}$ et $(y_i)_{i=1..n}$ des éléments de A tels que $\sum_i x_i g(y_i) = \delta_{g,1}$. Alors les applications suivantes (réciproques l'une de l'autre)*

$$\begin{array}{rcl} A & \longleftrightarrow & A^* \\ a & \longmapsto & \mathrm{tr}(a\,\bullet) \\ \sum_i h(x_i)y_i & \longleftarrow & h \end{array}$$

réalisent des isomorphismes entre les R-modules A et A^* (le dual de A).

En particulier, la forme bilinéaire symétrique $(a, b) \in A^2 \mapsto \mathrm{tr}(ab)$ est non dégénérée.

Démonstration On a simultanément

$$\sum \mathrm{tr}(ay_i)x_i = a \qquad \text{et} \qquad \mathrm{tr}\big(\sum h(x_i)y_i\ z\big) = h(z)$$

donc les deux applications sont réciproques l'une de l'autre. □

Aparté sur la norme

Définition I.3.2 *Soit A une algèbre galoisienne de groupe G sur un anneau R. On définit la **norme** d'un élément $a \in A$ par*

$$\mathrm{N}(a) = \prod_{g \in G} g(a)$$

Il est clair que $\mathrm{N}(a)$ appartient à $R = A^G$.

Propriété I.3.2 *Un élément $a \in A$ est un diviseur de 0 dans A si et seulement si sa norme l'est dans R. Ou encore, de façon équivalente, a est un élément régulier de A si et seulement si sa norme l'est dans R.*

Démonstration Si $a \in A$ est régulier, alors tous ses conjugués $g(a)$ ($g \in G$) le sont aussi : une égalité $g(a)x = 0$ devient $ag^{-1}(x) = 0$, d'où $g^{-1}(x) = 0$, et $x = 0$. Par conséquent, la norme de a est un élément régulier de A (donc de R), car il s'agit d'un produit d'éléments réguliers.

Maintenant, si $a \in A$ est un diviseur de 0, alors il existe un élément $x \in A$ non nul tel que $ax = 0$. En multipliant cette égalité par tous les conjugués de a, $g(a)$ avec $g \in G \backslash \{\mathrm{Id}\}$, il vient $\mathrm{N}(a)x = 0$. Comme A est un module projectif sur R (i.e. un facteur direct d'un R-module libre), $\mathrm{N}(a)$ est un diviseur de 0 dans R. □

I.4 Changement d'anneau

I.4.a Sous-algèbre de points fixes

Propriété I.4.1 *Soit A une algèbre galoisienne sur un anneau R de groupe G. Quel que soit H sous-groupe de G, A est une algèbre galoisienne sur A^H de groupe H.*

Démonstration Soit les idéaux maximaux $\mathfrak{p}'$ de A, $\mathfrak{p} = \mathfrak{p}' \cap R$ de R, $\mathfrak{p}_H = \mathfrak{p}' \cap A^H$ de A^H, et leur corps résiduels respectifs $k = R/\mathfrak{p}$, $k' = A/\mathfrak{p}'$, $k_H = A^H/\mathfrak{p}_H$. Il suffit de démontrer que le morphisme canonique $D(\mathfrak{p}') \cap H \twoheadrightarrow \mathrm{Aut}_{k_H} k'$ est injectif. Or ce morphisme est le restriction du morphisme injectif $D(\mathfrak{p}') \twoheadrightarrow \mathrm{Aut}_k k'$.

On peut également prouver ce résultat en utilisant l'assertion *2* du théorème I.1.2... □

Cette dernière propriété est bien connue en théorie de Galois classique et se généralise visiblement très bien aux algèbres galoisiennes. De plus, comme on peut s'en douter, nous avons la propriété suivante :

Propriété I.4.2 *Soit A une algèbre galoisienne sur un anneau R de groupe G. Si H est un sous-groupe normal de G, alors A^H est une algèbre galoisienne sur R de groupe G/H.*

Démonstration Le groupe G/H opère sur A^H de façon canonique : $\overline{g}(x) = g(x)$. Soit un élément $x \in A^H$ invariant par G/H. Alors il est invariant par G tout entier, donc x

appartient à R. Ceci prouve que R est bien l'anneau des points fixes de A^H sous l'action de G/H.

Pour conclure la preuve, il suffit de considérer les éléments $x_i, y_i \in A$ de l'assertion *2* du théorème I.1.2 : $\sum_i x_i\sigma(y_i) = \delta_{\mathrm{Id},\sigma}$ pour tout $\sigma \in G$. Soit un élément $c \in A$ dont la trace sur A^H soit 1 (A est galoisienne sur A^H de groupe H). Posons $x'_i = \sum_{h\in H} h(x_i c)$ et $y'_i = \sum_{h\in H} h(y_i)$. Ces éléments x'_i et y'_i appartiennent bien à A^H et pour tout $\sigma \in G$

$$\sum_i x'_i\sigma(y'_i) = \sum_i \sum_{h\in H} x'_i\ \sigma h(y_i) = \sum_i \sum_{h\in H} x'_i\ h\sigma(y_i) = \sum_{h\in H} h\left(\sum_i x'_i\sigma(y_i)\right)$$

$$\sum_i x'_i\sigma(y_i) = \sum_i \sum_{h\in H} h(x_i c)\sigma(y_i) = \sum_{h\in H} h(c)\sum_i h(x_i)\sigma(y_i) = \sum_{h\in H} h(c)\delta_{h,\sigma} = \sigma(c)\delta_{\sigma\in H}$$

Si bien que $\sum_i x'_i\sigma(y'_i) = 0$ lorsque $\sigma \notin H$, et

$$\sum_i x'_i\sigma(y'_i) = \sum_{h\in H} h\sigma(c) = \mathrm{tr}_{A:A^H}(c) = 1$$

lorsque $\sigma \in H$. Les éléments $x'_i, y'_i \in A^H$ vérifient la condition *2* du théorème I.1.2 : conclusion, A^H est galoisienne sur R de groupe G/H. □

Corollaire I.4.1 *Soit A une algèbre galoisienne sur R de groupe G. Quel que soit H un sous-groupe de G, la sous-algèbre A^H est un module projectif de type fini sur R.*

Démonstration Comme A est galoisienne sur R, A est un R-module projectif de type fini (corollaire I.1.1). Nous avons démontré que A était aussi une algèbre galoisienne sur A^H : A^H est en particulier un facteur direct de A (corollaire I.3.1) : plus précisément

$$A = A^H \oplus V$$

où V est un A^H-module. Or un facteur direct d'un projectif de type fini est projectif de type fini. □

I.4.b Localisation et quotient

Propriété I.4.3 *Soit A une algèbre galoisienne sur un anneau R de groupe G. Si S est une partie multiplicative de R, alors $S^{-1}A$ est une algèbre galoisienne sur $S^{-1}R$ de groupe G.*

Démonstration Le groupe G opère canoniquement sur $S^{-1}A$: $g(a/s) = g(a)/s$ où s appartient à $S \subset R$, $a \in A$. Ainsi les points de $S^{-1}A$ invariants par G sont exactement les éléments de $(S^{-1}A)^G = S^{-1}R$. En effet $g(a/s) = a/s$ équivaut à $s'_g(sg(a) - sa) = 0$. Par suite $a/s \in (S^{-1}A)^G$ implique $g(s'sa) = s'sa$ pour tout $g \in G$ où $s' = \prod_{g\in G} s'_g$, donc $s'sa \in R$ et $a \in S^{-1}R$.

Pour finir, on utilise l'assertion *2* du théorème I.1.2 : il existe des éléments $x_i, y_i \in A$ tels que $\sum_i x_i g(y_i) = \delta_{1,g}$ pour tout $g \in G$. Alors les éléments $x_i/1$, $y_i/1$ de $S^{-1}A$ vérifient la même propriété. □

Corollaire I.4.2 *Soit A une algèbre galoisienne sur un anneau R de groupe G et $\mathfrak{p}$ un idéal premier de R. On note $R_\mathfrak{p}$ le localisé de R par $S = R \setminus \mathfrak{p}$, $A_\mathfrak{p}$ le localisé de A par S. Alors $A_\mathfrak{p}$ est une algèbre galoisienne libre sur $R_\mathfrak{p}$ de groupe G.*

Par ailleurs, quel que soit l'idéal premier $\mathfrak{p}'$ de A au-dessus de $\mathfrak{p} \subset R$, le corps des fractions $k' = \mathrm{Frac}(A/\mathfrak{p}')$ est une extension galoisienne de $k = \mathrm{Frac}(R/\mathfrak{p})$ de groupe de Galois $D(\mathfrak{p}') = \mathrm{Stab}_G(\mathfrak{p}')$.

Démonstration Seule la seconde partie du corollaire reste à prouver. Pour cela, nous allons observer l'idéal $\mathfrak{p}'A_\mathfrak{p}$: il s'agit d'un idéal maximal de $A_\mathfrak{p}$ car il est au-dessus de l'idéal maximal $\mathfrak{p}R_\mathfrak{p}$. En utilisant la définition des algèbres galoisiennes, nous savons que le quotient $A_\mathfrak{p}/\mathfrak{p}'A_\mathfrak{p}$ est une extension galoisienne de $R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$ de groupe de Galois $\mathrm{Stab}_G(\mathfrak{p}'A_\mathfrak{p}) = \mathrm{Stab}_G(\mathfrak{p}')$. Nous concluons en signalant

$$R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p} = (R \setminus \mathfrak{p})^{-1}R/\mathfrak{p} = \mathrm{Frac}(R/\mathfrak{p}) \qquad \text{et} \qquad A_\mathfrak{p}/\mathfrak{p}'A_\mathfrak{p} = (R \setminus \mathfrak{p})^{-1}A/\mathfrak{p}' = \mathrm{Frac}(A/\mathfrak{p}')$$

car $A/\mathfrak{p}'$ est une algèbre intègre et entière sur $R/\mathfrak{p}$. □

Propriété I.4.4 *Soit A une algèbre galoisienne sur un anneau R de groupe G, I un idéal propre de A et $H \subset D(I) = \{g \in G \mid g(I) = I\}$. Alors A/I est une algèbre galoisienne sur $A^H/(I \cap A^H)$ de groupe H.*

Démonstration Nous savons déjà que A est une algèbre galoisienne sur A^H de groupe H.

Prouvons pour commencer que $\overline{A^H} = A^H/(I \cap A^H)$ est l'ensemble des points fixes de $\overline{A} = A/I$ sous l'action de H. Grâce à la propriété I.3.1, il existe $c \in A$ tel que

$$\sum_{h \in H} h(c) = 1$$

car A est galoisienne sur A^H. Soit $\overline{x} \in \overline{A}^H$:

$$\overline{x} = \overline{x} \sum_{h \in H} \overline{h(c)} = \sum_{h \in H} \overline{h(x)h(c)} = \overline{\sum_{h \in H} h(xc)}$$

Or $\sum_{h \in H} h(xc)$ appartient à A^H, donc $\overline{x}$ appartient à $\overline{A^H}$.

Il est facile de finir de démontrer que $\overline{A}$ est galoisienne sur $\overline{A^H}$ (c'est-à-dire prouver l'injectivité des morphismes canoniques de la définition I.1.1) car il y a correspondance bijective entre les idéaux (maximaux) de $\overline{A}$ et ceux de A contenant I...

On peut aussi se servir de l'assertion *2* du théorème I.1.2 : ses relations passent parfaitement modulo un idéal propre. □

Remarque. Nous verrons dans la section I.5 que l'idéal I est engendré par $A^H \cap I$ dans A.

I.4.c Produit tensoriel

En fait, les propriétés précédentes portant sur la localisation et le passage au quotient peuvent être englobées en un seul et même théorème :

Théorème I.4.1 (voir [23], pages 85-86) *Soit A une algèbre galoisienne de groupe G sur un anneau R. Si T est une R-algèbre commutative, alors $T \otimes_R A$ est une algèbre galoisienne sur T de groupe G (G opère sur $T \otimes_R A$ par $g(t \otimes a) = t \otimes g(a)$, et nous pouvons identifier $T = T \otimes_R R$ à $T \otimes 1$ car R est un facteur direct de A).*

Démonstration La partie la plus difficile pour prouver ce théorème est de montrer que l'ensemble des points invariants de $T \otimes_R A$ sous l'action de G est exactement $T \otimes 1$. En effet, une fois ce résultat préliminaire obtenu, on utilise le théorème I.1.2 : le produit tensoriel par T ne pose alors aucun problème.

Pour prouver que T est bien l'ensemble des points fixes, il faut faire une démonstration analogue à celle faite pour le passage au quotient dans le paragraphe précédent : soit $c \in A$ dont la trace est 1. Alors $1 \otimes c$ a aussi une trace (sur T) égale à 1. Soit $x \in (T \otimes_R A)^G$:

$$\begin{array}{rcccl} x & = & x \sum_{g\in G} g(1\otimes c) & = & \sum_{g\in G} g(x(1\otimes c)) \\ & = & \sum_{g\in G} g(\sum_i a_i \otimes b_i) & = & \sum_i \sum_{g\in G} a_i \otimes g(b_i) \\ & = & \sum_i a_i \otimes \mathrm{tr}_{A:R}(b_i) & = & \sum_i a_i \,\mathrm{tr}_{A:R}(b_i) \otimes 1 \quad \in \quad T \otimes 1 \end{array}$$

Ceci montre finalement que les éléments de $T \otimes_R A$ invariants par G appartiennent à $T \otimes 1$, c'est-à-dire T. □

I.5 Factorisation des idéaux maximaux

Théorème I.5.1 *Soit A une algèbre galoisienne sur un anneau R de groupe G, Υ l'ensemble des idéaux de A stables par G et $\mathcal{I}$ l'ensemble des idéaux de R. Alors les applications "extension" et "rétraction" entre $\mathcal{I}$ et Υ sont réciproques l'une de l'autre.*

$$\begin{array}{rcl} \mathcal{I} & \longleftrightarrow & \Upsilon \\ I & \longmapsto & IA \\ J \cap R & \longleftarrow\!\shortmid & J \end{array}$$

Démonstration Il faut prouver les deux égalités suivantes : $IA \cap R = I$ et $(J \cap R)A = J$. La première est vérifiée car R est un facteur direct de A. La seconde l'est aussi : en effet, comme A est une R-algèbre galoisienne de groupe G, il existe des éléments x_i et y_i de A tels que $\sum_i x_i g(y_i) = \delta_{g,1}$ quel que soit $g \in G$. Dans ces conditions, pour tout $z \in A$, nous avons $z = \sum_i \mathrm{tr}(y_i z) x_i$ (lemme I.3.1). Si de plus z appartient à un idéal J stable sous l'action de G, alors $\mathrm{tr}(yz) = \sum_g g(yz)$ appartient $J \cap R$ pour tout $y \in A$, ce qui prouve que $z = \sum_i \mathrm{tr}(y_i z) x_i$ appartient à $(J \cap R)A$. Conclusion : $J \subset (J \cap R)A \subset J$. □

Par exemple, si nous posons $J = \bigcap_{g\in G} g\mathfrak{p}'$ où $\mathfrak{p}'$ est un idéal premier de A, alors $J = \mathfrak{p}A$ où $\mathfrak{p} = \mathfrak{p}' \cap R$ est la trace sur R de tous les $g\mathfrak{p}'$. Il est alors clair que l'idéal $\mathfrak{p}A$ est semi-premier.

> Rappel. Un idéal I d'un anneau A est dit semi-premier s'il est égal à sa racine, c'est-à-dire si pour $x \in A$, on a l'implication $x^n \in I \Rightarrow x \in I$.

Un deuxième exemple : si nous posons $J = \cap_{\mathfrak{p}'}\mathfrak{p}'$ où l'intersection porte sur tous les idéaux premiers de A, alors nous obtenons $J = (\cap_{\mathfrak{p}}\mathfrak{p})A$ où l'intersection porte sur tous les idéaux premiers de R. En effet, tout idéal premier de R se relève dans A car A est une algèbre entière sur R, autrement dit tout idéal premier $\mathfrak{p}$ de R est de la forme $\mathfrak{p}' \cap R$.

En résumé, nous obtenons le corollaire suivant :

Corollaire I.5.1 *Soit A une algèbre galoisienne sur un anneau R de groupe G, $\mathfrak{p}$ un idéal premier de R. Alors $\mathfrak{p}A = \cap_{\mathfrak{p}'}\mathfrak{p}'$ où l'intersection porte sur les idéaux premiers $\mathfrak{p}'$ au-dessus de $\mathfrak{p}$. En particulier, $\mathfrak{p}A$ est semi-premier ($\sqrt{\mathfrak{p}A} = \mathfrak{p}A$).*

De plus le nilradical de A est engendrée par celui de R ; donc si R est réduit alors A l'est aussi.

> Rappel. Le nil-radical d'un anneau est l'idéal formé par l'ensemble de ses éléments nilpotents (élément dont une certaine puissance est nulle). Cet idéal est en particulier l'intersection des idéaux premiers de l'anneau.
>
> On dit que l'anneau est réduit si l'ensemble de ses éléments nilpotents est réduit à $\{0\}$.

Nous pouvons poursuivre notre raisonnement en prenant des idéaux $\mathfrak{m}$ maximaux de R. Nous obtenons alors une factorisation de $\mathfrak{m}A$:

$$\mathfrak{m}A = \bigcap_{g\in G} g.\mathfrak{m}' = \prod_{\mathfrak{p}'\in G.\mathfrak{m}'} \mathfrak{p}'$$

où $\mathfrak{m}'$ est un idéal maximal de A au-dessus de $\mathfrak{m}$.

Cette propriété montre que A est une R-algèbre séparable. Séparable au sens de la définition suivante :

Définition I.5.1 (voir [23], page 72) *Une algèbre A de type fini sur un anneau R commutatif est dite **séparable** si pour tout idéal maximal $\mathfrak{m}$ de R, l'algèbre $A/\mathfrak{m}A$ est séparable sur le corps $R/\mathfrak{m}$.*

> Rappel. Une extension K/k de type fini est dite séparable s'il existe une base de transcendance $\mathcal{B}$ de K sur k telle que K soit une extension algébrique séparable sur $k(\mathcal{B})$ (voir la définition IV.1.1, page 98).
>
> Une algèbre algébrique (de type fini) sur un corps k est séparable si et seulement si le polynôme minimal de chacun de ses éléments est séparable.

Effectivement, nous savons qu'une algèbre galoisienne A est un R-module de type fini, mais aussi que l'extension $A/\mathfrak{m}'$ est galoisienne sur $R/\mathfrak{m}$ quel que soit l'idéal maximal $\mathfrak{m}'$ de trace $\mathfrak{m}$ sur R. De ces deux propriétés, on déduit la séparabilité de $A/\mathfrak{m}A \simeq \prod_{\mathfrak{m}'} A/\mathfrak{m}'$ sur $R/\mathfrak{m}$ en tant qu'algèbre.

Théorème I.5.2 *Soit A une algèbre galoisienne sur un anneau R de groupe G. Alors A est une R-algèbre (de type fini) séparable.*

I.6 Quand l'anneau de base est intégralement clos...

Dans cette section, nous allons étudier la structure très particulière des algèbres galoisiennes lorsque leur anneau des points fixes est intégralement clos. En effet, dans cette simple configuration, nous savons par exemple qu'une telle algèbre A est réduite (corollaire I.5.1). Par suite, comme dans tout anneau réduit (voir [9] page 152), nous avons

$$\bigcup_{\substack{\mathcal{P}\subset A \\ 1^{er}\text{ minimal}}} \mathcal{P} = \{\text{diviseurs de } 0\}$$

Dans notre cadre particulier, les propriétés sont bien sûr plus nombreuses... Nous allons démontrer qu'une algèbre galoisienne sur un anneau intégralement clos est isomorphe canoniquement à un produit fini d'anneaux intégralement clos. De plus, chacun de ces anneaux est une algèbre galoisienne (sur l'anneau de base) dont le groupe de Galois est très bien déterminé (voir la propriété I.6.3, page 31).

Théorème I.6.1 (Deuxième théorème d'existence, voir [10], page 56)
Soit R un anneau intégralement clos, A un anneau contenant R et entier sur R. On suppose que 0 est le seul élément de R qui soit diviseur de 0 dans A. Soit $p \subset q$ deux idéaux premiers de R et $\mathfrak{q}$ un idéal premier de A au-dessus de q. Alors il existe un idéal premier $\mathfrak{p}$ de A au-dessus de p et contenu dans $\mathfrak{q}$.

En particulier, si nous considérons une algèbre galoisienne A sur un anneau R intégralement clos, 0 est le seul élément de R qui est diviseur de 0 dans A car A est un module projectif (i.e. facteur direct d'un module libre) sur l'anneau intègre R. Ainsi les hypothèses et la conclusion de ce théorème sont tout-à-fait valides dans notre cadre.

I.6.a Idéaux premiers minimaux

Il n'est pas rare que l'on considère des anneaux nœthériens, car d'une part ceux-ci forment une large classe, et d'autre part ils possèdent des propriétés parfois très utiles : par exemple, dans un anneau nœthérien, les idéaux premiers minimaux sont en nombre fini.

Dans le cadre de cette section, nous avons le résultat similaire suivant :

Lemme I.6.1 *Soit A une algèbre galoisienne de groupe G sur un anneau R intégralement clos. Les idéaux premiers minimaux de A sont les idéaux premiers de A au-dessus de l'idéal premier $(0) \subset R$.*

Le nombre d'idéaux premiers minimaux dans A est fini (car ils sont G-conjugués).

Démonstration Si deux idéaux premiers $\mathfrak{p} \subset \mathfrak{q}$ de A sont au-dessus de (0), alors ils sont égaux car au-dessus d'un même idéal premier (voir [44], page 50). Ainsi les idéaux premiers de A au-dessus de (0) sont minimaux.

Réciproquement, si $\mathfrak{q}$ est un idéal premier qui n'est pas au-dessus de (0), alors il existe un idéal premier $\mathfrak{p} \subset \mathfrak{q}$ au-dessus de (0) (théorème I.6.1). Par suite, on a nécessairement $\mathfrak{p} \neq \mathfrak{q}$, donc $\mathfrak{q}$ n'est pas minimal. □

Propriété I.6.1 *Soit A une algèbre galoisienne de groupe G sur un anneau R intégralement clos. Soit $\mathfrak{p}$ un idéal premier minimal de A (au-dessus de (0)). Alors $A/\mathfrak{p}$ est une R-algèbre galoisienne intègre de groupe $H = \mathrm{Stab}_G(\mathfrak{p}) = \{g \in G \mid g\mathfrak{p} = \mathfrak{p}\}$.*

Démonstration Soit $K_\mathfrak{p}$, K_H et K les corps des fractions des anneaux intègres $A/\mathfrak{p}$, $A^H/(A^H \cap \mathfrak{p})$ et R respectivement. Nous savons déjà que $A/\mathfrak{p}$ est galoisienne sur le quotient $A^H/(A^H \cap \mathfrak{p})$ de groupe H (propriété I.4.4). Nous en déduisons par localisation que l'extension $K_\mathfrak{p}$ est galoisienne sur K_H de groupe H.

D'autre part, grâce au corollaire I.4.2, nous savons que $K_\mathfrak{p}$ est une extension galoisienne de K de groupe de Galois H. Ainsi $K_H = K$, autrement dit $A^H/(A^H \cap \mathfrak{p})$ et R ont le même corps des fractions. Comme $A^H/(A^H \cap \mathfrak{p})$ est entier sur R et R est intégralement clos, nous avons l'égalité de ces deux anneaux : $A/\mathfrak{p}$ est galoisienne sur R de groupe H. □

> Remarque. On n'est pas obligé de supposer l'idéal $\mathfrak{p}$ de A au-dessus de (0). Si l'on suppose que $R/\mathfrak{q}$ est intégralement clos avec $\mathfrak{q} = \mathfrak{p} \cap R$, alors $A/\mathfrak{p}$ est une algèbre intègre galoisienne sur $R/\mathfrak{q}$ de groupe $H = \mathrm{Stab}_G(\mathfrak{p})$. Pour démontrer cela, il suffit d'utiliser la propriété I.6.1 en considérant l'algèbre $A/\mathfrak{q}A$ galoisienne sur $R/\mathfrak{q}$ de groupe G.

Propriété I.6.2 *Soit A une algèbre galoisienne de groupe G sur un anneau R intégralement clos de corps des fractions K. Alors A est intégralement fermée dans son anneau total des fractions $K \otimes_R A = (R^*)^{-1}A$ (algèbre galoisienne sur K, de groupe G).*

> Remarque. Par définition, **l'anneau total des fractions** d'anneau commutatif quelconque A est le localisé de A par les éléments réguliers (non diviseurs de 0) de A. En outre, A s'injecte dans son anneau total des fractions.
>
> Dans notre cas où R est intègre, les éléments réguliers de A sont ceux dont la norme sur R est non nulle (voir la propriété I.3.2). Ainsi, toute fraction $b^{-1}a$ où b est un élément régulier de A peut se mettre sous la forme $\mathrm{N}(b)^{-1}ab' \in (R^*)^{-1}A$, avec $b' = \prod_g g(b)$ où le produit porte sur les éléments $g \in G \setminus \{\mathrm{Id}\}$.

Démonstration Nous savons que $K \otimes_R A = (R^*)^{-1}A$ est une K-algèbre galoisienne de groupe G.

Soit $(x_i, y_i)_i$ des éléments de A vérifiant $\sum_i x_i g(y_i) = \delta_{1,g}$ pour tout $g \in G$. Ces éléments existent car A est une R-algèbre galoisienne de groupe G. Nous savons qu'il en existe également dans la K-algèbre galoisienne $K \otimes_R A = (R^*)^{-1}A$: nous pouvons prendre les mêmes $(x_i, y_i)_i$ puisque A s'injecte dans $K \otimes_R A = (R^*)^{-1}A$.

Grâce au lemme I.3.1 appliqué à $(R^*)^{-1}A$, nous avons

$$\forall\ z \in (R^*)^{-1}A, \qquad z = \sum_i \mathrm{tr}(zy_i)x_i$$

Si nous considérons un élément $z \in (R^*)^{-1}A$ entier sur A, alors celui-ci est entier sur R (car A est une algèbre entière sur R). Comme les y_i appartiennent à A, ils sont également entiers sur R, si bien que les produits zy_i le sont aussi. Dès lors, $\mathrm{tr}(zy_i)$ est un élément de K entier sur R. Or R est intégralement clos, donc $\mathrm{tr}(zy_i)$ appartient à R. Finalement, si un élément z de $(R^*)^{-1}A$ est entier sur A, alors z appartient au module $\sum_i Rx_i$, donc à A : l'algèbre A est intégralement fermée dans son anneau total des fractions. □

I.6.b Idempotents indécomposables

Lorsqu'un anneau nœthérien est réduit, il est connu que son anneau total des fractions est un produit fini de corps (voir [9], page 153). De plus, si cet anneau nœthérien réduit est intégralement fermé dans son anneau total des fractions, alors il est isomorphe à un produit d'anneaux intégralement clos.

Nous proposons ici un résultat tout-à-fait similaire pour les algèbres galoisiennes "montées" sur les anneaux intégralement clos.

Propriété I.6.3 *Soit A une algèbre galoisienne de groupe G sur un anneau R intégralement clos. Alors $A = \oplus_e Ae$ où la somme directe porte sur les idempotents indécomposables e de A. Ceux-ci sont G-conjugués. De plus, les R-algèbres Ae sont intégralement closes et galoisiennes de groupe* $\mathrm{Stab}_G(e)$.

Démonstration Soit K le corps des fractions de R et $A' = K \otimes_R A = (R^*)^{-1}A$. Nous rappelons que A' est une K-algèbre galoisienne de groupe G. Tout d'abord les idempotents de A' appartiennent à A. En effet, ces derniers sont entiers sur R (car racines de T^2-T) et font partie de la clôture intégrale de A' sur R, c'est-à-dire A en vertu de la propriété I.6.2.

D'autre part, la K-algèbre galoisienne A' est une K-algèbre artinienne (car de dimension finie) et réduite (corollaire I.5.1). Il s'agit donc d'un produit de corps

$$A' \simeq K \otimes_R A \simeq (R^*)^{-1}A \simeq \prod_{\substack{\mathfrak{m} \subset A' \\ \text{maximal}}} A'/\mathfrak{m}$$

De plus, tout idéal d'un produit de corps est engendré par un unique idempotent. Ainsi pour tout idéal maximal $\mathfrak{m} \subset A'$, nous noterons $e'_\mathfrak{m}$ l'idempotent qui engendre $\mathfrak{m}$. Ces idempotents engendrent des idéaux maximaux dans A'. De façon symétrique, les idempotents $e_\mathfrak{m} = 1 - e'_\mathfrak{m}$ forment l'ensemble des **idempotents indécomposables** de A', et même de A (puisqu'ils appartiennent à A). Nous obtenons simultanément deux sommes directes, l'une de corps, l'autre d'anneaux intègres :

$$A' = \bigoplus_{e_\mathfrak{m}} A'e_\mathfrak{m} \qquad \text{et} \qquad A = \bigoplus_{e_\mathfrak{m}} Ae_\mathfrak{m}$$

Justifions à présent que les idempotents indécomposables $e_\mathfrak{m}$ de A sont G-conjugués. Il revient au même de montrer que les idempotents $e'_\mathfrak{m} = 1-e_\mathfrak{m}$ le sont. Or les idempotents $e'_\mathfrak{m}$ sont des premiers de A car $A/(e'_\mathfrak{m}) \simeq Ae_\mathfrak{m} \subset A'e_\mathfrak{m}$ (corps). On pourrait également évoquer le fait que $Ae'_\mathfrak{m}$ est la trace sur A de l'idéal maximal $A'e'_\mathfrak{m}$ de A'.

Le théorème I.1.1 nous affirme que les idéaux premiers $Ae'_\mathfrak{m}$ de A sont G-conjugués car ils sont tous au-dessus de l'idéal premier $(0) \subset R$. Par unicité de l'idempotent générateur de tout idéal de A', nous obtenons bien le résultat : les $e_\mathfrak{m}$ sont G-conjugués.

De plus, grâce à la propriété I.6.1, nous savons que les quotients $A/(e'_\mathfrak{m}) \simeq Ae_\mathfrak{m}$ sont des R-algèbres galoisiennes intègres de groupe $\mathrm{Stab}_G(e'_\mathfrak{m}) = \mathrm{Stab}_G(e_\mathfrak{m})$.

Enfin, la propriété I.6.2 prouve que chaque R-algèbre $Ae_\mathfrak{m}$ est intégralement close. □

Corollaire I.6.1 *Toute algèbre galoisienne sur un anneau intégralement clos est un anneau normal ayant un nombre fini d'idéaux premiers minimaux.*

> Rappel. Un anneau commutatif est dit **normal** si le localisé de cet anneau en chacun de ses idéaux premiers est intégralement clos (voir [45], page 64).

Démonstration Nous savons maintenant qu'une algèbre galoisienne sur un anneau R intégralement clos est isomorphe à A^d où A est un anneau intégralement clos. Un idéal premier $\mathcal{P}$ de A^d est de la forme

$$\mathcal{P} = A \times \cdots \times A \times \mathfrak{p} \times A \times \cdots \times A$$

où $\mathfrak{p}$ est un idéal premier de A, si bien que le localisé $A^d{}_{\mathcal{P}}$ est isomorphe au localisé $A_{\mathfrak{p}}$. Or A est intégralement clos, donc $A^d{}_{\mathcal{P}} \simeq A_{\mathfrak{p}}$ l'est également. □

I.6.c Polynôme minimal et résolvante

Définition I.6.1 *Soit A un anneau commutatif sur lequel opère un groupe fini G et le sous-anneau des points fixes $R = A^G$. Pour tout élément $x \in A$, on définit le polynôme*

$$g(T) = \prod_{y \in G.x} (T - y)$$

*Ce polynôme unitaire est à coefficients dans R. Il est appelé **résolvante** associée à x.*

Lemme I.6.2 *Soit R un anneau intégralement clos, K son corps des fractions et P, Q deux polynômes unitaires de $K[T]$ tels que $P.Q \in R[T]$. Alors P et Q appartiennent à $R[T]$.*

Démonstration Les racines des polynômes P et Q sont des éléments entiers sur R car le produit $P.Q \in R[T]$ est unitaire. Donc les coefficients de P et Q sont entiers sur R. Or ils appartiennent à K, donc à R. □

Grâce à ce lemme, on peut définir le polynôme minimal d'un élément entier sur un anneau intégralement clos, le pgcd de deux polynômes unitaires à coefficients dans ce même anneau, ainsi que leurs parties sans facteur carré, etc...

Propriété I.6.4 *Soit A un anneau sur lequel opère un groupe fini G et $R = A^G$ le sous-anneau des points fixes. On sait que A est entier sur R. On suppose que R est un anneau intégralement clos. Soit x un élément de A. Soit μ_x le polynôme minimal de x sur R et g la résolvante associée à x. Alors μ_x divise g qui lui-même divise $\mu_x^{|G.x|}$ dans $R[T]$.*

Démonstration Le fait que μ_x divise $g \in R[T]$ est évident puisque $g(x) = 0$ et R est intégralement clos.

Comme x est racine de $\mu_x \in R[T]$, $T - x$ divise $\mu_x(T)$ dans $A[T]$. Si l'on pose $y = \sigma.x$ où $\sigma \in G$, on obtient la même chose, c'est-à-dire $T - y$ divise $\mu_x(T)$ dans $A[T]$, car μ_x appartient à $R[T]$. En multipliant toutes ces relations de divisibilité entre elles pour y variant dans $G.x$, on voit que $g = \prod_{y \in G.x}(T - y)$ divise $\mu_x^{|G.x|}$ dans $A[T]$... Or g est unitaire, donc on peut considérer la division euclidienne de $\mu_x^{|G.x|}$ par g dans $R[T]$. Par unicité des quotient et reste de cette division, on voit que g divise $\mu_x^{|G.x|}$ dans $R[T]$. □

Théorème I.6.2 *Soit A une algèbre galoisienne de groupe G sur un anneau R intégralement clos. Si x est un élément de A, alors le polynôme minimal de x sur R (noté μ_x) est la partie sans facteur carré de sa résolvante* $\prod_{y \in G.x} (T - y)$.

Démonstration Montrons que μ_x est sans facteur carré : si $h \in R[T]$ est un polynôme tel que h^2 divise μ_x dans $R[T]$ alors

$$\mu_x \frac{\mu_x}{h^2} = \left(\frac{\mu_x}{h}\right)^2 \quad \in R[T]$$

est un polynôme de $R[T]$ qui s'annule en x. Comme A est réduit (corollaire I.5.1), le polynôme $\frac{\mu_x}{h}$ s'annule aussi en x. Ainsi h est nécessairement égal à 1 si l'on ne veut pas contredire la définition de μ_x...

Pour montrer que le polynôme minimal de x est la partie sans facteur carré de sa résolvante, il suffit d'utiliser la propriété I.6.4 en remarquant que la partie sans facteur carré de μ_x est égale à μ_x comme on vient de le constater. □

Un exemple des plus classiques dans lequel le polynôme minimal de x n'est pas égal à la résolvante de x, est celui où x est un idempotent de A distinct de 0 et 1 : en effet, le polynôme minimal de x est $T^2 - T$, alors que sa résolvante n'a aucune raison d'être de degré 2 (cette dernière est de la forme $T^i - T^j$ où $j < i = |G.x|$).

I.7 Algèbre galoisienne libre

I.7.a Trace, norme et polynôme caractéristique

Définition I.7.1 (voir [47], chapitre 2) *Soit A une R-algèbre libre de rang fini. Pour un élément $x \in A$, on considère l'endomorphisme de multiplication par x, noté m_x. On définit* ***la norme, la trace et le polynôme caractéristique*** *de x comme étant respectivement le déterminant, la trace et le polynôme caractéristique de l'endomorphisme m_x. Les notations respectives sont* $\mathrm{N}_{A:R}(x)$, $\mathrm{tr}_{A:R}(x)$ *et* $\chi_{A:R}(x)$.

Le lecteur pourra consulter au besoin les références "bourbakistes" suivantes : Algèbre,

chap. 3 parag. 9 Normes et traces, pages 107-116, Hermann 1970,
Dans ce paragraphe sont données les définitions et quelques propriétés de la norme et de la trace d'un élément d'un module, puis dans une algèbre.

chap. 5 parag. 8 Normes et traces, pages 45-50, Masson 1981,
Ce paragraphe est consacré plus particulièrement aux algèbres étales : l'auteur fait le lien entre les norme, trace, polynôme caractéristique et les endomorphismes de l'algèbre étale.

chap. 8 parag. 12 Normes et traces, pages 142-150, Hermann 1958,
Ici est traité plus précisément le cas des traces et normes dans les algèbres réduites.

chap. 9 parag. 2 Discriminant d'une forme sesquilinéaire, pages 41-47, Hermann 1959,
C'est un paragraphe sur les discriminants des formes sesquilinéaires. On y trouve entre autre une démonstration de la formule de transitivité du discriminant et une condition de séparabilité des algèbres de dimension finie.

Dans le cadre d'une algèbre galoisienne A de groupe G, leurs définitions sont assez différentes : la trace d'un élément x est la somme $\sum_g g(x)$, sa norme est le produit $\prod_g g(x)$, et son polynôme caractéristique $\prod_g \big(T - g(x)\big)$.

Prouvons que ces "doubles définitions" sont compatibles dans le cadre d'une algèbre galoisienne libre. Ce résultat ne serait guère étonnant tellement on a l'habitude de ce fait en théorie des corps.

Théorème I.7.1 *Soit A une algèbre galoisienne libre sur R de groupe G et $x \in A$. On note m_x la multiplication par x dans A. Alors*

$$\mathrm{tr}(x) = \mathrm{tr}(m_x) = \sum_{g\in G} g(x) \qquad \mathrm{N}(x) = \det(m_x) = \prod_{g\in G} g(x)$$
$$\chi_x(T) = \det(T\,\mathrm{Id} - m_x) = \prod_{g\in G}(T - g(x))$$

Démonstration Considérons donc l'endomorphisme m_x, la multiplication par x dans A. Dans $A\otimes_R A$, les trace, déterminant, et polynôme caractéristique de $m_{1\otimes x}$ sont les mêmes que ceux de m_x. Grâce au théorème I.1.2, on sait qu'une algèbre galoisienne A de groupe G vérifie $A\otimes_R A \simeq \prod_G A$. Cet isomorphisme de A-algèbres qui envoie $1\otimes x$ sur $\big(g(x)\big)_{g\in G}$ conserve aussi ces trois quantités. Or dans $\prod_G A$, il est facile de les calculer : $\sum_g g(x)$, $\prod_g g(x)$ et $\prod_g \big(T - g(x)\big)$. □

I.7.b Discriminant

Dans cette section, nous proposons une autre approche pour établir le théorème précédent. La méthode est certes moins directe, mais elle fait appel à une notion non-abordée jusqu'à présent : la notion de discriminant.

Soit A un module libre sur un anneau R et $\mathcal{B}$ une base de A. On définit canoniquement la base duale de $\mathcal{B}$ dans le dual A^* de A. Si nous considérons une forme bilinéaire $\mu : A \times A \to R$, nous pouvons définir alors le discriminant d'une famille finie F de vecteurs comme étant le déterminant de la matrice formée par $\big(\mu(a,b)\big)_{a,b\in F}$.

Supposons de plus que cette forme bilinéaire μ est non dégénérée, c'est-à-dire réalisant un isomorphisme entre A et A^* par $a \mapsto \mu(a, \bullet)$. A tout élément b de la base $\mathcal{B}$ correspond une forme linéaire $b^* \in A^*$ tel que

$$\forall\ a \in A, \qquad a = \sum_{b\in\mathcal{B}} b^*(a)b$$

Nous définissons alors la base duale $\mathcal{B}' = \{b'\}_{b\in\mathcal{B}} \subset A$ pour la forme μ en posant

$$\mu(b', \bullet) = b^*$$

pour tout $b^* \in \mathcal{B}^*$. La base duale $\mathcal{B}'$ pour μ peut également être définie par les relations $\mu(b', c) = \delta_{b,c}$ pour $b, c \in \mathcal{B}$. Il est alors clair que la base duale de $\mathcal{B}'$ est $\mathcal{B}$ elle-même : $(\mathcal{B}')' = \mathcal{B}$.

Pour une telle forme bilinéaire, si une famille $\mathcal{B}$ est une base, alors son discriminant est inversible car il s'agit du déterminant de l'isomorphisme entre A et A^* donné par μ (non dégénérée).

Dans une R-algèbre galoisienne A de groupe G, nous possédons une forme bilinéaire non dégénérée très particulière. Il s'agit de l'application

$$\mu \ : \ (x, y) \in A \times A \longmapsto \mathrm{tr}_G(xy) = \sum_{g \in G} g(xy)$$

Nous notons provisoirement la trace d'une algèbre galoisienne tr_G pour la distinguer de la trace dans les algèbres libres. En fait, nous allons montrer qu'elles sont égales.

Nous disposons alors d'une base duale $\mathcal{B}' \subset A$, et nous savons que $\det\big(\mathrm{tr}_G(bc)\big)_{b,c \in \mathcal{B}}$ est inversible dans R. Numérotons les éléments de la base $\mathcal{B}$ par $b_1, \ldots, b_n$ et ceux de la base duale $\mathcal{B}'$ par $b'_1, \ldots, b'_n$, tout en conservant les égalités $b_i^* = \mathrm{tr}_G(b'_i \bullet)$ bien sûr (nous avons nécessairement $n = |G|$). Considérons maintenant la matrice

$$P = \big(g_i(b_j)\big)_{i,j=1..n}$$

Les coefficients de la matrice P appartiennent à l'algèbre A. En revanche, ceux de ${}^tP.P$ font partie de R comme le montre ce petit calcul :

$$({}^tP.P)_{ij} = \sum_k g_k(b_i) g_k(b_j) = \mathrm{tr}_G(b_i b_j) \in R$$

Nous obtenons en particulier la relation classique entre les déterminants

$$\Big(\det\big(g_i(b_j)\big)_{i,j}\Big)^2 = \det({}^tP.P) = \det\big(\mathrm{tr}_G(b_i b_j)\big)_{i,j} \in \mathrm{U}(R)$$

où $U(R)$ est le groupe des éléments inversibles de R. Ceci prouve l'inversibilité de la matrice P dans $M_n(A)$.

> Remarque. On peut vérifier ce résultat d'une autre façon en calculant QP où la matrice Q est égale à $\big(g_j(b'_i)\big)_{i,j=1..n}$:
>
> $$(QP)_{ij} = \sum_k g_k(b'_i) g_k(b_j) = \mathrm{tr}_G(b'_i b_j) = b_i^*(b_j) = \delta_{ij}$$
>
> La matrice Q est l'inverse de P.

Nous venons de démontrer le lemme suivant :

Lemme I.7.1 *Soit A une algèbre galoisienne libre sur R de groupe G et de base $\mathcal{B}$. Alors la matrice $P = \big(g(b)\big)_{\substack{g \in G \\ b \in \mathcal{B}}}$ est inversible dans $M_n(A)$ ($n = |G| = |\mathcal{B}|$).*

Théorème I.7.2 *Soit A une algèbre galoisienne libre sur R de groupe $G = \{g_1, \dots, g_n\}$ et $y \in A$. La matrice de multiplication par y (dans une base quelconque) est semblable dans $M_n(A)$ à la matrice diagonale $D = \operatorname{diag}\big(g_i(y)\big)_{i=1..n}$.*

Démonstration Dans une base $\mathcal{B} = \{b_1, \dots, b_n\}$ de A, la matrice $M = (y_{ij}) \in M_n(R)$ de la multiplication par y est définie par : $b_j y = \sum_k y_{kj} b_k$.

En appliquant g_i, il vient $g_i(y)g_i(b_j) = \sum_k y_{kj} g_i(b_k)$. Mais $g_i(y)g_i(b_j) = (DP)_{ij}$, tandis que $\sum_k y_{kj} g_i(b_k) = (PM)_{ij}$. Cela prouve que $DP = PM$ et le résultat puisque P est inversible. □

Les matrices D et M ont alors les mêmes "invariants", entre autres les mêmes traces, déterminants, polynômes caractéristiques... Nous venons de démontrer à nouveau le théorème I.7.1.

Théorème I.7.3 *Soit A une R-algèbre galoisienne libre de groupe G. Alors le discriminant de A sur R est inversible.*

> Rappel. Le discriminant d'une algèbre libre est par définition le discriminant par rapport à la forme bilinéaire "tracique" $(x, y) \mapsto \operatorname{tr}(xy)$ d'une base quelconque $\mathcal{B}$ de l'algèbre, c'est-à-dire $\det\big(\operatorname{tr}(ab)\big)_{a,b\in\mathcal{B}}$. Cette valeur est la même pour toute base, au carré d'un inversible près.

I.8 Éléments primitifs, normaux

I.8.a Algèbres étales

Le lecteur trouvera dans [14] (pages 28-40) une étude approfondie portant sur les algèbres étales. Les résultats de cette étude nous intéressent particulièrement puisque les algèbres galoisiennes sur des corps sont de dimension finie et séparables, i.e. étales. Nous en rappelons ici quelques propriétés.

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

Définition I.8.1 *On dit qu'une K-algèbre A est **étale** s'il existe une extension Ω de K telle que $A \otimes_K \Omega$ soit isomorphe à Ω^n. (A est alors nécessairement une K-algèbre commutative de dimension finie.)*

*On dit alors que Ω **diagonalise** A sur K.*

Théorème I.8.1 *Soit A une algèbre commutative de dimension finie sur un corps K. L'algèbre A est étale sur K si et seulement si elle est séparable, i.e. le polynôme minimal sur K de tout élément de A est à racines simples.*

Propriété I.8.1 *Soit A une algèbre étale sur K. Il n'existe qu'un nombre fini de sous-algèbres et d'idéaux de A. De plus, toute extension de K qui diagonalise A diagonalise toute sous-algèbre et toute algèbre quotient de A, et en particulier ces algèbres sont étales.*

Théorème I.8.2 *Supposons K infini ; soit A une K-algèbre commutative ne possédant qu'un nombre fini de sous-algèbres, et soit V un sous-espace vectoriel de A qui engendre A. Il existe $x \in V$ tel que $A = K[x]$.*

Corollaire I.8.1 *Soit K un corps infini et A une K-algèbre étale. Alors il existe $x \in A$ tel que $A = K[x]$. En particulier, toute algèbre galoisienne sur un corps infini possède un élément primitif.*

Démonstration Il est tout-à-fait possible de démontrer ce corollaire en utilisant la propriété I.8.1 puis le théorème I.8.2. Cependant, nous proposons ici une autre démonstration de ce corollaire. Comme une algèbre étale est engendrée par un nombre fini d'éléments séparables, il suffit de prouver qu'une algèbre engendrée par deux éléments séparables est monogène. Soit donc $A = K[a, b]$ une algèbre étale sur K.

Par définition, $A' = A \otimes_K \Omega$ est isomorphe à Ω^n ($n = \dim_K A$) en tant que Ω-algèbre. On note v et w les images respectives de a et b par cet isomorphisme. Notre but est maintenant de prouver l'existence d'un élément primitif de la forme $v + \lambda w$ ($\lambda \in K$) engendrant Ω^n : si ce but est atteint, on aura alors $A = K[a + \lambda b]$ car les polynômes minimaux de $v + \lambda w$ sur Ω et de $a + \lambda b$ sur K sont égaux (rationalité).

Un élément $u \in \Omega^n$ est primitif si (et seulement si) toutes ses coordonnées sont distinctes. Prouvons que l'ensemble des $\lambda \in K$ tel que $v + \lambda w$ ait au moins deux coordonnées identiques est un ensemble fini. Comme K est supposé infini, l'objectif que nous nous sommes fixé sera atteint.

L'équation en λ, $(v + \lambda w)_i = (v + \lambda w)_j$ avec $i \neq j$, revient à

$$\lambda(w_i - w_j) = v_j - v_i$$

Il est impossible d'avoir $w_i = w_j$ et $v_j = v_i$ simultanément, sinon pour tout vecteur u de $\Omega[v, w]$, on a $u_i = u_j$ et donc $n = \dim_\Omega A' = \dim_\Omega \Omega[v, w] < n$...

Si $w_i - w_j = 0$ alors $0 = v_i - v_j \neq 0$: absurde. Si $w_i - w_j \neq 0$ alors

$$\lambda = (v_j - v_i)(w_i - w_j)^{-1}$$

(si cette valeur appartient à K). Finalement on voit qu'il n'existe qu'un nombre fini de valeurs possibles λ pour que $v + \lambda w$ ait deux coordonnées i et j identiques, c'est-à-dire pour que $a + \lambda b$ ne soit pas un élément primitif de A... □

> Remarque. Si $A = K[x_1, \ldots, x_n]$ est étale sur un corps K infini, alors il existe une combinaison K-linéaire des x_i qui est un élément primitif de A.

I.8.b Base normale

Considérons une algèbre galoisienne A de groupe G sur un corps K. Il est clair que A est libre, et de dimension $|G|$ sur K d'après le corollaire I.1.1 (page 19). Il s'agit donc d'une algèbre artinienne sur K. Or les anneaux artiniens sont très bien classifiés :

Théorème I.8.3 (cf [44], page 126) *Soit un anneau A artinien commutatif et dont les idéaux maximaux sont $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$. Alors*

- $\mathrm{rad}(A) = \sqrt{(0)} = \mathfrak{p}_1 \dots \mathfrak{p}_s$
- $\exists\ n \in \mathbb{N} - \{0\},\ \mathrm{rad}(A)^n = (0)$
- $\exists\ n \in \mathbb{N} - \{0\},\ A \simeq \prod_{i=1}^{s} A/\mathfrak{p}_i^n$ *produit d'anneaux artiniens locaux d'idéal maximal* $\mathfrak{p}_i$
- $A/\mathfrak{p}_i^n$ *est isomorphe au localisé de* A *en* $\mathfrak{p}_i$

Sachant qu'une algèbre galoisienne sur un corps est toujours séparable, elle est obligatoirement un produit de corps : $A \simeq \prod_{\mathfrak{m}\ \text{maxi.}} A/\mathfrak{m}$. Nous savons de plus que les idéaux maximaux de A sont conjugués sous l'action du groupe de Galois, car ils sont tous au-dessus de l'idéal maximal (0) du corps de base. Les quotients $(A/\mathfrak{m})_{\mathfrak{m}\ \text{maxi.}}$ sont donc tous isomorphes. Enfin nous savons, par définition d'une algèbre galoisienne, que $A/\mathfrak{m}$ est une extension galoisienne de K de groupe de Galois $D(\mathfrak{m}) = \mathrm{Stab}_G(\mathfrak{m})$.

Montrons, **sans utiliser** la théorie de Galois classique, qu'il existe une base normale dans A lorsque K est un corps infini.

Démonstration Nous savons grâce au corollaire I.8.1 qu'il existe une K-base de A formée par les premières puissances d'un élément primitif α (K est supposé infini). Grâce à la propriété I.1.4, il existe des $a_j \in A$ tels que

$$\sum_j a_j \tau(\alpha)^j = \delta_{1,\tau} \qquad \forall\ \tau \in G$$

Les quantités a_j sont uniques car les premières puissances de α forment une base sur R. Elles ne sont pas difficiles à exprimer si l'on connaît le polynôme minimal f de α sur K. En effet ce sont les coefficients du polynôme

$$g(T) = \frac{f(T)}{(T-\alpha)f'(\alpha)} = \sum_j a_j T^j \quad \in A[T]$$

> Remarque. Ce polynôme est donné par Artin dans [5] (page 66) dans le cadre classique de la théorie des extensions galoisiennes.

Précisons pourquoi $f'(\alpha)$ est inversible dans A : il suffit de spécialiser en α une relation de Bezout entre f et f'.

Considérons les polynômes conjugués de g : $g_\sigma(T) = \sum_j \sigma(a_j) T^j$. Lorsqu'on les évalue en α, on obtient ces relations : $g_\sigma(\alpha) = \delta_{\sigma,1}$, si bien que nous avons

$$\sum_{\sigma \in G} g_{\sigma\tau}(\alpha) g_{\sigma\tau'}(\alpha) = \delta_{\tau,\tau'} \qquad \forall\ \tau, \tau' \in G$$

On déduit de cette dernière égalité la non nullité du polynôme

$$h(T) = \det\left(\sum_{\sigma \in G} g_{\sigma\tau}(T) g_{\sigma\tau'}(T)\right)_{\tau,\tau' \in G}$$

puisque ce dernier vaut 1 lorsqu'on l'évalue en α. Comme le corps de base K est infini, il existe $x \in K$ qui n'est pas racine de h. Posons

$$y = g(x) = \frac{f(x)}{(x-\alpha)f'(\alpha)}$$

Nous avons alors $g_{\sigma\tau}(x) = \sigma\tau(y)$, donc $0 \neq h(x) = \det\left(\mathrm{tr}\left(\tau(y)\tau'(y)\right)\right)_{\tau,\tau' \in G}$. Ceci prouve que $\{\tau(y),\ \tau \in G\}$ forme une K-base de A, c'est-à-dire que y est un élément normal de A sur K. □

Nous venons de démontrer qu'il existe une base normale dans toute algèbre galoisienne sur un corps infini. Le théorème suivant généralise cette propriété :

Théorème I.8.4 (voir [16], pages 27-28) *Soit A une algèbre galoisienne de groupe G sur un anneau semi-local R (R ne contient qu'un nombre fini d'idéaux maximaux). Alors A et $R[G]$ sont isomorphes en tant que $R[G]$-modules. De manière équivalente, il existe une R-base normale dans A.*

Démonstration La preuve que nous allons donner **utilise** la théorie de Galois classique, contrairement à tout ce que nous avons présenté jusqu'ici...

Lemme I.8.1 *Soit A une algèbre galoisienne de groupe G sur un corps K. Alors il existe une K-base normale dans A.*

Pour démontrer ce lemme, utilisons la décomposition de la K-algèbre galoisienne A en somme directe d'extensions galoisiennes

$$A = \bigoplus_x A.x = \bigoplus_{\sigma \in (G/H)_g} A.\sigma(e)$$

où la somme de gauche porte sur tous les idempotents indécomposables x de A et, dans la somme de droite, e est un idempotent indécomposable de A fixé et $H = \mathrm{Fix}_G(e)$ (voir la propriété I.6.3, page 31). De plus, $A.e$ est une extension galoisienne au sens classique de K : il existe donc un élément normal z de $A.e$ sur K. Ainsi

$$A.e = \bigoplus_{h \in H} K.h(z) \qquad A.\sigma(e) = \sigma(A.e) = \bigoplus_{h \in \sigma.H} K.h(z)$$

Finalement, comme G est la réunion disjointe des classes à gauche de $(G/H)_g$, nous obtenons

$$A = \bigoplus_{g \in G} K.g(z)$$

Autrement dit, l'élément $z \in A$ est normal.

Maintenant que ce lemme est prouvé, revenons aux hypothèses du théorème. Nous rappelons que A est en particulier un module libre de rang $|G|$ sur l'anneau semi-local R car A est un R-module projectif.

Soit $\mathfrak{m}$ un idéal maximal de R. Nous savons que $A/\mathfrak{m}A$ est une algèbre galoisienne sur le corps $R/\mathfrak{m}$ de groupe G (propriété I.4.4). Il existe donc un élément normal $z_\mathfrak{m}$ de $A/\mathfrak{m}A$ sur le corps $R/\mathfrak{m}$. En appliquant le théorème chinois aux idéaux co-maximaux $\mathfrak{m}A$, nous prouvons l'existence d'un élément $z \in A$ dont la classe modulo $\mathfrak{m}A$ est $z_\mathfrak{m}$, quel que soit l'idéal maximal $\mathfrak{m}$ de R.

Notons $d \in R$ le déterminant de la famille $G.z$ dans une R-base quelconque $\mathcal{B}$ de A. Si d n'est pas inversible dans R, alors il existe un idéal maximal $\mathfrak{m} \subset R$ contenant d. Par suite, dans l'algèbre galoisienne résiduelle $A/\mathfrak{m}A$, le déterminant $d \pmod{\mathfrak{m}}$ de la famille $G.z \pmod{\mathfrak{m}A} = G.z_\mathfrak{m}$ dans la base $\mathcal{B} \pmod{\mathfrak{m}A}$ est nul. Or ceci est impossible par définition de $z_\mathfrak{m}$...

Conclusion : d est inversible dans R et $G.z$ est une base normale de A sur R. □

Remarque. En théorie de Galois classique (extensions de corps), il existe toujours des éléments normaux. Ceux-ci sont en particulier des éléments primitifs de l'extension galoisienne.

En revanche, dans une algèbre galoisienne, un élément normal (s'il existe) n'est pas nécessairement un élément primitif. Prenons l'exemple le plus simple possible :

$$A = R^n$$

où R est un anneau commutatif quelconque. L'algèbre A est galoisienne sur R pour tout groupe d'ordre n transitif sur $\{1, \dots, n\}$ (ce groupe opère sur A en permutant les coordonnées). L'idempotent $(1, 0, 0, \dots)$ est bien un élément normal de A, mais il est clair qu'il n'en est pas un élément primitif si $n > 2$.

Nous pouvons même ajouter que, si le cardinal de R est strictement inférieur à n, alors il n'existe pas d'élément primitif de A sur R ! Les notions d'éléments primitifs et normaux sont donc tout-à-fait disjointes dans le cadre de la théorie des algèbres galoisiennes...

Chapitre II

Algèbre de décomposition universelle

Soit R un anneau commutatif unitaire et $f \in R[T]$ un polynôme unitaire non constant de degré n. On suppose qu'il existe un sur-anneau A de R dans lequel f se factorise :

$$f(T) = (T - \theta_1) \cdots (T - \theta_n)$$

où les $\theta_i \in A$ sont inconnus.

Peut-on faire du calcul dans $R[\theta_1, \ldots, \theta_n]$? La réponse est oui. Mais alors, quels genres de calcul peut-on faire ? Par exemple, calculer des expressions symétriques en les θ_i. On sait que leurs valeurs appartiennent à R grâce au théorème suivant.

Théorème II.0.1 *Soit un polynôme $P \in R[X_1, \ldots, X_n]$. Si P est stable par toute permutation des indéterminées X_i, alors P est un polynôme en les polynômes symétriques élémentaires (la réciproque étant claire).*

$$R[X_1, \ldots, X_n]^{\mathcal{S}_n} = R[\sigma_1, \ldots, \sigma_n] \qquad \text{avec} \qquad \sigma_i = \sum_{1 \leq j_1 < \cdots < j_i \leq n} X_{j_1} \ldots X_{j_i}$$

Deux stratégies totalement différentes sont couramment utilisées pour réaliser ces calculs. La première est plutôt numérique, c'est-à-dire qu'elle utilise les nombres flottants. Elle se restreint donc aux sous-anneaux de $\mathbb{C}$. Cependant tous les calculs se font très rapidement, même si le nombre de décimales utilisées est important. C'est ainsi que l'on peut déterminer avec une marge d'erreur suffisamment petite les racines $\theta_i \in \mathbb{C}$ du polynôme f, puis effectuer tout calcul dans un ensemble proche de $R[\theta_1, \ldots, \theta_n]$. Un résultat suffisamment précis indiquera le résultat réel de l'évaluation en les racines θ_i. Cette méthode a été introduite par R.P. Stauduhar, et récemment concrétisée par H. Cohen, M. Olivier, et Y. Eichenlaub avec le logiciel de calcul formel Pari.

La seconde méthode est basée sur le calcul formel, qui peut s'utiliser sur des anneaux a priori quelconques. L'inconvénient de ce genre de méthode est de ne pas être très expéditive lorsque l'on veut faire des calculs laborieux. Ceci est dû au manque d'hypothèses sur l'anneau de base. Bien sûr ce point faible est contrebalancé par sa cause même : l'avantage de travailler avec des anneaux quelconques se révèle intéressant, voire indispensable... Pour accélérer les calculs, on utilise généralement des algorithmes supposant par exemple que R est infini, de caractéristique nulle, intègre, etc...

Je me suis intéressé plus particulièrement au calcul du groupe de Galois d'un polynôme f sur un corps K quelconque. Pour déterminer un groupe, il existe une technique s'appuyant sur la connaissance des actions de ce groupe sur différents ensembles bien choisis. Dans le cadre de la recherche du groupe de Galois, cela se fait par la factorisation de certains polynômes (appelés résolvantes). Il a été démontré par J.M. Arnaudiès et A. Valibouze que cette méthode est déterministe pour un groupe fini (voir [61]).

Une grosse partie du problème est de pouvoir calculer efficacement ces résolvantes, car celles-ci ont une définition liée aux racines θ_i du polynôme f, qui sont bien sûr inconnues... Pour ce genre de calculs, il y a, nous l'avons vu, au moins deux façons de s'y prendre : le calcul numérique et le calcul formel.

L'algèbre de décomposition universelle devait dans un premier temps servir d'outil pour réaliser formellement de tels calculs. Sa mise en œuvre en machine (en Axiom par exemple) est un exercice intéressant, et surtout permet (plus ou moins efficacement) de calculer toute expression symétrique des racines θ_i d'un polynôme unitaire f, sans algorithme particulier... En considérant cette algèbre comme un outil informatique, mais aussi et surtout mathématique, on s'aperçoit qu'elle apporte une couche algébrique (peut-être non négligeable) à la théorie purement "groupiste" (ou "groupistique") qui est développée dans la méthode classique de calcul de groupes de Galois par factorisation des résolvantes : nous évoquerons les notions d'algèbre étale, d'élément primitif, de relèvement d'idéaux, de groupe de décomposition, etc...

Les qualités de l'algèbre de décomposition universelle m'ont amené à changer mon fusil d'épaule : par exemple, mon but n'est plus de calculer le groupe de Galois de f en tant que tel, mais de réaliser un corps de décomposition de f.

En fait l'algèbre de décomposition universelle d'un polynôme f séparable sur un corps K est un produit (fini) de corps de décomposition de f. De plus, elle fait partie des algèbres galoisiennes, ce qui laisse entrevoir des propriétés semblables à celles connues en théorie de Galois classique.

II.1 Décomposition et universalité

Pour calculer une expression polynomiale symétrique $P(\theta_1, \ldots, \theta_n)$ en les racines θ_i d'un polynôme

$$f(T) = T^n - a_1 T^{n-1} + \cdots + (-1)^n a_n$$

on peut bien sûr utiliser le théorème II.0.1 : il suffit d'exprimer P dans $R[\sigma_1, \ldots, \sigma_n]$ puis de substituer les a_i aux σ_i.

Ceci permet effectivement de calculer toute expression symétrique des racines de f. Cependant il est peut-être coûteux de travailler dans des extensions telles $R[X_1, \ldots, X_n]$ et $R[\sigma_1, \ldots, \sigma_n]$... Une idée consiste à effectuer l'évaluation des polynômes symétriques avant même de commencer tout calcul : soit

$$\Sigma_f = \{\sigma_i - a_i,\ i = 1..n\}$$

alors la substitution $\sigma_i \mapsto a_i$ est équivalente au passage modulo $\langle \Sigma_f \rangle$, où $\langle \Sigma_f \rangle$ est le noyau du morphisme d'évaluation $\sigma_i \mapsto a_i$. Ainsi, au lieu de passer successivement un polynôme symétrique P de $R[X_1, \ldots, X_n]$ dans $R[\sigma_1, \ldots, \sigma_n]$ puis d'évaluer, il suffira de connaître la classe de P modulo $\langle \Sigma_f \rangle$.

$$\begin{array}{rcl} R[\sigma_1, \ldots, \sigma_n] & \hookrightarrow & R[X_1, \ldots, X_n] \\ \downarrow & & \downarrow \\ R \simeq R[\sigma_1, \ldots, \sigma_n]/\langle \Sigma_f \rangle & \to & R[X_1, \ldots, X_n]/\langle \Sigma_f \rangle \end{array}$$

La condition impérative, pour être capable de calculer une expression symétrique en les racines de f dont le résultat appartient à R, est de connaître les classes des éléments de R : en effet si P appartient à $R[X_1, \ldots, X_n]^{\mathcal{S}_n}$ alors sa classe modulo $\langle \Sigma_f \rangle$ est la classe de $P(\theta_1, \ldots, \theta_n) \in R$.

Définition II.1.1 (voir [13] pages 68-70, ou [48]) *On appelle* ***algèbre de décomposition universelle****, et l'on note $\mathbb{D}_R^f$, la R-algèbre $R[X_1, \ldots, X_n]/\langle \Sigma_f \rangle$.*

On note désormais x_i l'élément $\overline{X_i} = X_i \mod \langle \Sigma_f \rangle$ de $\mathbb{D}_R^f$.

Théorème II.1.1 *Soit $f \in R[T]$ unitaire de degré n. Dans $\mathbb{D}_R^f[T]$, $f(T)$ se factorise en*

$$f(T) = \prod_{i=1}^{n} (T - x_i)$$

Démonstration Soit $g(T)$ le polynôme générique unitaire de degré n,

$$g(T) = T^n - \sigma_1 T^{n-1} + \cdots + (-1)^n \sigma_n = \prod_{i=1}^{n} (T - X_i) \tag{II.1}$$

Quand on "quotiente" $R[X_1, \ldots, X_n]$ par l'idéal engendré par $\Sigma_f = \{\sigma_i - a_i \mid i = 1..n\}$, on trouve effectivement $f(T) = \prod_{i=1}^{n} (T - x_i)$. □

Le théorème suivant révèle que l'algèbre de décomposition est universelle pour la propriété de factorisation de f.

Théorème II.1.2 *Soit $u : R \to R'$ un morphisme d'anneaux et $f \in R[T]$ unitaire. On pose $f_u = u(f)$ et on suppose qu'il existe n éléments de R', $\theta_1, \ldots, \theta_n$, tels que*

$$f_u(T) = \prod_{i=1}^{n} (T - \theta_i)$$

Alors il existe un unique morphisme $U : \mathbb{D}_R^f \to R'$ prolongeant u et tel que $U(x_i) = \theta_i$.

Démonstration Posons $f = T^n - a_1 T^{n-1} + \cdots + (-1)^n a_n$. On commence par prolonger le morphisme d'anneaux u en l'application

$$\begin{array}{rcl} R[X_1, \ldots, X_n] & \longrightarrow & R' \\ X_i & \longmapsto & \theta_i \end{array}$$

L'image de $\sigma_i(X_1,\dots,X_n)-a_i$ par cette nouvelle application est $\sigma_i(\theta_1,\dots,\theta_n)-u(a_i)$, qui est nulle car $f_u(T)=\prod_{i=1}^n(T-\theta_i)$. Cette application passe donc au quotient et devient $U : \mathbb{D}_R^f \to R'$ tel que $U(x_i)=\theta_i$.

Le morphisme d'anneaux U est unique car $\mathbb{D}_R^f$ est engendré par R et les x_i. □

Remarque. Si certains x_i sont égaux (ce qui peut effectivement avoir lieu mais dans un seul cas, voir corollaire II.1.1) alors les θ_i sur lesquels sont envoyés ces x_i sont nécessairement égaux.

Théorème II.1.3 *L'algèbre $R[X_1,\dots,X_n]$ est libre de type fini sur $R[\sigma_1,\dots,\sigma_n]$, de rang $n!$. La famille $X_1^{k_1}\cdots X_n^{k_n}$ avec $0\le k_j<j$ et $1\le j\le n$ forme une base du module $R[X_1,\dots,X_n]$ sur $R[\sigma_1,\dots,\sigma_n]$.*

Démonstration par récurrence sur n : si $n=1$, le résultat est trivial ; si $n>1$, on note σ'_i le polynôme symétrique élémentaire homogène de degré i en les $n-1$ premières indéterminées $X_1,\dots,X_{n-1}$.

Il est facile de démontrer $R[\sigma'_1,\dots,\sigma'_{n-1},X_n]=R[\sigma_1,\dots,\sigma_n,X_n]$ en utilisant les formules $\sigma_i=\sigma'_i+\sigma'_{i-1}X_n \quad (\sigma'_0=1)$.

L'algèbre $R[\sigma_1,\dots,\sigma_n,X_n]$ sur $R[\sigma_1,\dots,\sigma_n]$ est isomorphe à $R[\sigma_1,\dots,\sigma_n][T]/(g)$ où g est le polynôme générique unitaire de degré n (équation II.1). En effet, X_n est une racine de $g(T)$ et si un polynôme P appartenant à $R[\sigma_1,\dots,\sigma_n][T]$ est annulé par X_n alors il l'est aussi par tous les X_i ($\mathcal{S}_n$ agit transitivement sur les X_i tout en laissant fixe P), ce qui a pour conséquence que $g(T)=\prod_i(T-X_i)$ divise P (quels que soient $i\neq j$, X_j-X_i n'est pas un diviseur de zéro dans $R[X_1,\dots,X_n]$). Ainsi $g(T)$ engendre l'idéal des polynômes s'annulant en X_n.

La base canonique de $R[\sigma_1,\dots,\sigma_n,X_n]$ sur $R[\sigma_1,\dots,\sigma_n]$ est donc X_n^j avec $0\le j<n$. Par hypothèse de récurrence, la famille $X_1^{k_1}\dots X_{n-1}^{k_{n-1}}$ avec $0\le k_j<j$ forme une base de $R[X_n][X_1,\dots,X_{n-1}]$ sur $R[X_n][\sigma'_1,\dots,\sigma'_{n-1}]$. En multipliant les deux bases, on obtient le résultat pour $R[X_1,\dots,X_n]$ sur $R[\sigma_1,\dots,\sigma_n]$. □

Lemme II.1.1 *Soit M un R-module libre de base $\mathcal{B}$, I un idéal de R. Alors M/IM est un R/I-module de base $\mathcal{B}$ mod I.*
En particulier, si M est une R-algèbre libre et si 1 fait partie de la base $\mathcal{B}$, alors R/I s'injecte dans M/IM par r mod $I\mapsto r.1$ mod IM.

Démonstration Le fait que $\mathcal{B}$ soit un système générateur de M a pour conséquence que $\mathcal{B}$ mod I l'est pour M/IM en tant que R/I-module.

Il reste à montrer que $\mathcal{B}$ mod I est une famille libre sur R/I. Soit une relation de dépendance entre les éléments de $\mathcal{B}$ mod I : $\overline{\lambda_i}\in R/I$, $\overline{b_i}\in\mathcal{B}$ mod I, $\sum_{\text{finie}}\overline{\lambda_i b_i}=0$ se remonte en $\sum_{\text{finie}}\lambda_i b_i\in IM=\sum_{\text{finie}}I.b_i$. Comme les b_i sont libres, les λ_i sont tous dans I, et donc nuls modulo I. □

Théorème II.1.4 *Quels que soient l'anneau commutatif R et $f\in R[T]$ unitaire, $\mathbb{D}_R^f$ est libre de type fini, de rang $n!$ et de R-base $x_1^{k_1}\cdots x_n^{k_n}$ avec $0\le k_j<j$. En outre R s'injecte dans $\mathbb{D}_R^f$.*

Démonstration On sait que $X_1^{k_1} \cdots X_n^{k_n}$ avec $0 \leq k_j < j$ est une base de $R[X_1, \ldots, X_n]$ sur $R[\sigma_1, \ldots, \sigma_n]$. On a posé $\Sigma_f = \{\sigma_1 - a_1, \ldots, \sigma_n - a_n\}$. Alors $X_1^{k_1} \cdots X_n^{k_n} \mod \langle \Sigma_f \rangle$ est une base de $R[x_1, \ldots, x_n]$ sur R. □

Corollaire II.1.1 *On sait que les $x_1, \ldots, x_{n-1}$ sont des éléments distincts de $\mathbb{D}_R^f$ (ils sont même linéairement indépendants sur R...). Cependant, x_n peut être égal à l'un d'entre eux : le seul cas où cela est réalisé est le cas où* $\mathrm{carac}(R) = 2$ *et $f(T) = T^2 + a_2$ (on a alors $x_1 = x_2$).*

Démonstration Si on suppose que x_n est égal à l'un des autres x_i :

$$x_{i_0} = x_n = a_1 - x_1 - \cdots - x_{n-1}$$

Comme les $1, x_1, \ldots, x_{n-1}$ sont linéairement indépendants, il s'en suit que $a_1 = 0, n-1 = 1$ et $-1 = 1$, c'est-à-dire $\mathrm{carac}(R) = 2$ et $f(T) = T^2 + a_2$. Il est alors facile de constater que dans ce cas on a bien $x_1 = x_2$. □

II.2 Approche algorithmique

Définition II.2.1 *Soit f un polynôme unitaire non constant et considérons $R[X]/(f)$. On dit que $\overline{X}$ est la* ***racine canonique*** *de f sur R.*

En effet, en plongeant R dans $R[X]/(f)$, on crée un zéro de f car $f(T) = (T - \overline{X})g(T)$ avec $g(T) \in \frac{R[X]}{(f)}[T]$. En répétant l'opération avec g, on crée la racine canonique de g, qui devient aussi une racine de f... En répétant l'opération n fois, on "invente" ainsi une factorisation de f.

En fait on construit une famille de polynômes $M_n, \ldots, M_1$ où chaque *modulus* M_i est défini par

$$M_n(X_n) = f(X_n) \qquad \text{et}$$

$$M_i(X_n, \ldots, X_i) = \left[M_{i+1}(X_n, \ldots, X_{i+2}, X_i) - M_{i+1}(X_n, \ldots, X_{i+2}, X_{i+1})\right](X_i - X_{i+1})^{-1}$$

Il faut remarquer que les polynômes M_i ont une structure échelonnée, c'est-à-dire que M_i (de degré i) appartient à $R[X_i, \ldots, X_n] \setminus R[X_{i+1}, \ldots, X_n]$. Ceci va être essentiel pour la construction algorithmique de $\mathbb{D}_R^f$. En effet cette construction se fera comme suit :

$$\begin{aligned} A_n &= R[X_n]/\langle M_n \rangle \\ A_{n-1} &= A_n[X_{n-1}]/\langle M_{n-1} \rangle \\ &\vdots \\ A_1 &= A_2[X_1]/\langle M_1 \rangle = R[X_1, \ldots, X_n]/M \end{aligned}$$

où M l'idéal engendré par tous les *moduli*. Finalement $\mathbb{D}_R^f = A_1$ (théorème II.2.1).

Ces *moduli* M_i forment en fait une base de Gröbner réduite de l'idéal $\langle \Sigma_f \rangle$ pour plusieurs ordres (lexicographique ou lexicographique gradué ou lexicographique gradué inverse, par exemple...) en écrivant les monômes de cette façon : $X_1^? X_2^? \cdots X_n^?$. (On a alors $X_1 > X_2 > \cdots > X_n$ pour les trois ordres ci-dessus.) Les M_i sont appelés également

modules de Cauchy, ou même les **différences divisées d'ordre** $n-i$ du polynôme f pour i parcourant $\{1,\ldots,n\}$ (voir [36], pages 13-18).

On rappelle que f se factorise dans A_1 : $f(T) = (T-\overline{X_n})\ldots(T-\overline{X_1})$. En effet $\overline{X_n} \in A_n$ est la racine canonique de f sur R, $\overline{X_{n-1}} \in A_{n-1}$ est la racine canonique de $\frac{f(T)}{T-\overline{X_n}}$ sur A_n, etc.

Lemme II.2.1 *Les idéaux $\langle\Sigma_f\rangle$ et M de $R[X_1,\ldots,X_n]$ sont égaux.*

Démonstration Dans l'anneau $R' = R[X_1,\ldots,X_n]/M$, f se factorise en

$$f(T) = \prod_{i=1}^{n} \left(T-\overline{X_i}\right)$$

(histoire de racines canoniques). De plus R s'injecte canoniquement dans R'. En utilisant le théorème II.1.2 on sait qu'il existe un morphisme de $\mathbb{D}_R^f = R[X_1,\ldots,X_n]/\langle\Sigma_f\rangle$ dans R'. Le morphisme suivant convient tout-à-fait :

$$\begin{array}{rcl} \mathbb{D}_R^f & \longrightarrow & R' \\ x_i & \longmapsto & \overline{X_i} \end{array}$$

Ce morphisme canonique est surjectif car l'algèbre R' est engendrée sur R par les $\overline{X_i}$.

Or nous savons que $\mathbb{D}_R^f$ est une R-algèbre libre de dimension $n!$. Il est facile de voir que R' l'est également : R' est construite par une tour d'algèbres A_i/A_{i+1} libres les unes sur les autres, respectivement de rang i, pour i parcourant $\{1,\ldots,n\}$.

Ainsi le morphisme canonique ci-dessus est un morphisme surjectif entre deux algèbres libres de même rang : il s'agit d'un isomorphisme. Finalement les idéaux $\langle\Sigma_f\rangle$ et M sont égaux. □

Le théorème suivant découle naturellement du lemme.

Théorème II.2.1 *Quels que soient R et $f \in R[T]$ unitaire, $\mathbb{D}_R^f = R[X_n,\ldots,X_1]/M$ où M est l'idéal engendré par les modules de Cauchy.*

Pour mettre en œuvre le domaine $\mathbb{D}_R^f$ en machine, on tiendra compte de ces propriétés. Informatiquement, il est possible de construire $R[X_n,\ldots,X_1]/M$. Mathématiquement, il est souvent plus intéressant de considérer $R[X_n,\ldots,X_1]/\langle\Sigma_f\rangle$.

Application. Il est maintenant possible d'illustrer de façon effective le théorème II.0.1. Grâce au théorème précédent, on a l'algorithme simple suivant :

initialisation :
$X_1, \ldots, X_n, T$ indéterminées sur R
$f(T) := T^n - a_1 T^{n-1} + \cdots + (-1)^n a_n \in R[T]$
$M_n := f(X_n)$
for $i := n$ to 2 do
$$M_{i-1} := \frac{M_i(X_n, \ldots, X_{i+1}, X_{i-1}) - M_i(X_n, \ldots, X_{i+1}, X_i)}{X_{i-1} - X_i}$$

utilisation :
entrée : $P \in R[X_1, \ldots, X_n]$ symétrique en les X_i.
sortie : l'évaluation de P en les racines de f

for $i := 1$ to n do (ici, $P \in R[X_i, \ldots, X_n]$)
$P := \text{remainder}_{X_i}(P, M_i)$
return P

Pour donner un exemple, lorsque $f = T^4 - a_1 T^3 + a_2 T^2 - a_3 T + a_4$, les modules de Cauchy sont :

$$\begin{aligned}
M_4 &= X_4^4 - a_1\ X_4^3 + a_2\ X_4^2 - a_3\ X_4 + a_4 \\
M_3 &= (X_3^3 + X_3^2\ X_4 + X_3\ X_4^2 + X_4^3) - (X_3^2 + X_3\ X_4 + X_4^2)\ a_1 + (X_3 + X_4)\ a_2 - a_3 \\
M_2 &= (X_2^2 + X_2\ X_3 + X_2\ X_4 + X_3^2 + X_3\ X_4 + X_4^2) - (X_2 + X_3 + X_4)\ a_1 + a_2 \\
M_1 &= (X_1 + X_2 + X_3 + X_4) - a_1
\end{aligned}$$

Nous pouvons alors remarquer que le module de Cauchy M_i est un polynôme symétrique en $X_i, \ldots, X_4$. Plus précisément, M_i est une combinaison linéaire de polynômes homogènes complets de degré $j \in \{0, \ldots, i\}$ symétriques en $X_i, \ldots, X_4$, dont les facteurs sont les coefficients a_{i-j} de f ($a_0 = 1$). Ces remarques se généralisent bien sûr à n'importe quel degré de f.

Le résultat de ce dernier théorème est intéressant car il donne une vision particulière de $\mathbb{D}_R^f$: en effet la R-algèbre $\mathbb{D}_R^f$ peut être considérée comme une tour d'algèbres montées les unes sur les autres :

$$R = A_{n+1} \subset A_n \subset \cdots \subset A_2 \subset A_1 = \mathbb{D}_R^f$$

ou encore, de manière récursive,

$$\begin{aligned}
\mathbb{D}_R^f &= R[X_1]/(f) \quad \text{si } \deg(f) = 1 \\
\mathbb{D}_R^f &= \mathbb{D}_{R[X_n]/(f)}^g \quad \text{si } n = \deg(f) > 1 \text{ et } g(T) = \tfrac{f(T)}{T - \overline{X_n}}
\end{aligned}$$

Cette vision de tour montre par une rapide récurrence que $R[x_n, \ldots, x_l]$ est une algèbre libre sur $R[x_n, \ldots, x_j]$ (où $j \geq l$), de base canonique $x_l^{k_l} \ldots x_{j-1}^{k_{j-1}}$ avec $0 \leq k_i < i$ et $i \in \{l, \ldots, j-1\}$. En particulier, on retrouve le résultat du théorème II.1.4 en posant $j = n+1$ et $l = 1$.

Corollaire II.2.1 *Quels que soient R et f, considérons deux sous-algèbres de $\mathbb{D}_R^f$ particulières : $R[x_n,\ldots,x_l]$ et $R[x_n,\ldots,x_j]$ où $j \geq l$. Alors $R[x_n,\ldots,x_l]$ est une algèbre libre sur $R[x_n,\ldots,x_j]$, de rang $\frac{(j-1)!}{(l-1)!}$ et de base canonique $x_l^{k_l}\ldots x_{j-1}^{k_{j-1}}$ où $0 \leq k_i < i$ et $i \in \{l,\ldots,j-1\}$.*

Propriété II.2.1 *Quels que soient l'anneau R et le polynôme f de degré $n \geq 2$, le discriminant de la base canonique de la R-algèbre libre $\mathbb{D}_R^f$ est $\mathrm{dis}(f)^{\frac{n!}{2}}$.*

Démonstration par récurrence sur n. Si $n = 2$ alors le résultat est trivial car

$$\mathbb{D}_R^f = R[x_1] \simeq R[T]/(f) \qquad \text{et} \qquad \mathrm{dis}_R\, R[T]/(f) = \mathrm{dis}(f)$$

Si l'hypothèse de récurrence est admise pour un certain rang $n-1 \geq 2$, montrons qu'elle est réalisée au rang n. Pour cela considérons un polynôme unitaire f de degré n et son algèbre de décomposition universelle $\mathbb{D}_R^f = R[x_1,\ldots,x_n]$ sur l'anneau R. Si nous posons

$$g(T) = \frac{f(T)}{T - x_n} \in R[x_n]$$

alors $\mathbb{D}_R^f$ est l'algèbre de décomposition universelle de g sur $R[X_n]$. Par hypothèse (de récurrence), le discriminant de la base canonique de $\mathbb{D}_{R[x_n]}^g = \mathbb{D}_R^f$ est $\mathrm{dis}(g)^{\frac{(n-1)!}{2}}$ car g est de degré $n-1$.

Or $\mathbb{D}_R^f$ est libre sur $R[x_n]$, qui est elle-même libre sur R. Il suffit à présent d'utiliser la formule de "transitivité" des discriminants (voir [47], page 60).

$$\mathrm{dis}_R\, \mathbb{D}_R^f = \mathrm{Norm}_{R[x_n]/R}\left(\mathrm{dis}_{R[x_n]}\, \mathbb{D}_R^f\right) \,.\, \left(\mathrm{dis}_R\, R[x_n]\right)^{\dim_{R[x_n]}\mathbb{D}_R^f}$$

Nous connaissons les égalités suivantes : $\mathrm{dis}_{R[x_n]}\, \mathbb{D}_R^f = \mathrm{dis}(g)^{\frac{(n-1)!}{2}}$, $\mathrm{dis}_R\, R[x_n] = \mathrm{dis}(f)$ et $\dim_{R[x_n]}\mathbb{D}_R^f = (n-1)!$. Il ne nous reste plus qu'à calculer $\mathrm{Norm}_{R[x_n]/R}(\mathrm{dis}(g))$. Or le discriminant de g est $\prod_{1\leq i<j<n}(x_i - x_j)^2$, si bien que

$$\mathrm{Norm}_{R[x_n]/R}(\mathrm{dis}(g)) = \prod_{k=1}^{n}\prod_{i<j<n}(k,n).(x_i-x_j)^2 = \prod_{1\leq i<j\leq n}(x_i-x_j)^{2(n-2)} = \mathrm{dis}(f)^{n-2}$$

Finalement, nous obtenons $\mathrm{dis}_R\, \mathbb{D}_R^f = \mathrm{dis}(f)^{(n-2)\frac{(n-1)!}{2}}\mathrm{dis}(f)^{(n-1)!} = \mathrm{dis}(f)^{\frac{n!}{2}}$. L'hypothèse de récurrence est bien vérifiée au rang n. □

II.3 Changement d'anneau de base

Propriété II.3.1 *Soit $\rho : R \to R'$ un morphisme d'anneaux, des polynômes $f \in R[X]$ unitaire et $f_\rho = \rho(f) \in R'[X]$. Il existe alors un morphisme unique $\tilde{\rho} : \mathbb{D}_R^f \to \mathbb{D}_{R'}^{f_\rho}$ prolongeant ρ et envoyant la base canonique de $\mathbb{D}_R^f$ sur celle de $\mathbb{D}_{R'}^{f_\rho}$.*

Démonstration Notons $\mathbb{D}_R^f = R[x_1, \ldots, x_n]$ et $\mathbb{D}_{R'}^{f_\rho} = R'[\theta_1, \ldots, \theta_n]$. On sait que f_ρ se factorise dans l'algèbre de décomposition universelle $\mathbb{D}_{R'}^{f_\rho}$: $f_\rho = (X - \theta_1) \cdots (X - \theta_n)$. On prolonge ρ par le morphisme composé $R \xrightarrow{\rho} R' \hookrightarrow \mathbb{D}_{R'}^{f_\rho}$. Le théorème II.1.2 nous dit qu'il existe un morphisme $\tilde{\rho} : \mathbb{D}_R^f \to \mathbb{D}_{R'}^{f_\rho}$ qui prolonge ρ et qui envoie x_i sur θ_i. Par conséquent $\tilde{\rho}$ est un morphisme d'algèbres qui envoie la base canonique de $\mathbb{D}_R^f$ sur celle de $\mathbb{D}_{R'}^{f_\rho}$. □

Corollaire II.3.1 *Soit R' une R-algèbre et $f \in R[X]$ unitaire non constant. On note encore f le polynôme $1 \otimes f \in R' \otimes_R R[X] = R'[X]$. Alors $\mathbb{D}_{R'}^f \simeq \mathbb{D}_R^f \otimes_R R'$.*

Démonstration Tout vient du fait que $\mathbb{D}_R^f$ est une R-algèbre libre : le morphisme allant de $\mathbb{D}_R^f$ dans $\mathbb{D}_R^f \otimes R'$ envoie la base canonique de $\mathbb{D}_R^f$ sur la base canonique de $\mathbb{D}_R^f \otimes R'$. □

Si l'on préfère ne pas utiliser le produit tensoriel, on peut redémontrer rapidement à la main le corollaire suivant à l'aide de la propriété II.3.1 :

Corollaire II.3.2 *Avec les mêmes notations que la propriété II.3.1,*

$$\rho : R \to R' \qquad \text{et} \qquad \tilde{\rho} : \mathbb{D}_R^f \to \mathbb{D}_{R'}^{f_\rho}$$

On pose $\mathbb{D}_{R'}^{f_\rho} = R'[\theta_1, \ldots, \theta_n]$. L'image de $\tilde{\rho}$ est $\rho(R)[\theta_1, \ldots, \theta_n]$ et son noyau est $\ker(\rho).\mathbb{D}_R^f$. Par conséquent si ρ est injectif ou surjectif alors il en est de même pour $\tilde{\rho}$.

De plus, $\tilde{\rho}\left(\mathbb{D}_R^f\right) \cap R' = \rho(R)$.

Propriété II.3.2 *Soit R un anneau, $(R_i)_i$ une famille de R-algèbres, et f un polynôme unitaire de $R[X]$. On pose $f_i = f \otimes 1_{R_i} \in R_i[X]$. Alors $\mathbb{D}_R^f \otimes (\prod_i R_i) \simeq \prod_i \mathbb{D}_{R_i}^{f_i}$.*

Démonstration Cette propriété est le corollaire d'un théorème classique du produit tensoriel entre un produit de R-modules et un R-module libre de type fini. En effet si les $(E_i)_i$ sont des R-modules et F un R-module libre alors le morphisme canonique $F \otimes (\prod_i E_i) \to \prod_i (F \otimes E_i)$ est injectif ; si de plus F est de type fini, alors ce morphisme est bijectif. □

Corollaire II.3.3 *Avec les mêmes notations, si $\rho : R \to \prod_i R_i$ est un morphisme injectif (respectivement surjectif) alors il existe un unique morphisme injectif (respectivement surjectif) $\tilde{\rho}$ prolongeant ρ de $\mathbb{D}_R^f$ dans $\prod_i \mathbb{D}_{R_i}^{f_i}$.*

II.4 Action du groupe symétrique

Il est facile de voir que $\mathcal{S}_n$ agit sur $\mathbb{D}_R^f$ car $\mathcal{S}_n$ opère sur $R[X_1, \ldots, X_n]$ par permutation des indéterminées tout en laissant stable l'idéal $\langle \Sigma_f \rangle$, puisque celui-ci est engendré par des polynômes symétriques. L'action de $\mathcal{S}_n$ passe directement sur le quotient

$$R[X_1, \ldots, X_n]/\langle \Sigma_f \rangle = \mathbb{D}_R^f$$

D'un autre coté, on peut construire un morphisme de $\mathcal{S}_n$ dans $\mathrm{Aut}_R\, \mathbb{D}_R^f$. En effet, grâce au théorème II.1.2, en posant $R' = \mathbb{D}_R^f$, $u : R \hookrightarrow \mathbb{D}_R^f$, et $\theta_i = x_{\sigma(i)}$ ($\sigma \in \mathcal{S}_n$) on voit qu'il existe un R-endomorphisme U_σ de $\mathbb{D}_R^f$ qui envoie x_i sur $x_{\sigma(i)}$. En fait U_σ est un automorphisme dont l'application réciproque est $U_{\sigma^{-1}}$.

Propriété II.4.1 *L'action de $\mathcal{S}_n$ sur les x_i est toujours transitive. Elle est aussi fidèle sauf dans le cas où* $\mathrm{carac}(R) = 2$ *et* $f = X^2 + c$.

Démonstration voir le corollaire II.1.1 □

II.4.a L'égalité $\left(\mathbb{D}_R^f\right)^{\mathcal{S}_n} = R$

Nous allons étudier les éléments fixés par l'action de $\mathcal{S}_n$. Deux démonstrations du théorème II.4.1 seront données : la première est uniquement algébrique, sans calcul, et fait appel au lemme qui suit ; la seconde est faite "sur mesure" pour l'algèbre de décomposition universelle et demande juste un petit calcul.

Lemme II.4.1 *Soit R' un anneau quelconque et $f(T) = (T-\theta_1)\dots(T-\theta_n)$ avec $\theta_i \in R'$. Si* $\mathrm{dis}(f)$ *est inversible dans R' alors $\mathbb{D}_{R'}^f$ et $\prod_{\tau\in\mathcal{S}_n} R'$ sont isomorphes en tant que R'-algèbres à groupe d'opérateurs $\mathcal{S}_n$. Par suite $\left(\mathbb{D}_{R'}^f\right)^{\mathcal{S}_n} = R'$.*

Démonstration Posons $\theta = (\theta_1, \dots, \theta_n)$ et considérons le $\mathcal{S}_n$-morphisme de R'-algèbres

$$\begin{array}{rccc} \phi & : & R'[X_1,\dots,X_n] & \longrightarrow & \prod_{\mathcal{S}_n} R' \\ & & P & \longmapsto & \big((\tau P)(\theta)\big)_{\tau\in\mathcal{S}_n} \end{array}$$

Le noyau de ϕ est l'ensemble des polynômes qui s'annulent en $\big(\theta_{\tau(1)},\dots,\theta_{\tau(n)}\big)$ pour toute permutation $\tau \in \mathcal{S}_n$. Or un polynôme s'annule en un tel n-uplet si et seulement s'il appartient à l'idéal $I_\tau \subset R'[X_1,\dots,X_n]$ engendré par $\{X_1-\theta_{\tau(1)},\dots,X_n-\theta_{\tau(n)}\}$. Ainsi $\ker\phi = \cap_\tau I_\tau$, et on voit qu'il contient l'idéal engendré par $\Sigma_f = \{\sigma_1 - a_1, \dots, \sigma_n - a_n\}$ (où les σ_i sont les polynômes symétriques élémentaires et $f = T^n - a_1T^{n-1} + \dots + (-1)^n a_n$). Donc le morphisme ϕ passe au quotient et on définit un nouveau morphisme

$$\overline{\phi} \ : R'[X_1,\dots,X_n]/\langle\Sigma_f\rangle = \mathbb{D}_{R'}^f \longrightarrow \prod_{\mathcal{S}_n} R'$$

Montrons que $\overline{\phi}$ ainsi défini est un isomorphisme. En fait, il suffit de démontrer que $\overline{\phi}$ est surjectif, et pour des raisons d'égalité de rangs on aura l'isomorphie. Par hypothèse, on sait que $\mathrm{dis}(f)$ est inversible dans R', ce qui a pour effet que les idéaux $(I_\tau)_{\tau\in\mathcal{S}_n}$ sont co-maximaux deux à deux : en effet, si $\tau \neq \tau'$ alors il existe $i \in \{1,\dots,n\}$ tel que

$$\theta_{\tau(i)} - \theta_{\tau'(i)} = \big(X_i - \theta_{\tau'(i)}\big) - \big(X_i - \theta_{\tau(i)}\big) \in I_\tau + I_{\tau'}$$

soit non nul, c'est-à-dire diviseur de $\mathrm{dis}(f)$, et donc inversible. Grâce au théorème chinois,

$$R'[X_1,\dots,X_n]/\ker(\phi) \simeq \prod_{\tau\in\mathcal{S}_n} R'[X_1,\dots,X_n]/I_\tau \simeq \prod_{\mathcal{S}_n} R'$$

où les isomorphismes de R'-algèbres ci-dessus sont compatibles avec l'action de $\mathcal{S}_n$.

Par conséquent $\overline{\phi}$ est surjectif, et donc bijectif. Remarquer que l'on a démontré :

$$\ker(\phi) = \bigcap_{\tau\in\mathcal{S}_n} I_\tau = \prod_{\tau\in\mathcal{S}_n} I_\tau = \langle\Sigma_f\rangle$$

L'intersection des idéaux I_τ est égale à leur produit car ceux-ci sont comaximaux 2 à 2.

De plus, l'application $\overline{\phi}$ est compatible avec l'action de $\mathcal{S}_n$: en effet $\overline{\phi}(\tau P)$ et $\tau\overline{\phi}(P)$ coïncident. Alors le fait que $P \in \mathbb{D}^f_{R'}$ soit invariant sous l'action de $\mathcal{S}_n$ est équivalent au fait que $\overline{\phi}(P)$ le soit. Or les éléments invariants de $\prod_{\mathcal{S}_n} R'$ sous l'action de $\mathcal{S}_n$ sont les vecteurs à coordonnées toutes égales, c'est-à-dire les images des éléments de R' par l'injection canonique $R' \hookrightarrow \prod_{\mathcal{S}_n} R'$ (qui est l'injection diagonale, ou encore le morphisme structural pour la structure de R'-algèbre). Comme $\overline{\phi}$ est un isomorphisme, l'ensemble des points fixes de $\mathbb{D}^f_{R'}$ sous l'action de $\mathcal{S}_n$ est R'. □

Théorème II.4.1 *Si R est un anneau quelconque et $f \in R[X]$ unitaire de discriminant régulier (non diviseur de 0) alors $\left(\mathbb{D}^f_R\right)^{\mathcal{S}_n} = R$.*

Première démonstration Soit $S = \{\mathrm{dis}(f)^k,\ k \in \mathbb{N}\}$. Le discriminant de f étant non diviseur de zéro, R s'injecte dans le localisé de R en S : $S^{-1}R = R[\mathrm{dis}(f)^{-1}]$, ce qui a pour effet de rendre le discriminant de f inversible. Dans l'algèbre de décomposition universelle de f sur $S^{-1}R$, f se factorise canoniquement en un produit de polynômes de degré 1 et son discriminant reste inversible. Posons $R' = \mathbb{D}^f_{S^{-1}R}$. Par le corollaire II.3.2, on sait que $\mathbb{D}^f_R$ s'injecte dans $\mathbb{D}^f_{R'}$ car R s'injecte dans $S^{-1}R$, qui lui-même s'injecte dans R'. Si $P \in \mathbb{D}^f_R$ est stable par l'action de $\mathcal{S}_n$ alors $P \in \left(\mathbb{D}^f_{R'}\right)^{\mathcal{S}_n}$, et grâce au lemme II.4.1, $P \in R'$. Or $P \in R' \cap \mathbb{D}^f_R = R$ en considérant le corollaire II.3.2. □

Deuxième démonstration par récurrence sur n (inspirée de [48], pages 46-47). On pose

$$f = X^n - a_1X^{n-1} + \cdots + (-1)^n a_n$$

- Si $n = 1$, le résultat est clair.

- Si $n = 2$: $f = X^2 - a_1X + a_0$. Soit $y \in \mathbb{D}^f_R$ stable par $\mathcal{S}_2$.

$$\lambda_1x_1 + \lambda_0 = y = (1,2)y = \lambda_1x_2 + \lambda_0 = -\lambda_1x_1 + \lambda_0 + \lambda_1a_1$$

Ceci implique $\lambda_1a_1 = 0$ et $\lambda_1 = -\lambda_1$, et donc $\lambda_1\,\mathrm{dis}(f) = \lambda_1(a_1^2 - 4a_0) = 0$. Comme f est séparable, $\lambda_1 = 0$ et $y \in R$.

- Si $n > 2$: soit $y \in \left(\mathbb{D}^f_R\right)^{\mathcal{S}_n}$ et $g(X) = \dfrac{f(X)}{X - x_n}$. Comme $\mathbb{D}^f_R = \mathbb{D}^g_{R[x_n]}$ (voir section II.2, après le théorème II.2.1), $y \in \left(\mathbb{D}^g_{R[x_n]}\right)^{\mathcal{S}_{n-1}}$. Le polynôme $g \in R[x_n][X]$ est séparable car $\mathrm{dis}(g)$ divise $\mathrm{dis}(f)$. Par récurrence, y appartient à $R[x_n]$: $y = \sum_{k=0}^{n-1} \lambda_k x_n^k$. Or y est invariant par la transposition $(n, n-1)$ donc

$$\sum_{k=0}^{n-1} \lambda_k x_n^k = (n,n-1).\sum_{k=0}^{n-1} \lambda_k x_n^k = \sum_{k=0}^{n-1} \lambda_k x_{n-1}^k = \lambda_{n-1}x_{n-1}^{n-1} + \sum_{k=0}^{n-2} \lambda_k x_{n-1}^k$$

Or $x_{n-1}^{n-1} = -x_n x_{n-1}^{n-2} + \cdots$ en $x_n^j x_{n-1}^k$ avec $k < n-2$ car $g(X) = X^{n-1} + x_n X^{n-2} + \cdots$ et $g(x_{n-1}) = 0$. Ainsi, nous obtenons

$$\sum_{k=0}^{n-1} \lambda_k x_n^k = \lambda_{n-1} x_{n-1}^{n-1} + \sum_{k=0}^{n-2} \lambda_k x_{n-1}^k = -\lambda_{n-1} x_n x_{n-1}^{n-2} + \cdots$$

Comme les $x_n^j x_{n-1}^k$ avec $j \leq n-1,\ k \leq n-2$ forment une famille libre et $n-2 > 0$, cette dernière égalité montre d'une part que $\lambda_{n-1} = 0$, et d'autre part que $\lambda_k = 0$ pour tout $k > 0$. Finalement $y = \lambda_0 \in R$. □

Corollaire II.4.1 *Si R est un anneau quelconque et $f \in R[X]$ unitaire dont le discriminant est inversible dans R alors $\mathbb{D}_R^f$ est une algèbre galoisienne sur R de groupe $\mathcal{S}_n$.*

Démonstration Nous savons déjà que R est l'ensemble des points de $\mathbb{D}_R^f$ invariants sous l'action de $\mathcal{S}_n$. Le polynôme f se décompose totalement dans l'anneau $R' = \mathbb{D}_R^f$. Le lemme II.4.1 nous donne également l'isomorphisme

$$\begin{array}{rcl} \mathbb{D}_R^f \otimes_R \mathbb{D}_R^f = \mathbb{D}_{R'}^f & \longleftrightarrow & \prod_{\mathcal{S}_n} R' = \prod_{\mathcal{S}_n} \mathbb{D}_R^f \\ P \otimes Q & \longmapsto & (P.\tau Q)_{\tau \in \mathcal{S}_n} \end{array}$$

On termine la preuve en utilisant le théorème I.1.2 (page 19). □

II.4.b Norme de $\mathbb{D}_R^f$ sur R

Revenons sur la vision de $\mathbb{D}_R^f$ abordée dans la section II.2. On y constate que $\mathbb{D}_R^f$ est une tour d'algèbres libres de rangs finis :

$$R \subset R[x_n] \subset R[x_n, x_{n-1}] \subset \cdots \subset R[x_n, \ldots, x_1] = \mathbb{D}_R^f$$

Le but de cette section est d'expliciter la norme d'un élément de $\mathbb{D}_R^f$ (on verra qu'il y a deux formules principales : le corollaire II.4.3 et la propriété II.4.3). Nous nous intéressons particulièrement à la norme car celle-ci nous permet de connaître le polynôme caractéristique de tout élément, et par suite sa révolvante et son polynôme minimal (voir le corollaire II.4.4 et la propriété II.5.1).

Propriété II.4.2 *Soit R un anneau quelconque, $f \in R[T]$ un polynôme unitaire non constant, et $x \in \mathbb{D}_R^f$. Alors $\chi_{\mathbb{D}_R^f : R}(x) = \mathrm{N}_{\mathbb{D}_{R[T]}^f : R[T]}(T - x)$.*

Démonstration Le foncteur $R \mapsto R[T]$ commute avec $R \mapsto \mathbb{D}_R^f = R[x_1, \ldots, x_n]$, si bien que $\chi_x(T) = \det(T - x\,\mathrm{Id}) = \mathrm{N}_{\mathbb{D}_{R[T]}^f : R[T]}(T - x)$. □

On rappelle que si $A \subset B \subset C$ sont trois anneaux tels que B soit une algèbre libre de rang fini sur A, de même pour C sur B, alors C est libre de rang fini sur A et

$$\mathrm{N}_{C:A} = \mathrm{N}_{B:A} \circ \mathrm{N}_{C:B} \qquad \mathrm{tr}_{C:A} = \mathrm{tr}_{B:A} \circ \mathrm{tr}_{C:B} \qquad \chi_{C:A} = \mathrm{N}_{B[T]:A[T]} \circ \chi_{C:B}$$

D'autre part si R est un sous-anneau de R', $f \in R[T]$ tel que $f(T) = (T-\theta_1)\cdots(T-\theta_n)$ où les θ_i appartiennent à R', alors pour tout $\overline{g} \in R[T]/(f)$,

$$\mathrm{N}_{R[T]/(f):R}(\overline{g}) = \mathrm{res}(f,g) = \prod_{i=1}^{n} g(\theta_i)$$

Voir [47], pages 39-62.

Par une récurrence facile on obtient le corollaire suivant :

Corollaire II.4.2 *Considérons une tour d'algèbres $R = A_0 \subset A_1 \subset \cdots \subset A_n$ définies par $A_i = A_{i-1}[X_i]/(f_i)$ et $f_i(X_i)$ est unitaire. Alors $A_n = R\left[\overline{X_1}, \ldots, \overline{X_n}\right]$ et pour $\overline{g} \in A_n$,*

$$\mathrm{N}_{A_n:R}(\overline{g}) = \mathrm{res}_{X_1}\left(f_1, \mathrm{res}_{X_2}\left(f_2, \ldots \mathrm{res}_{X_n}(f_n, g)\right)\right)$$

où g est un polynôme de $R[X_1, \ldots, X_n]$ dont la classe modulo l'idéal $\langle f_1, \ldots, f_n\rangle$ est $\overline{g}$.

Revenons plus particulièrement à l'algèbre de décomposition universelle :

Corollaire II.4.3 *Soit R un anneau quelconque, $f \in R[T]$ un polynôme unitaire non constant. Alors $\mathbb{D}_R^f = R[X_n, \ldots, X_1]/\langle f_n, \ldots, f_1\rangle$ où les f_i sont les modules de Cauchy (voir section II.2). Alors pour tout $\overline{g} \in \mathbb{D}_R^f$,*

$$\mathrm{N}_{\mathbb{D}_R^f:R}(\overline{g}) = \mathrm{res}_{X_n}\left(f_n, \mathrm{res}_{X_{n-1}}\left(f_{n-1}, \ldots \mathrm{res}_{X_1}(f_1, g)\right)\right)$$

Propriété II.4.3 *Soit R un anneau quelconque, $f \in R[T]$ un polynôme unitaire non constant, et $x \in \mathbb{D}_R^f$. Alors $\mathrm{N}_{\mathbb{D}_R^f:R}(x) = \prod_{\sigma\in\mathcal{S}_n} \sigma.x$.*

Démonstration par récurrence sur n. Si $n = 1$ alors le résultat est clair. Admettons qu'il soit vrai pour un certain entier $n-1$. Soit f un polynôme unitaire de degré n et $x \in \mathbb{D}_R^f$. On sait que $\mathrm{N}_{\mathbb{D}_R^f:R}(x) = \mathrm{N}_{R[x_n]:R} \circ \mathrm{N}_{\mathbb{D}_R^f:R[x_n]}(x)$. Or $\mathbb{D}_R^f = \mathbb{D}_{R[x_n]}^g$ où le polynôme $g = \frac{f(T)}{T-x_n}$, si bien que

$$\mathrm{N}_{\mathbb{D}_R^f:R[x_n]}(x) = \mathrm{N}_{\mathbb{D}_{R[x_n]}^g:R[x_n]}(x) = \prod_{\sigma\in\mathcal{S}_{n-1}} \sigma.x$$

en utilisant l'hypothèse de récurrence avec le polynôme $g \in R[x_n][T]$. Regardons maintenant la norme d'un élément de $R[x_n]$ sur R : cette norme est le produit des conjugués de cet élément : $\mathrm{N}_{R[x_n]:R}(P(x_n)) = \prod_{i=1}^n P(x_i) = \prod_{i=1}^n (i,n).P(x_n)$. Ainsi

$$\mathrm{N}_{\mathbb{D}_R^f:R}(x) = \prod_{i=1}^{n} \prod_{\sigma\in\mathcal{S}_{n-1}} (i,n).\sigma.x = \prod_{\sigma\in\mathcal{S}_n} \sigma.x$$

□

Cette propriété n'est pas surprenante. En effet nous avons vu le même genre de relation dans les algèbres galoisiennes libres : $\mathrm{N}(x) = \prod_{g\in G} g(x)$. Or $\mathbb{D}_R^f$ est une algèbre galoisienne libre si (et seulement si) le discriminant de f est inversible. Les deux résultats coïncident alors.

Cependant, la propriété II.4.3 nous permet de voir que la norme d'un élément x de $\mathbb{D}_R^f$ s'écrit toujours comme le produit de $\prod_{\sigma\in\mathcal{S}_n} \sigma.x$, et ce sans aucune hypothèse, ni sur le discriminant de f, ni sur R.

II.4.c Polynôme minimal et résolvante

Corollaire II.4.4 *Si R est un anneau intégralement clos et $f \in R[T]$ un polynôme unitaire de discriminant régulier (non diviseur de 0), alors le polynôme minimal de $x \in \mathbb{D}_R^f$ est la partie sans facteur carré de sa résolvante $\prod_{y \in S_n.x} (T - y)$.*

Démonstration Soit d le discriminant de f. Comme R est intégralement clos, l'anneau $R' = R[d^{-1}]$ l'est également, ce qui implique en particulier que la R'-algèbre galoisienne $\mathbb{D}_{R'}^f$ est réduite (corollaire I.5.1). On utilise le résultat du théorème I.6.2 pour conclure que le polynôme minimal de tout élément de $\mathbb{D}_{R'}^f$ sur R' est la partie sans facteur carré de sa résolvante. Enfin, le polynôme minimal de $x \in \mathbb{D}_R^f$ sur R est égal au polynôme minimal de x sur R' où x est vu comme un élément de $\mathbb{D}_{R'}^f$, car R est un anneau intégralement clos. □

Corollaire II.4.5 *Soit R un anneau intégralement clos et $f \in R[T]$ un polynôme unitaire de discriminant inversible. On considère un élément x de $A = \mathbb{D}_R^f$ dont le stabilisateur dans $\mathcal{S}_n$ est H. Si le discriminant de la résolvante g de x est inversible dans R, alors on a l'égalité $A^H = R[x]$.*

En particulier, deux résolvantes associées à un même sous-groupe H et dont les discriminants sont inversibles dans R sont images l'une de l'autre par une transformation de Tschirnhaus.

Démonstration Il faut bien sûr montrer l'inclusion non triviale $A^H \subset R[x]$. Nous rappelons que $A = \mathbb{D}_R^f$ est une algèbre galoisienne sur R car le discriminant de f est inversible dans R.

Soit $a \in A^H$ et l'idéal $I = \{r \in R \mid ra \in R[x]\}$ de R. Supposons que a n'appartienne pas à $R[x]$, c'est-à-dire $I \neq R$. Il existe donc un idéal maximal $\mathfrak{m}$ de R contenant I. Soit S la partie multiplicative $R \setminus \mathfrak{m}$. Localisons par S :

$$S^{-1}R = R_{\mathfrak{m}} \longrightarrow S^{-1}R[x] = R_{\mathfrak{m}}[x] \subset S^{-1}A^H = \left(S^{-1}A\right)^H \longrightarrow S^{-1}A = \mathbb{D}_{R_{\mathfrak{m}}}^f$$

Toutes les algèbres de ce diagramme sont libres sur l'anneau local $R_{\mathfrak{m}}$ (propriété des algèbres galoisiennes). Le rang de $R_{\mathfrak{m}}[x]/R_{\mathfrak{m}}$ est égal au degré du polynôme minimal de x sur $R_{\mathfrak{m}}$ (ou sur R). Or ce dernier n'est autre que la résolvante g de x car g est sans facteur carré (son discriminant n'est pas nul dans R). Ainsi $\dim_{R_{\mathfrak{m}}} R_{\mathfrak{m}}[x] = [S_n : H]$. Or ce nombre est également la dimension de $S^{-1}A^H$ sur $R_{\mathfrak{m}}$. Ainsi nous déduisons l'existence de la formule

$$\operatorname{dis} \mathcal{B}_x = \operatorname{dis} \mathcal{B}. \det(M)^2$$

où M est une matrice exprimant la $R - \mathfrak{m}$-base canonique $\mathcal{B}_x$ de $R_{\mathfrak{m}}[x]$ (formée par les premières puissances de x) dans une $R_{\mathfrak{m}}$-base $\mathcal{B}$ de $S^{-1}A^H$. Or $\operatorname{dis} \mathcal{B}_x = \operatorname{dis} g$ est inversible dans R (donc dans $R_{\mathfrak{m}}$), M est une matrice inversible et nous avons l'égalité $R_{\mathfrak{m}}[x] = S^{-1}A^H$.

Pour finir, dans $R_{\mathfrak{m}}[x] = S^{-1}A^H$, on peut écrire $\dfrac{a}{1} = \dfrac{p}{s}$ avec $p \in R[x]$ et $s \in S = R \setminus \mathfrak{m}$. Cela signifie qu'il existe $s' \in S$ tel que $s'(sa - p) = 0$ dans R, ou encore $s'sa \in R[x]$:

$s's$ appartient donc à I par définition. Or ceci est impossible car $s's \in S$ n'appartient pas à $\mathfrak{m}$... La supposition que nous avons faite est donc fausse : tout élément de A^H appartient à $R[x]$.

Si g_1 et g_2 sont les résolvantes de x_1 et x_2 associées à un même groupe H, ayant des discriminants inversibles dans R, alors nous avons $R[x_1] = A^H = R[x_2]$. Ceci montre que $x_1 = P(x_2)$ et $x_2 = Q(x_1)$ avec $P, Q \in R[T]$. Ainsi g_1 est la transformée de Tschirnhaus de g_2 par P, et g_2 est la transformée de Tschirnhaus de g_1 par Q. □

II.5 Calcul de résolvantes

D'une manière générale dans un algorithme de calcul de groupe de Galois, on cherche à calculer non pas un polynôme caractéristique d'un élément, mais plutôt sa résolvante (par exemple, voir [29], deuxième partie, page 19 et suivantes). Or, dans l'algèbre de décomposition universelle, la résolvante d'un élément $z \in \mathbb{D}_R^f$ et son polynôme caractéristique sur R sont fortement liés par la propriété suivante :

Propriété II.5.1 *Soit R un anneau quelconque, $f \in R[T]$ un polynôme unitaire quelconque, un élément z dans l'algèbre de décomposition universelle $\mathbb{D}_R^f$, χ le polynôme caractéristique de z sur R et $h = \prod_{y \in \mathcal{S}_n.z}(T - y)$ sa résolvante, et enfin $G = \mathrm{Stab}_{\mathcal{S}_n} z$ le fixateur de z sous l'action de $\mathcal{S}_n$. Alors*

$$h^{|G|} = \chi$$

Démonstration La preuve est établie par un petit calcul fort simple. Notons N la norme de $\mathbb{D}_R^f$ sur R et, par un petit abus, notons encore N la norme de $\mathbb{D}_{R[T]}^f$ sur $R[T]$ (T est une indéterminée sur R).

$$\chi = N(T - z) = \prod_{\sigma \in \mathcal{S}_n} \big(T - \sigma(z)\big) = \prod_{y \in \mathcal{S}_n.z} (T - y)^{|G|} = h^{|G|}$$

□

Ainsi, en théorie, il est facile de connaître la résolvante de z à partir de son polynôme caractéristique, moyennant un calcul de racine "$|G|$-ième". Mais dans la réalité il en va tout autrement car le cardinal de G peut être énorme, de l'ordre de $n!$: il est alors tout-à-fait inefficace d'utiliser cette relation telle qu'elle est présentée dans la propriété précédente.

Revenons à la tour d'algèbres libres aboutissant à $\mathbb{D}_R^f$ que nous avons mise en évidence dans la section II.2 :

$$A_{n+1} = R \ \subset \ A_n = R[x_n] \ \subset \ A_{n-1} = R[x_n, x_{n-1}] \subset \cdots \subset A_1 = R[x_n, \ldots, x_1] = \mathbb{D}_R^f$$

On sait que chaque A_i est une algèbre libre de dimension i sur A_{i+1} pour tout $i \in \{1, \ldots, n\}$ (voir la section II.2) :

$$A_i = A_{i+1}[X_i]/(f_i)$$

où f_i est le i-ième module de Cauchy (de degré i). En fait, l'algèbre de décomposition universelle $\mathbb{D}_R^f$ de f sur R est isomorphe canoniquement à l'algèbre de décomposition

universelle $\mathbb{D}^{f_i}_{A_{i+1}}$ du module de Cauchy f_i sur A_{i+1} pour tout i. Dès lors, $\mathcal{S}_i$ opère sur l'algèbre $\mathbb{D}^{f_i}_{A_{i+1}}$ et $\left(\mathbb{D}^{f_i}_{A_{i+1}}\right)^{\mathcal{S}_i} = A_{i+1}$, etc.

Si nous notons N_i la norme de A_i sur A_{i+1} pour tout $i \in \{1, \dots, n\}$, (et abusivement encore N_i celle de $A_i[T]$ sur $A_{i+1}[T]$) alors la norme de $\mathbb{D}^f_R$ sur R est donnée par la composition $N_n \circ N_{n-1} \circ \cdots N_1$.

Une idée consiste à utiliser la propriété II.5.1 pour chaque module de Cauchy f_i sur l'anneau A_{i+1}. En effet, si z appartient à $\mathbb{D}^f_R = \mathbb{D}^{f_i}_{A_{i+1}}$, sa résolvante $h_i = \prod_{y \in \mathcal{S}_i.z}(T-y)$ et son polynôme caractéristique $\chi_i = N_i \circ \cdots \circ N_1(T-z)$ sur A_{i+1} sont liés par :

$$h_i^{|G_i|} = \chi_i \qquad \text{avec} \qquad G_i = \mathrm{Stab}_{\mathcal{S}_i} z$$

Supposons que l'on connaisse $h_{i-1} \in A_i[T]$. Pour obtenir $h_i \in A_{i+1}[T]$, il suffit de calculer la norme de h_{i-1} sur $A_{i+1}[T]$ et d'en prendre la racine "$[G_i : G_{i-1}]$-ième" comme le montre ce petit calcul :

$$h_i^{|G_i|} = \chi_i = N_i \circ \cdots \circ N_1(T-z) = N_i(\chi_{i-1}) = N_i(h_{i-1})^{|G_{i-1}|}$$

Ainsi, par des calculs successifs de normes de résolvantes intermédiaires et de racines k-ièmes relativement petites ($[G_i : G_{i-1}] \leq [\mathcal{S}_i : \mathcal{S}_{i-1}] = i \leq n$), on peut obtenir la résolvante h de z sur R :

$$h_1 = T - z, \qquad h_i = N_i(h_{i-1})^{\frac{1}{[G_i:G_{i-1}]}} \quad \text{pour } i = 2 \dots n, \qquad h = h_n \tag{II.2}$$

$$h_i \in R[x_n, \dots, x_{i+1}][T]$$

Nicolas Rennert (Université Paris 6) a remarqué qu'il est assez fréquent (en petit degré et quand $G = \mathrm{Stab}_{\mathcal{S}_n} z$ est transitif) que le calcul de racine k-ième soit "inutile" ou bien que deux résolvantes consécutives h_{i-1} et h_i soient égales. Ce sont là des phénomènes bien sûr ponctuels, mais qui sont intéressants.

En effet, même si l'indice de G_{i-1} dans G_i est relativement petit, le cas où celui-ci est égal à 1 est appréciable... Ce cas se résume simplement à $G_i = G_{i-1}$, c'est-à-dire $G_i = \mathrm{Stab}_{\mathcal{S}_i} z \subset \mathcal{S}_{i-1}$. On a alors

$$h_i = N_i(h_{i-1})$$

De même, un indice de G_{i-1} dans G_i maximal (égal à $i = [\mathcal{S}_i : \mathcal{S}_{i-1}]$) est également appréciable : dans ce cas h_i et h_{i-1} sont deux polynômes égaux ! En effet, si nous avons $[G_i : G_{i-1}] = i = [\mathcal{S}_i : \mathcal{S}_{i-1}]$ alors $[\mathcal{S}_i : G_i] = [\mathcal{S}_{i-1} : G_{i-1}]$ et

$$|\mathcal{S}_i.z| = [\mathcal{S}_i : G_i] = [\mathcal{S}_{i-1} : G_{i-1}] = |\mathcal{S}_{i-1}.z|$$

Donc $\mathcal{S}_i.z = \mathcal{S}_{i-1}.z$, si bien que

$$h_i = \prod_{y \in \mathcal{S}_i.z} (T-y) = \prod_{y \in \mathcal{S}_{i-1}.z} (T-y) = h_{i-1}$$

Remarquons que $[G_i : G_{i-1}] = i$ est équivalent à G_i transitif sur $x_1, \ldots, x_i$ car l'indice de $G_{i-1} = G_i \cap \mathcal{S}_{i-1} = \mathrm{Stab}_{G_i} x_i$ dans G_i est précisément le cardinal de l'orbite de x_i sous l'action de G_i.

Finalement, nous obtenons la propriété suivante :

Propriété II.5.2 *Soit R un anneau, $f \in R[T]$ un polynôme unitaire dont le discriminant est régulier, un élément z dans l'algèbre de décomposition universelle $\mathbb{D}_R^f = R[x_1, \ldots, x_n]$ et $G_i = \mathrm{Stab}_{\mathcal{S}_i} z$ pour $i \in \{1, \ldots, n\}$. On suppose que pour tout $i \in \{1, \ldots, n\}$, l'une des deux assertions suivantes est vérifiée :*

- *G_i transitif sur $\{x_1, \ldots, x_i\}$ (lié à l'égalité $h_i = h_{i-1}$)*
- *$G_i \subset S_{i-1}$ (lié à $h_i = N_i(h_{i-1})$)*

(pour $i = 1$, la première condition est trivialement réalisée.) Alors on peut ramener la détermination de la résolvante liée à z à une simple succession de calculs de normes (i.e. de résultants) de l'algèbre $R[x_i, \ldots, x_n]$ sur $R[x_{i+1}, \ldots, x_n]$ où $i \in \{1, \ldots, n\}$ (si $i = n$, alors par convention on pose $R[x_{i+1}, \ldots, x_n] = R$).

La table des sous-groupes de degré inférieur à 8 vérifiant les critères de cette propriété (notation du logiciel GAP 3 release 4, voir [19]) est donnée ci-dessous. Les sous-groupes sont identifiés à leur classe de conjugaison dans $\mathcal{S}_n$.

On remarquera le symbole $*$ figurant sur certaines lignes. Il s'agit en fait de certaines classes de conjugaison dont seuls certains éléments vérifient le critère de la propriété II.5.2. En effet, l'algorithme donné par les relations (II.2) fixe un ordre d'élimination des x_i par des calculs successifs de normes : on commence par éliminer x_1, puis x_2, jusqu'à x_n. A cause de cet ordre, un sous-groupe de $\mathcal{S}_n$ peut réaliser la condition de la propriété II.5.2 sans que ce soit le cas pour tous ses conjugués.

Exemple : choisissons le polynôme générique de degré 4 pour f sur un anneau R quelconque et prenons l'élément $z = x_1x_2 + x_3x_4 \in \mathbb{D}_R^f$ dont le stabilisateur est le groupe $\langle (1,2), (1,3,2,4) \rangle \subset \mathcal{S}_4$ (groupe diédral) que nous noterons G. Ce groupe G possède les propriétés suivantes :

$$G \cap \mathcal{S}_2 = \mathcal{S}_2 \text{ transitif sur } \{x_1, x_2\} \qquad G \cap \mathcal{S}_3 = \mathcal{S}_2 \qquad G \text{ transitif sur } \{x_1, \ldots, x_4\}$$

Ce groupe G répond donc aux critères de la propriété II.5.2 et nous pouvons calculer la résolvante h de z uniquement avec "des coups" de normes. Ceci se traduit par :

$$h_1 = T - z \qquad h_2 = h_1 \in R[x_4, x_3][T] \qquad h = h_4 = h_3 = \mathrm{res}_{x_3}(f_3, h_2) \in R[T]$$

où f_3 est le module de Cauchy de degré 3. Nous avons donc besoin de calculer une seule norme (ou résultant) pour obtenir la résolvante de z. Ceci était loin d'être évident a priori.

En revanche, si nous considérons $x_1x_3 + x_2x_4$ dont le stabilisateur dans $\mathcal{S}_4$ est un conjugué de G, à savoir $G' = \langle (1,3), (1,2,3,4) \rangle$, nous ne pouvons pas utiliser la conclusion

de la propriété II.5.2 car $G' \cap S_3 = \{\mathrm{Id}, (1,3)\}$ est un groupe ni inclus dans $\mathcal{S}_2$, ni transitif sur $\{1,2,3\}$. Il faudra donc calculer une racine carrée et non se contenter d'enchaîner "les coups" de normes (ou alors changer l'ordre d'élimination des x_i). Cela se traduit par :

$$h_1 = T - z \qquad h_2 = \mathrm{res}_{x_2}(f_2, h_1) \in R[x_4, x_3][T] \qquad h_4 = h_3 = \mathrm{res}_{x_3}(f_3, h_2)^{\frac{1}{2}} \in R[T]$$

Cet exemple du groupe diédral montre bien pourquoi il faut parfois distinguer certains sous-groupes conjugués.

degré	ordre	classe
$n=1$	1	$S1$
$n=2$	2	$S2$
$n=3$	3	$A3$
	6	$S3$

degré 4 :

ordre	classe	r
4	$C(4)=4$	
4	$E(4)=2[\times]2$	
8	$D(4)$	$*$
12	$A4$	
24	$S4$	

degré 5 :

ordre	classe
5	$C(5)=5$
20	$F(5)=5:4$
60	$A5$
120	$S5$

degré 7 :

ordre	classe	r
7	$C(7)=7$	
42	$F_{42}(7)=7:6$	
168	$L(7)=L(3,2)$	$*$
2520	$A7$	
5040	$S7$	

degré 6 :

ordre	classe	r
6	$6T1 = C(6) = 6 = 3[\times]2$	
6	$6T2 = D_6(6) = [3]2$	
18	$6T5 = F_{18}(6) = [3^2]2 = 3 \wr 2$	$*$
24	$6T7 = S_4(6d) = [2^2]S(3)$	$*$
24	$6T8 = S_4(6c) = 1/2[2^3]S(3)$	$*$
48	$6T11 = 2S_4(6) = [2^3]S(3) = 2 \wr S(3)$	$*$
120	$6T14 = L(6):2 = PGL(2,5) = S_5(6)$	
360	$A6$	
720	$S6$	

degré 8 :

ordre	classe	r
8	$8T1 = C(8) = 8$	
8	$8T2 = 4[\times]2$	
8	$8T3 = E(8) = 2[\times]2[\times]2$	
8	$8T4 = D_8(8) = [4]2$	
8	$8T5 = Q_8(8)$	
32	$8T17 = [4^2]2$	$*$
32	$8T18 = E(8) : E_4 = [2^2]D(4)$	$*$
48	$8T23 = 2S_4(8) = GL(2,3)$	$*$
56	$8T25 = E(8) : 7 = F_{56}(8)$	
192	$8T39 = [2^3]S(4)$	$*$
192	$8T40 = 1/2[2^4]S(4)$	$*$
336	$8T43 = L(8) : 2 = PGL(2,7)$	
384	$8T44 = [2^4]S(4)$	$*$
1344	$8T48 = E(8) : L_7 = AL(8)$	$*$
20160	$A8$	
40320	$S8$	

Puisque le symbole $*$ implique une condition de bon choix d'un sous-groupe parmi ses conjugués, voici une liste fournissant des générateurs de bons sous-groupes dans les cas litigieux (l'ordre d'élimination étant $x_1, x_2, \ldots, x_n$) :

degré	classe de G	générateurs de G
$n = 4$	$D(4)$	$[(1,4,2,3),(3,4)]$
$n = 6$	$F_{18}(6) = [3^2]2 = 3 \wr 2$	$[(4,6,5),(1,6)(2,4)(3,5)]$
$n = 6$	$S_4(6d) = [2^2]S(3)$	$[(1,2)(3,4),(1,6,4)(2,5,3),(1,4)(2,3)]$
$n = 6$	$S_4(6c) = 1/2[2^3]S(3)$	$[(1,2)(3,4),(1,5,4)(2,6,3),(1,4)(2,3)(5,6)]$
$n = 6$	$2S_4(6) = [2^3]S(3) = 2 \wr S(3)$	$[(5,6),(1,5,4)(2,6,3),(1,4)(2,3)]$
$n = 7$	$L(7) = L(3,2)$	$[(1,6,2,3,4,7,5),(2,6)(3,5)]$
$n = 8$	$[4^2]2$	$[(1,4,2,3),(1,5)(2,6)(3,7)(4,8)]$
$n = 8$	$E(8) : E_4 = [2^2]D(4)$	$[(1,4)(2,3)(5,8)(6,7),(1,3)(2,4)(5,7)(6,8),$ $(1,8)(2,7)(3,6)(4,5),(5,8)(6,7),(5,7)(6,8)]$
$n = 8$	$2S_4(8) = GL(2,3)$	$[(1,3,8,4,2,5,7,6),(1,8,6)(2,7,4)]$
$n = 8$	$[2^3]S(4)$	$[(1,7)(2,8)(3,5)(4,6),(1,3)(2,4)(5,7)(6,8),$ $(1,6)(2,5)(3,8)(4,7),(3,5,7)(4,6,8),$ $(3,5,4,6)(7,8)]$
$n = 8$	$1/2[2^4]S(4)$	$[(1,2)(7,8),(1,8)(2,7)(3,5)(4,6),$ $(3,5,8)(4,6,7),(1,2)(3,5)(4,6)]$
$n = 8$	$[2^4]S(4)$	$[(1,2),(1,8)(2,7),(1,8,3,5)(2,7,4,6)]$
$n = 8$	$E(8) : L_7 = AL(8)$	$[(1,4)(2,3)(5,8)(6,7),(1,3)(2,4)(5,7)(6,8),$ $(1,8)(2,7)(3,6)(4,5),(1,2,7,3,5,8,6),$ $(1,2,3)(5,7,8),(1,2)(7,8)]$

II.6 Détermination du corps de décomposition

Jusqu'à présent, nous pouvions uniquement calculer la valeur d'une expression symétrique des racines $(\theta_i)_i$ d'un polynôme séparable f. En effet, comme nous l'avons vu dans la section II.2, grâce à un petit algorithme fort simple, on peut déterminer la valeur de $P(\theta_1, \ldots, \theta_n)$ si P appartient à $R[X_1, \ldots, X_n]^{\mathcal{S}_n}$. Ce type de calcul est appelé **calcul absolu**.

Par opposition, le but du **calcul relatif** est d'obtenir la valeur d'une expression non symétrique des racines, si celle-ci appartient à l'anneau de base. Par exemple, si P appartient à $K[X_1, \ldots, X_n]^G$ où K est un corps commutatif et $G \subset \mathcal{S}_n$ un groupe contenant le groupe de Galois de f, alors $P(\theta_1, \ldots, \theta_n)$ appartient à K.

Notre but, dans cette section, est de montrer comment l'algèbre de décomposition universelle peut servir pour résoudre le problème du calcul relatif. Précision : lorsque nous dirons qu'un sous-groupe G de $\mathcal{S}_n$ contient le groupe de Galois Γ d'un polynôme f séparable de degré n, nous entendrons par là que les racines de f ont été numérotées, que Γ est identifié à son image dans $\mathcal{S}_n$ définie par cette numérotation, et que $\Gamma \subset G$ (il ne s'agit donc plus ici de sous-groupes de $\mathcal{S}_n$ à une conjugaison près). Les hypothèses sous-entendues par la phrase "on suppose $\Gamma \subset G$" sont donc bien plus restrictives que la seule connaissance des classes de conjugaison de Γ et G dans $\mathcal{S}_n$.

II.6.a Calcul relatif

En général, le calcul relatif se fait par rapport à un sous-groupe $H \subset \mathcal{S}_n$ donné et contenant le groupe de Galois de f. Pour réaliser concrètement ce genre de calcul, il nous faut tout d'abord construire une algèbre galoisienne sur K de groupe H, tout comme l'est $\mathbb{D}_K^f$ dont le groupe de Galois est $\mathcal{S}_n$.

Considérons un élément x de $\mathbb{D}_K^f$ dont le stabilisateur H sous l'action de $\mathcal{S}_n$ contient le groupe de Galois de f. La résolvante qui lui est associée

$$\prod_{y \in \mathcal{S}_n.x} (T - y)$$

est à coefficients dans K et admet au moins une racine dans K. En effet, comme x est invariant par H qui contient le groupe de Galois de f, modulo un certain idéal maximal de $\mathbb{D}_K^f$ l'élément x appartient à K.

Théorème II.6.1 *Soit K un corps quelconque, A une K-algèbre galoisienne de groupe G (par exemple $\mathbb{D}_K^f$ de groupe $\mathcal{S}_n$, si $f \in K[T]$ est séparable). On considère un élément $x \in A$ tel que sa résolvante $\prod_{y \in G.x}(T - y)$ soit séparable et admette une racine $k \in K$. Alors le quotient $A/(x - k)$ est une algèbre galoisienne sur K de groupe $H = \mathrm{Stab}_G x$.*

Démonstration La résolvante de x étant séparable, elle est égale au polynôme minimal de x sur K (voir le théorème I.6.2, page 33). Autrement dit, la dimension de l'algèbre $K[x]$ sur K est $[G : H]$. Or ce nombre est exactement la dimension de A^H sur K, si bien que l'on peut conclure l'égalité $K[x] = A^H$ car x appartient à A^H.

D'autre part, la résolvante de x se factorise dans $K[T]$ en $(T-k)g(T)$ où k n'est pas racine de g. En évaluant cette factorisation en x, on trouve $(x-k)g(x)=0$ où $g(x)\neq 0$ car g est de degré strictement inférieur à $\dim_K K[x]$. On voit alors que $x-k$ est un diviseur de 0 dans A^H. Par suite $(x-k)A^H \cap K = (0)$ et

$$A^H/(x-k) = K[x]/(x-k) = K$$

Ainsi l'idéal $(x-k)A^H$ est en particulier un idéal maximal de A^H de degré résiduel 1.

De plus A est une algèbre galoisienne sur A^H de groupe H bien sûr. Étant donnée l'égalité $(x-k)A^H = (x-k)A \cap A^H$ (théorème I.5.1, page 27), la propriété I.4.4 appliquée à l'idéal $(x-k)A$ et l'anneau A^H justifie que $A/(x-k)$ est une algèbre galoisienne sur $A^H/(x-k)=K$ de groupe $\mathrm{Stab}_H(x-k)A = H$. □

Ainsi en choisissant $x \in \mathbb{D}_K^f$ tel que son stabilisateur soit exactement H (contenant le groupe de Galois de f) et sa résolvante séparable, nous pouvons obtenir une algèbre galoisienne sur K de groupe H. En effet, la résolvante de x admet au moins une racine λ dans K et le quotient

$$A = \mathbb{D}_K^f/(x-\lambda) = K[X_1,\ldots,X_n]/\left(\Sigma_f, x-\lambda\right)$$

donne naissance à une nouvelle algèbre galoisienne sur K de groupe H. Maintenant, dans A, toute expression en les X_i invariante sous l'action de H est à valeur dans K. De plus, si H est le groupe de Galois de f, alors A est un corps de décomposition de f sur K.

Pour effectuer des calculs dans le quotient A, deux possibilités s'offrent à nous : la première est de connaître une base de Gröbner pour l'ordre lexicographique de l'idéal engendré par Σ_f et $x-\lambda$ dans $K[X_1,\ldots,X_n]$. La seconde est d'utiliser l'idempotent engendrant l'orthogonal de l'idéal $(x-\lambda)$ dans $\mathbb{D}_K^f$. Nous rappelons à ce sujet que, dans un produit de corps (tel $\mathbb{D}_K^f$), tout idéal I est engendré par un unique idempotent e. De plus, l'orthogonal de I est alors engendré par l'idempotent $e'=1-e$. Nous donnons par ailleurs une méthode pour calculer ce dernier quand $\lambda \in K$ est une racine simple de la résolvante de x.

Propriété II.6.1 *Soit A une K-algèbre commutative, G un groupe fini opérant sur A tel que $A^G = K$, et $x \in A$. On suppose que la résolvante de x, $h = \prod_{y\in G.x}(T-y)$, admet une racine simple $\lambda \in K$. Alors l'idéal $(x-\lambda)A$ est idempotent et on sait calculer l'idempotent $e' \in A$ orthogonal de $(x-\lambda)A$:* $A = (x-\lambda)A \oplus e'A$ *avec*

$$e' = h'(\lambda)^{-1} \prod_{y\in G.x-\{x\}} (\lambda - y) = h'(\lambda)^{-1} \left(\frac{h(T)}{T-x}\right)_{T=\lambda}$$

Démonstration Ecrivons

$$h(T) = (T-x)g(T) \qquad \text{où} \qquad A[T] \ni g = \prod_{y\in G.x-\{x\}} (T-y)$$

En dérivant h, on obtient $h'(T) = g(T) + (T-x)g'(T)$, et en évaluant cette dernière en λ, $h'(\lambda) = g(\lambda) + (\lambda - x)g'(\lambda)$. Or $h'(\lambda) \in K$ est différent de 0 car λ est une racine simple de h. En posant

$$u = g(\lambda) \qquad v = (\lambda - x)g'(\lambda) \qquad a = h'(\lambda)^{-1}$$

il est clair que $au + av = 1$ et $uv = g(\lambda)(\lambda - x)g'(\lambda) = h(\lambda)g'(\lambda) = 0$. Ces deux dernières relations prouve que $e' = au$ est un idempotent ($au = au(au + av) = (au)^2$) et que $Ae' \oplus A(\lambda - x) = A$. □

Ainsi l'algèbre $\mathbb{D}_K^f$ se coupe en deux morceaux

$$\mathbb{D}_K^f = e'\mathbb{D}_K^f \oplus (x - \lambda)\mathbb{D}_K^f$$

Le quotient $A = \mathbb{D}_K^f/(x-\lambda)$ est isomorphe (en tant qu'algèbre) à $e'\mathbb{D}_K^f$. Les calculs relatifs se feront dans $e'\mathbb{D}_K^f$ (algèbre galoisienne sur K de groupe $H = \mathrm{Stab}(x)$). Par exemple, e' et x (vus comme des éléments de A) sont égaux respectivement à 1 et λ.

II.6.b Corps de décomposition et groupe de Galois

Considérons le corps des fractions rationnelles $K = \mathbb{Q}(a)$ et le polynôme irréductible (séparable) $f = T^4 - a$. Nous choisissons un polynôme f assez simple afin que les calculs n'obscurcissent pas l'exposé. Il est assez clair que le corps de décomposition de f sur $\mathbb{Q}(a)$ est $\mathbb{Q}(\sqrt[4]{a}, i)$ et que son groupe de Galois est le groupe diédral D_4. Cependant, notre but sera de retrouver ces résultats en utilisant le calcul relatif grâce à l'algèbre de décomposition universelle de f sur K.

L'algèbre $\mathbb{D}_K^f$ est galoisienne sur K de groupe $\mathcal{S}_4$. Soit $x = x_1x_2 + x_3x_4 \in \mathbb{D}_K^f$. Son stabilisateur sous l'action de $\mathcal{S}_4$ est exactement $D_4 = \langle (1,2), (1,3,2,4) \rangle$. Calculons la résolvante de x :

$$h = \prod_{y \in S_4.x} (T - y) = T(T^2 + 4a)$$

Ce polynôme (séparable) admet $0 \in K$ comme racine. Nous pouvons donc obtenir une seconde algèbre galoisienne sur K par le quotient $A = \mathbb{D}_K^f/(x-0)$. Ce quotient peut être réalisé par la donnée de la base de Gröbner (pour l'ordre lexicographique) de l'idéal (Σ_f, x) de $K[X_1, \ldots, X_4]$, à savoir

$$\mathcal{B} = \{X_4^4 - a, \quad X_3 + X_4, \quad X_2^2 + X_4^2, \quad X_1 + X_2\}$$

ou encore par l'idempotent $e' \in \mathbb{D}_K^f$ engendrant l'orthogonal de l'idéal $(x-0)\mathbb{D}_K^f$, à savoir

$$e' = \frac{x_4^2x_3^2 + a}{2a}$$

Nous poursuivons ensuite nos recherches : testons si le groupe cyclique Z_4 d'ordre 4, contenu dans D_4, contient le groupe de Galois de f en calculant la résolvante relative à D_4 de $x' = x_1x_3^2 + x_3x_2^2 + x_2x_4^2 + x_4x_1^2 \in A$ (le stabilisateur de x' dans D_4 est Z_4). Nous obtenons

$$\prod_{y \in D_4.x'} (T - y) = T^2 + 16a^2$$

Visiblement ce polynôme n'a pas de racine dans $K = \mathbb{Q}(a)$. Le groupe de Galois de f ne peut pas être contenu dans Z_4.

Poursuivons toujours la recherche : testons si le sous-groupe des double-transpositions, $V_4 \subset D_4$, contient le groupe de Galois de f en calculant la résolvante relative à D_4 de $x' = x_1x_3 + x_2x_4 \in A$ (le stabilisateur de x' dans D_4 est V_4). Nous obtenons

$$\prod_{y \in D_4.x'} (T - y) = T^2 + 4a$$

Visiblement ce polynôme n'a pas de racine dans $K = \mathbb{Q}(a)$. Le groupe de Galois ne peut pas être contenu dans V_4.

Finalement, comme le groupe de Galois de f est inclus dans D_4 et n'est inclus ni dans Z_4 ni dans V_4 (les deux sous-groupes maximaux transitifs de D_4), celui-ci est nécessairement égal à D_4. De plus l'algèbre galoisienne A est le corps de décomposition de f sur $K = \mathbb{Q}(a)$. La base de Gröbner $\mathcal{B}$ nous montre les relations qu'il existe entre les racines de f : si x_4 est une racine 4-ième quelconque de a, alors $x_3 = -x_4$, x_2 est racine carrée quelconque de $-x_4^2$ et $x_1 = -x_2$.

La méthode ci-dessus peut être employée de façon systématique pour trouver le corps de décomposition d'un polynôme séparable unitaire $f \in K[T]$ (K corps quelconque) ainsi que son groupe de Galois sur K. La méthode peut se résumer rapidement à ceci :

1. *On considère une K-algèbre A galoisienne de groupe G (initialement $\mathbb{D}_K^f$ dont le groupe de Galois sur K est $\mathcal{S}_n$ où $n = \deg f$) ;*

2. *On parcourt les sous-groupes maximaux de G. On note G' un de ces sous-groupes ;*

3. *On choisit un élément $x \in A$ dont le stabilisateur sous l'action de G est exactement G' : x est appelé G'-résolvant relatif à G ;*

4. *On calcule dans A le polynôme $h = \prod_{y \in G.x} (T - y)$ appartenant à $K[T]$ (que l'on appelle G'-résolvante relative à G). On suppose que h est séparable. On sait qu'il existe des $x \in A$ qui satisfont cette condition si K est un corps infini (corollaire I.8.1) ;*

5. *Si h admet une racine $k \in K$ alors on pose $I = (x - k)A$ et on repart de l'étape 1 en considérant la K-algèbre galoisienne A/I de groupe de Galois $G' = \mathrm{Stab}_G I$:*

$$A \leftarrow A/I \qquad \text{et} \qquad G \leftarrow G'$$

6. *Si h n'admet pas de racine dans K, on sait alors que G' ne contient pas le groupe de Galois de f (théorème II.6.2). On revient à l'étape 2 en changeant de sous-groupe G' ;*

7. *Si aucun sous-groupe G' ne contient le groupe de Galois de f alors G est égal au groupe de Galois et A au corps de décomposition de f.*

Théorème II.6.2 *Soit $P \in K[X_1, \ldots, X_n]$ et $\theta = (\theta_1, \ldots, \theta_n)$ où les θ_i sont les racines d'un polynôme séparable $f \in K[T]$ dans une clôture algébrique de K. Soit G un sous-groupe de $\mathcal{S}_n$ contenant le groupe de Galois de f sur K. Alors le polynôme*

$$h = \prod_{Q \in G.P} \big(T - Q(\theta)\big)$$

appartient à $K[T]$. Si de plus h est séparable alors il y a équivalence entre "h admet une racine dans K" et "$\mathrm{Stab}_G P \supset \mathrm{Gal}_K(f)$ pour une certaine numérotation des θ_i".

Démonstration Le fait que h appartient à $K[T]$ est évident car G contient $\mathrm{Gal}_K(f)$.

Si h admet une racine dans K, quitte à renuméroter les θ_i (la renumérotation se fait grâce à un élément de G), on peut supposer qu'il s'agit de $x = P(\theta)$. Le fait que x appartient à K est équivalent à x est stable sous l'action de $\mathrm{Gal}_K(f)$, ce qui équivaut aussi à P stable sous l'action de $\mathrm{Gal}_K(f)$ (si $g \in \mathrm{Gal}_K(f)$ tel que $P \neq g.P$, alors

$$P(\theta) = x = g.x = g.P(\theta)$$

implique que x est racine multiple de h : impossible si h est séparable). Pour conclure, P stable sous l'action de $\mathrm{Gal}_K(f)$ équivaut à $\mathrm{Stab}_G P \supset \mathrm{Gal}_K(f) \cap G = \mathrm{Gal}_K(f)$. □

II.7 Exemples et applications

Le lecteur trouvera dans cette section des exemples d'applications du calcul des résolvantes. Nous ne faisons que rappeler certaines propriétés bien connues et très classiques, mais nous les démontrons ici "à la main", à titre d'exercice...

II.7.a Actions non conjuguées de $\mathrm{Aut}_K E$

On se propose de calculer deux polynômes irréductibles de $K[T]$, de même degré, ayant même corps de décomposition E sur $\mathbb{Q}$, et tels que les actions du groupe $\mathrm{Aut}_{\mathbb{Q}} E$ sur leurs racines soient vraiment différentes (i.e. non conjuguées).

Lemme II.7.1 *Soit G un groupe et H_1, H_2 deux sous-groupes de G. Il existe une G-application ϕ de $(G/H_1)_g$ dans $(G/H_2)_g$ si et seulement si H_1 est inclus dans un conjugué de H_2.*

> Remarque. Les ensembles $(G/H_1)_g$ et $(G/H_2)_g$ désignent les classes à gauche de G modulo H_1 et H_2.

Démonstration
• Soit $\phi : (G/H_1)_g \to (G/H_2)_g$ une G-application. Soit $y \in G$ tel que $\phi(1.H_1) = y.H_2$. Comme ϕ est une G-application

$$H_1 = \mathrm{Stab}_G 1.H_1 \subset \mathrm{Stab}_G \phi(1.H_1) = \mathrm{Stab}_G y.H_2 = y.H_2.y^{-1}$$

• Réciproquement, si $H_1 \subset y.H_2.y^{-1}$ alors l'application $(G/H_1)_g \to (G/H_2)_g$ qui envoie $x.H_1$ sur $xy.H_2$ est bien définie et c'est une G-application. □

Le corollaire suivant découle simplement du lemme précédent.

Corollaire II.7.1 *Soit G un groupe, H_1 et H_2 deux de ses sous-groupes. Il existe une G-bijection $\phi : (G/H_1)_g \to (G/H_2)_g$ si et seulement si H_1 et H_2 sont conjugués dans G.*

Pour trouver les deux polynômes qui font l'objet de notre exemple, considérons deux actions de $\mathcal{S}_4$:

1. La première consiste à restreindre l'action de $\mathcal{S}_4$ sur l'orbite du polynôme

$$P = X_1X_2^2 + X_2X_3^3 + X_3X_4^2 + X_4X_1^2$$

   Le stabilisateur G de P contient exactement les éléments de $\mathcal{S}_4$ permutant les couples $(X_1, X_2), (X_2, X_3), (X_3, X_4), (X_4, X_1)$, ou encore les permutations échangeant les couples $(1, 2), (2, 3), (3, 4), (4, 1)$, c'est-à-dire finalement, G est le groupe engendré par le cycle $(1, 2, 3, 4)$. L'action de $\mathcal{S}_4$ sur l'orbite de P est isomorphe à celle de $\mathcal{S}_4$ sur le quotient $(\mathcal{S}_4/G)_g$ via la bijection $\sigma.P \mapsto \sigma.G$.

2. La seconde consiste à restreindre l'action de $\mathcal{S}_4$ sur l'orbite du polynôme

$$Q = X_1X_3 - X_2X_4$$

   Le stabilisateur H de Q est formé exactement par les permutations laissant fixes les ensembles $\{1, 3\}$ et $\{2, 4\}$, c'est-à-dire G est le groupe $\mathcal{S}_2 \times \mathcal{S}_2$. L'action de S_4 sur l'orbite de Q est alors isomorphe à celle de $\mathcal{S}_4$ sur le quotient $(\mathcal{S}_4/H)_g$ via la bijection $\sigma.P \mapsto \sigma.H$.

Dans les deux cas (actions de $\mathcal{S}_4$ sur $\mathcal{S}_4.P$ ou $\mathcal{S}_4.Q$), l'action est transitive et le cardinal de $\mathcal{S}_4.P$ ou $\mathcal{S}_4.Q$ est $\frac{24}{4} = 6$. Ainsi on exhibe deux sous-groupes de $\mathcal{S}_6$ dont les actions sur $\{1, \ldots, 6\}$ sont identiques respectivement aux actions de $\mathcal{S}_4$ sur $\mathcal{S}_4.P$ et $\mathcal{S}_4.Q$. Ces deux sous-groupes sont transitifs, isomorphes à $\mathcal{S}_4$, mais ils ne sont pas conjugués car les stabilisateurs de P et Q ne le sont pas dans $\mathcal{S}_4$.

Propriété II.7.1 *Soit E une extension galoisienne d'un corps K et une représentation transitive de $\mathrm{Aut}_K E$ dans $\mathcal{S}_n$. Alors il existe un polynôme $f \in K[X]$ séparable de degré n dont le corps de décomposition est inclus dans E et tel que l'action de $\mathrm{Aut}_K E$ sur ses n racines soit isomorphe à la représentation de $\mathrm{Aut}_K E$ dans $\mathcal{S}_n$ donnée.*

Ce polynôme f est en fait le polynôme minimal d'un élément primitif de l'extension E^H où H est le stabilisateur d'un élément de $\{1, \ldots, n\}$ dans la représentation de $\mathrm{Aut}_K E$.

Démonstration Par hypothèse, $G = \mathrm{Aut}_K E$ opère sur $\{1, \ldots, n\}$. Soit $H \subset \mathrm{Aut}_K E$ le stabilisateur de 1 sous son action. Comme cette action est transitive, l'indice de H dans $\mathrm{Aut}_K E$ est égal à n. Cette action est isomorphe à celle de G sur $(G/H)_g$ via la bijection $\sigma.1 \mapsto \sigma H$. Le corps E^H est une sous-extension intermédiaire de degré n sur K. Puisque E^H est une extension séparable ($K \subset E$ est galoisienne), il existe un élément primitif x de E^H. Soit f son polynôme minimal. Enfin, il est facile de vérifier que l'action de $\mathrm{Aut}_K E$ sur les racines de f est isomorphe à celle de G sur $(G/H)_g$ via la bijection $\sigma(x) \mapsto \sigma H$. □

Corollaire II.7.2 *Avec les mêmes hypothèses que la propriété précédente, on peut ajouter le résultat suivant : la représentation de* $\mathrm{Aut}_K E$ *est fidèle (bijection entre* $\mathrm{Aut}_K E$ *et le sous-groupe de* $\mathcal{S}_n$*) si et seulement si le corps de décomposition du polynôme* f *est égal à* E*.*

Démonstration En effet la représentation de $\mathrm{Aut}_K E$ est fidèle si et seulement si l'intersection des stabilisateurs des éléments de $\{1, \ldots, n\}$ est réduite à $\{\mathrm{Id}\}$. Or la plus petite extension normale de E contenant $E^H = K(x)$ est l'extension $E^{H'}$ où H' est le plus grand sous-groupe de H normal dans $\mathrm{Aut}_K E$. Ce plus grand sous-groupe est en fait l'intersection des conjugués de H dans $\mathrm{Aut}_K E$. Conclusion : l'action est fidèle si et seulement si le corps de décomposition du polynôme minimal de x (c'est-à-dire $E^{H'}$) est E. □

Par exemple, prenons un polynôme dont le groupe de Galois est $\mathcal{S}_4$:

$$f = X^n - X - 1 \in \mathbb{Q}[X] \qquad n = 4$$

Notons x_1, x_2, x_3, x_4 les racines de f (dans $\mathbb{C}$) et E son corps de décomposition engendré par les x_i. Nous possédons deux représentations de $\mathrm{Aut}_{\mathbb{Q}} E$ dans $\mathcal{S}_6$: $\mathcal{S}_4 \to \mathrm{Aut}\ (\mathcal{S}_4/H_1)_g$ et $\mathcal{S}_4 \to \mathrm{Aut}\ (\mathcal{S}_4/H_2)_g$, ainsi que des éléments de E dont les stabilisateurs sont respectivement $H_1 = \langle (1,2,3,4) \rangle$ et $H_2 = \langle (1,3),(2,4) \rangle$:

$$x_1x_2^2 + x_2x_3^3 + x_3x_4^2 + x_4x_1^2 \qquad \text{et} \qquad x_1x_3 - x_2x_4$$

Les polynômes minimaux de ces deux éléments (c'est-à-dire les résolvantes associées si celles-ci sont séparables) réaliseront l'objectif que l'on s'était proposé. Pour s'assurer que les corps de décomposition des deux derniers polynômes minimaux sont bien égaux (à E), il suffit de remarquer que le plus grand sous-groupe de H_1 normal dans $\mathcal{S}_4$ est $\{\mathrm{Id}\}$, idem pour H_2. Nous obtenons après calcul

$$T^6 - 4T^4 - 1$$
de groupe de Galois $S_4(6d) : \mathcal{S}_4 \to \mathrm{Aut}\ (\mathcal{S}_4/H_1)_g$

$$T^6 + 6T^5 + 24T^4 + 56T^3 + 160T^2 + 224T + 384$$
de groupe de Galois $S_4(6c) : \mathcal{S}_4 \to \mathrm{Aut}\ (\mathcal{S}_4/H_2)_g$

Les notations $S_4(6d)$ et $S_4(6c)$ proviennent de la classification des groupes de Conway, Hulpke et McKay [19]. Le premier polynôme possède un discriminant carré, pas le second.

Signalons pour finir que le groupe $H_3 \subset \mathcal{S}_4$ formé par les doubles transpositions (le groupe de Klein) ne donne pas un résultat satisfaisant car il est normal dans $\mathcal{S}_4$, si bien que le corps de décomposition d'une résolvante associée à H_3 n'est pas E...

II.7.b Premiers totalement décomposés

Soit K une extension finie du corps $\mathbb{Q}$ et $\mathcal{O}_K$ l'anneau des entiers de K. La théorie des nombres nous dit que $\mathcal{O}_K$ est un **anneau de Dedekind**, c'est-à-dire un anneau nœthérien, intégralement clos et dont tous les idéaux premiers non nuls sont maximaux. Dans cet

anneau $\mathcal{O}_K$, tout idéal propre non nul admet une décomposition unique en produit fini d'idéaux premiers.

Soit $f \in \mathbb{Z}[X]$ un polynôme unitaire irréductible, θ une de ses racines (dans $\mathbb{C}$ par exemple) et $A = \mathbb{Z}[\theta]$. Il est clair que A n'est pas en général intégralement clos (on connaît des fameux contre-exemples en dimension 2 avec $\mathbb{Z}\left[\sqrt{\Delta}\right]$, pour $\Delta \equiv -1 \mod 4$). Ce n'est donc pas un anneau de Dedekind. Cependant tout idéal pA où p est un nombre premier ne divisant pas le discriminant de f peut être factorisé dans A en produit d'idéaux premiers. La théorie des nombres montre que la factorisation de pA dans A est alors liée à celle de f dans $\mathbb{F}_p[X]$. En effet, si l'on considère les isomorphismes

$$A/pA \simeq \mathbb{Z}[X]/(f,p) \simeq \mathbb{F}_p[X]/(f) \qquad \text{produit fini d'extensions de } \mathbb{F}_p$$

il est clair que les idéaux maximaux de A contenant p sont en rapport étroit avec les idéaux maximaux de $\mathbb{F}_p[X]$ contenant f, i.e. les idéaux engendrés par les diviseurs irréductibles de $f \in \mathbb{F}_p[X]$.

Par exemple pA se factorise en un produit de n idéaux premiers distincts de A si et seulement si f se factorise en un produit de n facteurs linéaires distincts dans $\mathbb{F}_p[X]$. On se propose donc de chercher des (une infinité...) premiers qui se décomposent totalement dans A, ou encore tels que f se scinde totalement dans $\mathbb{F}_p[X]$.

Théorème II.7.1 *Soit $f \in \mathbb{Z}[X]$ unitaire. Il existe une infinité de premiers $p \in \mathbb{N}$ tels que $f \mod p$ ait toutes ses racines dans $\mathbb{F}_p$.*

Remarque. Il existe un théorème beaucoup plus général (théorème II.7.2, page 69).

Ce théorème sera démontré "à la main" après quelques lemmes... Ces lemmes proviennent d'éléments "extérieurs" au cadre qui nous intéresse dans cette section : ce sont des propriétés classiques qui ont de multiples conséquences mathématiques... Il ne faudrait surtout pas croire que ce sont simplement des lemmes pour démontrer le théorème II.7.1 !

Soit $f \in \mathbb{Z}[X]$ unitaire non constant. On considère ses racines dans une clôture algébrique de $\mathbb{Q}$ (quitte à remplacer f par sa partie sans facteur carré, on suppose f séparable). Soit $\theta_1, \ldots, \theta_n$ ses racines et S l'ensemble formé par les différences

$$(\theta_{\tau.1}, \ldots, \theta_{\tau.n}) - (\theta_{\sigma.1}, \ldots, \theta_{\sigma.n}) \tag{II.3}$$

où $\sigma \neq \tau$ varient dans $\mathcal{S}_n$. Il est clair que S ne contient pas $(0, \ldots, 0)$ puisque les θ_i sont distincts.

Lemme II.7.2 *Soit un corps K, E un espace vectoriel, et S une partie finie de E^n ne contenant pas $(0, \ldots, 0)$. Si $|K| \geq |S|$ alors il existe un polynôme P de la forme $\sum_i a_i X_i$ ($a_i \in K$) tel que $P(s_1, \ldots, s_n) \neq 0$ pour tout $s \in S$.*

Démonstration Pour $s \in S$, posons $E_s = \{a \in K^n | \sum_{i=1}^n a_i.s_i = 0\}$. E_s est bien un sous-espace vectoriel propre de K^n car les s_i sont non tous nuls. On sait que $|K| \geq |S|$ entraîne, par la propriété II.7.2, que les $(E_s)_{s \in S}$ ne peuvent recouvrir K^n. Il existe donc un élément $k \in K^n$ qui n'appartient à aucun E_s, i.e. tel que $\forall\ s \in S,\ \sum_{i=1}^n k_i.s_i \neq 0$. □

Dans notre cas, nous avons $K = \mathbb{Q}$ et S formé par les différences données par $(II.3)$. Grâce au lemme II.7.2, on tient un polynôme P à coefficients dans $\mathbb{Q}$, linéaire en ses variables et tel que

$$P(\theta_{\tau.1}, \ldots, \theta_{\tau.n}) - P(\theta_{\sigma.1}, \ldots, \theta_{\sigma.n}) \neq 0$$

dès que τ et σ sont différents. On peut supposer que les coefficients de P sont entiers quitte à les multiplier par un entier (un dénominateur commun). Ainsi le polynôme

$$g = \prod_{\sigma \in \mathcal{S}_n} (X - \sigma.P(\theta_1, \ldots, \theta_n)) = \prod_{\sigma \in \mathcal{S}_n} (X - P(\theta_{\sigma.1}, \ldots, \theta_{\sigma.n}))$$

est séparable. Le polynôme g appartient à $\mathbb{Z}[X]$ car ses coefficients sont stables sous l'action de $\mathcal{S}_n$. Le polynôme g est une résolvante liée au groupe $\{\mathrm{Id}\}$. Soit $p \in \mathbb{N}$ un nombre premier ne divisant pas le discriminant de g tel que p divise un élément de $g(\mathbb{Z})$ (on a le choix parmi une infinité, voir propriété II.7.3). Alors $\overline{g} \in \mathbb{F}_p[X]$ est séparable et admet une racine dans $\mathbb{F}_p$.

Lemme II.7.3 *Soit $f \in \mathbb{Z}[X]$ unitaire et $\theta_1, \ldots, \theta_n$ ses racines dans une clôture algébrique de $\mathbb{Q}$. Si p est nombre premier alors il existe un idéal maximal $\mathcal{P}$ de $\mathbb{Z}[\theta_1, \ldots, \theta_n]$ tel que $\mathbb{Z}/p\mathbb{Z}$ soit contenu dans $\mathbb{Z}[\theta_1, \ldots, \theta_n]/\mathcal{P}$ et $\theta_1, \ldots, \theta_n \mod \mathcal{P}$ soient les racines de $f \mod p$.*

Démonstration Pour commencer, p ne devient pas inversible dans $\mathbb{Z}[\theta_1, \ldots, \theta_n]$. Il est donc contenu dans un idéal maximal $\mathcal{P}$ de $\mathbb{Z}[\theta_1, \ldots, \theta_n]$. Montrons maintenant que $\mathbb{Z}/p\mathbb{Z}$ est inclus $\mathbb{Z}[\theta_1, \ldots, \theta_n]/\mathcal{P}$: il suffit en fait de montrer que $\mathbb{Z} \cap \mathcal{P} = p\mathbb{Z}$, ce qui est clair car $p\mathbb{Z} \subset \mathbb{Z} \cap \mathcal{P} \subsetneq \mathbb{Z}$ et $p\mathbb{Z}$ maximal. Enfin, il est encore clair que les $\theta_1, \ldots, \theta_n \mod \mathcal{P}$ sont les racines de $f \bmod p$ car $f \bmod p = \prod_{i=1}^n (X - \theta_i) \mod \mathcal{P}$. □

Ainsi dans le corps $D_{\mathbb{F}_p} = \mathbb{Z}[\theta_1, \ldots, \theta_n]/\mathcal{P}$, les polynômes $\overline{f}$ et $\overline{g}$ se factorisent en

$$\overline{f} = \prod_{i=1..n} (X - \overline{\theta_i}) \qquad \overline{g} = \prod_{\sigma \in \mathcal{S}_n} \left(X - \sigma.P(\overline{\theta_1}, \ldots, \overline{\theta_n})\right)$$

où $P(\overline{\theta_1}, \ldots, \overline{\theta_n})$ (quitte à renuméroter les θ_i) appartient à $\mathbb{F}_p$. Le corps de décomposition de f est bien $\mathbb{F}_p$. En effet, considérons le groupe de Galois sur $\mathbb{F}_p$ du corps de décomposition $D_{\mathbb{F}_p}$ de $\overline{f}$, et montrons qu'il est réduit à $\{\mathrm{Id}\}$. Si $\tau \in \mathrm{Aut}_{\mathbb{F}_p} D_{\mathbb{F}_p}$, alors

$$D_{\mathbb{F}_p} \ni P(\overline{\theta_1}, \ldots, \overline{\theta_n}) = \tau.P(\overline{\theta_1}, \ldots, \overline{\theta_n})$$

Comme $P(\overline{\theta_1}, \ldots, \overline{\theta_n})$ et $\sigma.P(\overline{\theta_1}, \ldots, \overline{\theta_n})$ sont deux racines distinctes de $\overline{g}$ si $\sigma \neq \mathrm{Id}$ ($\overline{g}$ est séparable), nécessairement $\tau = \mathrm{Id}$, et le corps de décomposition de $\overline{f}$ est $\mathbb{F}_p$.

> Remarque. le fait que $\overline{g}$ est séparable, de degré $n!$, et à racines dans $\mathbb{F}_p$, implique que $p \geq n!$: il y a une infinité de premiers décomposant totalement f, mais ils ne sont pas tous "humains"...

Revenons maintenant sur les lemmes auxquels nous avons fait appel.

Propriété II.7.2 (voir [14] page 40) *Soit E un espace vectoriel sur un corps K. S'il existe un recouvrement fini de sous-espaces vectoriels propres $(E_i)_{i\in S}$ de E, alors K est un corps fini et $|K| < |S|$.*

Démonstration Quitte à enlever quelques E_i, on peut supposer que la famille $(E_i)_{i\in S}$ est minimale pour le recouvrement de E. Le cardinal de S est supérieur à deux puisque les E_i sont des sous-espaces propres. Fixons-nous $j \in S$ et soit $e \in E_j - \cup_{i\neq j} E_i$ (cet élément existe car la famille est minimale) et $f \in E - E_j$. Considérons maintenant les ensembles $L_i = \{\lambda \in K \mid \lambda.e + f \in E_i\}$. Les $(L_i)_{i\in S}$ forment un recouvrement de K car les $(E_i)_{i\in S}$ recouvrent E. Majorons le cardinal de L_i : $L_j = \emptyset$ car $f \notin E_j$, et pour $i \neq j$ $|L_i| \leq 1$. En effet, si $\lambda.e + f$ et $\mu.e + f$ sont dans E_i alors $\lambda.e - \mu.e \in E_i$. Comme $e \notin E_i$ alors $\lambda = \mu$ (K est un corps).

Enfin, la preuve se termine par $|K| \leq \sum_{i\in S-\{j\}} |L_i| < |S|$. □

On utilise généralement ce lemme en supposant que K est infini : un K-espace vectoriel ne peut pas être alors une réunion finie de sous-espaces propres.

Propriété II.7.3 *Soit $g \in \mathbb{Z}[X]$ un polynôme non constant. L'ensemble des nombres premiers divisant au moins un élément de $g(\mathbb{N})$ est infini.*

Démonstration Quitte à multiplier par -1 le polynôme g, on peut admettre que son coefficient dominant est positif. Supposons que pour tout $x \in \mathbb{N}$, $g(x) = \pm \prod_{p\in P} p^{n_p(x)}$ où P est un ensemble fini de nombres premiers. Pour un $n \in \mathbb{N}$ assez grand, g est strictement croissant et positif sur $[n, +\infty[$. Si $j \in \mathbb{N}$ alors le cardinal de $g(\{n+1, \ldots, n+j\})$ est exactement j.

Majorons maintenant le cardinal de l'ensemble formé par $\prod_{p\in P} p^{n_p(x)}$ pour x parcourant l'ensemble $\{n, \ldots, n+j\}$: si $x \in \{n+1, \ldots, n+j\}$ alors $p^{n_p(x)} \leq g(x) \leq g(n+j)$, et donc

$$0 \leq n_p(x) < \log_p(g(n+j)) \leq \log_2(g(n+j))$$

autrement dit $n_p(x)$ est un entier appartenant à $[0, \log_2(g(n+j))]$. Ainsi nous avons $j = |g(\{n+1, \ldots, n+j\})| \leq \big(\log_2(g(n+j)) + 1\big)^{|P|}$ quel que soit $j \in \mathbb{N}$. Mais cela devient absurde lorsque j tend vers l'infini (comparer les croissances d'un logarithme et de l'identité). □

Le théorème suivant est plus qu'une généralisation du théorème II.7.1 : il ne se contente pas d'énoncer l'existence de premiers qui se décomposent totalement dans une clôture intégrale, mais il précise leur densité... Ce théorème donne naissance à une méthode pour cerner le groupe de Galois d'une extension (bien qu'elle n'aboutisse pas pour des groupes particuliers).

Théorème II.7.2 (de densité de Čebotarev, voir [37], pages 166 à 170)
Soit K un corps de nombres et L une extension galoisienne de K. On note G son groupe de Galois. Soit $C \subset G$ la classe de conjugaison d'un élément de G et E l'ensemble

des idéaux premiers $\mathfrak{p}$ *de* $\mathcal{O}_K$ *non ramifiés dans* $\mathcal{O}_L$ *et vérifiant* $C = \left(\frac{L/K}{\mathfrak{p}}\right)$ *(symbole d'Artin). Alors* E *possède une densité de Dirichlet égale à* $\frac{|C|}{|G|}$*, i.e.*

$$\lim_{x\to+\infty} \frac{|\{\mathfrak{p} \in E \mid \mathrm{Norm}(\mathfrak{p}) \leq x\}|}{|\{\mathfrak{p} \text{ premier} \mid \mathrm{Norm}(\mathfrak{p}) \leq x\}|} = \frac{|C|}{|G|}$$

En clair, si l'on se place sur $\mathbb{Z}$ ($\mathrm{Norm}(p\mathbb{Z}) = p$) et que l'on considère un polynôme de $\mathbb{Z}[X]$, on obtient le corollaire qui suit. Le lecteur trouvera la définition des types d'une permutation, d'une partition et d'une factorisation page 75 (définition II.7.1).

Corollaire II.7.3 *Soit* L *le corps de décomposition d'un polynôme unitaire séparable* f *à coefficients dans* $\mathbb{Z}$ *et de degré* n*. On note* G *le groupe de Galois* $\mathrm{Aut}_{\mathbb{Q}}(L)$ *et on le considère comme un sous-groupe des permutations des racines de* f*. Soit* u *le type d'une partition de* n*,* D *l'ensemble des éléments de* G *dont le type soit* u*, et* E *l'ensemble des nombres premiers* p *ne divisant pas le discriminant de* $\mathcal{O}_L$ *et tels que le type de la décomposition en irréductibles de* $f \bmod p$ *soit* u*. Alors*

$$\lim_{x\to+\infty} \frac{|\{p \in E \mid p \leq x\}|}{|\{p \text{ premier} \mid p \leq x\}|} = \frac{|D|}{|G|}$$

> Remarque. Le discriminant d'une algèbre libre de rang fini sur $\mathbb{Z}$ est a priori défini au carré d'un inversible de $\mathbb{Z}$ près comme étant le discriminant d'une $\mathbb{Z}$-base quelconque. Or seul $1 \in \mathbb{Z}$ est le carré d'un inversible dans $\mathbb{Z}$, donc le discriminant d'une $\mathbb{Z}$-algèbre libre de rang fini est un nombre entier bien déterminé.

Démonstration Pour utiliser le théorème précédent, il faut considérer l'ensemble des classes C de conjugaison de G dont le type des éléments est u. On applique alors le théorème II.7.2 à chaque classe C, puis on somme les densités (qui sont d'ailleurs toutes égales) pour trouver celle de D. □

Exemple : si l'on prend $u = (1, 1, \ldots, 1)$, $D = \{\mathrm{Id}\} \subset G$, et E l'ensemble des nombres premiers p ne divisant pas le discriminant de $\mathcal{O}_L$ et tels que f soit totalement scindé modulo p, alors

$$\lim_{x\to+\infty} \frac{|\{p \in E \mid p \leq x\}|}{|\{p \text{ premier} \mid p \leq x\}|} = |G|^{-1}$$

Si le groupe de Galois de f est énorme, les premiers scindant totalement f sont rares...

II.7.c Paramétrisation rationnelle des polynômes de groupe de Galois D_4

Une certaine méthode pour déterminer le groupe de Galois d'un polynôme consiste à cerner ce groupe grâce à son action sur des ensembles (voir [29], [61]). Chaque action est codée par la factorisation d'une résolvante adéquate. Il n'est pas difficile de constater que ce sont toujours les mêmes résolvantes qui doivent être calculées en premiers lieux (pour

des raisons de calculabilité, de départage...). Par exemple pour un polynôme unitaire séparable irréductible f de degré 4, une méthode répandue est celle qui consiste à calculer la *résolvante tripartite* de f. Suivant la factorisation de cette résolvante, on tire des conclusions d'inclusion ou de non inclusion, ces conclusions pouvant elles-mêmes être affinées par un calcul de discriminant ou d'une résolvante départageant deux sous-groupes de $\mathcal{S}_4$... En fait la *résolvante tripartite* n'est autre qu'une résolvante associée au groupe diédral, et dont la qualité est d'être toujours séparable.

Afin de ne pas recalculer à chaque fois les résolvantes les plus utilisées, il est tout-à-fait légitime de vouloir les calculer génériquement (une fois pour toutes). Ceci est effectivement possible pour les petits degrés car les expressions intermédiaires obtenues au cours des calculs sont raisonnables...

Dans l'exemple qui est traité ici, on se propose de calculer la résolvante tripartite générique, et d'en tirer une famille de polynômes avec paramètres dont le groupe de Galois est toujours le goupe diédral D_4. On essaiera de donner une famille la plus générale possible sur un corps K quelconque... (Voir les familles de polynômes $f_{\substack{a,c\\d,\lambda}}$ pages 73 et 74.)

Propriété II.7.4 *Soit R un anneau, $P \in R[X_1, \ldots, X_n]$ un polynôme. Alors la résolvante qui lui est associée, i.e. $\prod_{Q \in S_n.P} (T - Q)$, est à coefficients dans $R[\sigma_1, \ldots, \sigma_n]$.*

Par exemple, prenons $P = X_1X_2 + X_3X_4 \in \mathbb{Z}[X_1, \ldots, X_4]$. Son stabilisateur est le groupe diédral $D_4 = \langle (1,2), (1,3,2,4) \rangle$ et sa résolvante nommée la *résolvante tripartite*. Les coefficients de ce polynôme s'expriment en fonction des polynômes symétriques élémentaires.

Propriété II.7.5 *Soit K un corps, f un polynôme de $K[T]$ unitaire séparable, et x un élément de $\mathbb{D}_K^f = K[x_1, \ldots, x_n]$ dont le stabilisateur sous l'action de $\mathcal{S}_n$ est G. Soit les racines $\theta_1, \ldots, \theta_n$ de f dans une clôture algébrique de K. On suppose*

$$\mathrm{Gal}_K f = \mathrm{Aut}_K K(\theta_1, \ldots, \theta_n) \subset G$$

Alors le polynôme $g(T) = \prod_{y \in S_n.x} (T - y) \in K[T]$ admet une racine dans K, cette racine étant l'image de x par le morphisme évaluation $\phi : x_i \mapsto \theta_i$.

Démonstration Comme x est un élément dont le stabilisateur contient le groupe des automorphismes de $K(\theta_1, \ldots, \theta_n)$ (extension galoisienne de K), il est clair que $\phi(x)$ est stable sous l'action de $\mathrm{Gal}_K f$. En conséquence, $\phi(x)$ appartient donc à $K(\theta_1, \ldots, \theta_n)^{\mathrm{Gal}_K f}$, c'est-à-dire K. □

Ainsi tout polynôme $f(T) = T^4 + aT^3 + bT^2 + cT + d$ dont le groupe de Galois est inclus dans D_4 possède des coefficients liés par une relation dépendant de a, b, c, d et un scalaire $\lambda \in K$. Cette relation est

$$\lambda^3 - b\lambda^2 + (ac - 4d)\lambda + 4bd - a^2d - c^2 = 0$$

Précisons que la valeur λ est la valeur prise par $X_1X_2+X_3X_4$ lorsque l'on évalue celui-ci en les racines θ_i de f, en choisissant une certaine numérotation des θ_i... C'est l'appartenance de λ à K qui indique que le groupe de Galois de f est inclus dans D_4.

Propriété II.7.6 *Si $f(T) = T^4 + aT^3 + bT^2 + cT + d \in K[T]$ est séparable alors la résolvante tripartite l'est aussi, et il y a équivalence entre les assertions*
" $T^3 - bT^2 + (ac - 4d)T + 4bd - a^2d - c^2$ admet une racine dans K " et
" $\mathrm{Gal}_K f \subset D_4$ ".

Démonstration En effet les discriminants de f et de la résolvante tripartite sont égaux, ce qui est un fait peu banal pour une résolvante. Grâce au théorème II.6.2, on conclut qu'il y a effectivement équivalence entre les deux propositions. □

Du point de vue géométrique, on peut énoncer la dernière proposition comme suit :

Propriété II.7.7 *Soit la variété algébrique $\mathcal{V}$ de K^5 définie par la relation*

$$T^3 - BT^2 + (AC - 4D)T + 4BD - A^2D - C^2 = 0$$

On considère la projection $\pi : K^5 \to K^4$ en oubliant la coordonnée T. Soit $\mathcal{O} \subset K^4$ l'image réciproque de $K - \{0\}$ par l'application

$$\begin{array}{ccc} K^4 & \longrightarrow & K \\ (A,B,C,D) & \longmapsto & \mathrm{dis}(X^4 + AX^3 + BX^2 + CX + D) \end{array}$$

Il existe une bijection entre les points de $\pi(\mathcal{V}) \cap \mathcal{O}$ et les polynômes unitaires séparables de degré 4 dont le groupe de Galois est inclus dans le groupe diédral.

On peut paramétrer presque entièrement la variété $\mathcal{V}$ à l'aide de quatre paramètres : revenons sur la relation liant a, b, c, d, λ. On remarque que l'on peut facilement exprimer le paramètre b en fonction des autres en supposant $4d - \lambda^2 \neq 0$:

$$b = \frac{c^2 + a^2d - \lambda^3 + (4d - ac)\lambda}{4d - \lambda^2} \tag{II.4}$$

La condition $4d - \lambda^2 = 0$ entraîne l'égalité $a^2d = c^2$: en effet, comme la résolvante tripartite et $T^2 - 4d$ ont une racine en commun (à savoir λ), le résultant $(a^2d - c^2)^2$ est nul. Ainsi, si c^2 et a^2d ne sont pas égaux, la quantité $4d - \lambda^2$ n'est pas nulle.

En particulier, si a, c, d sont des indéterminées algébriquement indépendantes sur un corps k, alors b est une fraction rationnelle en a, c, d, λ et nous avons l'égalité des corps

$$k(a, b, c, d, \lambda) = k(a, c, d, \lambda)$$

Si de plus b est une quatrième indéterminée sur k, le corps $k(a, b, c, d, \lambda)$ est une extension pure de k.

En caractéristique distincte de 2.

Pour ne pas avoir à manipuler des fractions rationnelles, on effectue le changement de variables

$$d' \leftarrow 4^{-1}\lambda^2 - d \qquad c' \leftarrow \frac{c}{\lambda^2 - 4d} \qquad b' \leftarrow \frac{b}{\lambda^2 - 4d} \qquad a' \leftarrow \frac{a}{\lambda^2 - 4d} \qquad \lambda' \leftarrow \frac{\lambda}{\lambda^2 - 4d}$$

c'est-à-dire

$$\lambda \to 4\lambda' d' \qquad a \to 4a'd' \qquad b \to 4b'd' \qquad c \to 4c'd' \qquad d \to 4\lambda'^2 d'^2 - d'$$

Alors l'expression (II.4) de b en fonction des autres paramètres devient polynomiale (on laisse les *primes* de côté pour simplifier l'écriture) : $b = \lambda - c^2 - 4a^2d^2\lambda^2 + 4acd\lambda + a^2d$.

Finalement, la famille de polynômes obtenus est l'ensemble des polynômes s'écrivant :

$$f_{\substack{a,c\\d,\lambda}}(T) = T^4 + 4adT^3 + 4d\left(\lambda - c^2 - 4a^2d^2\lambda^2 + 4acd\lambda + a^2d\right)T^2 + 4cdT + 4\lambda^2d^2 - d \tag{II.5}$$

où a, c, d, λ sont des éléments du corps K. Notons $\mathcal{W}$ la sous-variété de $\mathcal{V}$ définie par $T^2 - 4D = 0$. A ce stade, on vient de calculer une paramétrisation de l'ensemble $\mathcal{V} - \mathcal{W}$, en caractéristique distincte de 2.

En fait, toute spécialisation en a, c, d, λ du polynôme $f_{\substack{a,c\\d,\lambda}}$ ne donne pas un polynôme dont le groupe de Galois est le groupe diédral : par exemple si K est un corps fini, aucune spécialisation ne convient (le groupe de Galois d'un polynôme sur un corps fini est cyclique donc différent de D_4). Nous allons chercher une famille de spécialisations pour $K = \mathbb{Q}$ telles que le groupe de Galois des polynômes obtenus soit effectivement D_4.

Posons par exemple $a = a_0 = 0,\ c = c_0 = 1,\ d = d_0 = -1,\ \lambda = \lambda_0 = 0$: on obtient alors le polynôme $f = T^4 + 4T^2 - 4T + 1$. Prouvons rapidement que le groupe de Galois de f est D_4 : par des réductions bien choisies modulo des premiers de $\mathbb{Z}$, ceci n'est pas difficile (voir le corollaire II.7.4). En effet modulo 3, $\overline{f}$ est irréductible donc f est irréductible dans $\mathbb{Z}[T]$: son groupe de Galois est donc un sous-groupe transitif de D_4. Si l'on factorise f modulo 5, on trouve $\overline{f} = (T+1)(T+3)(T^2+T+2)$: le groupe de Galois de f contient donc une transposition. Conclusion : $\mathrm{Gal}_{\mathbb{Q}}\, f = D_4$.

Pour montrer que $\mathrm{Gal}_{\mathbb{Q}}\, f = D_4$, il nous a suffit de tirer des informations de réductions modulo 3 et 5 : pour des spécialisations de a, c, d, λ respectivement égales à a_0, c_0, d_0, λ_0 modulo le produit $3.5 = 15$ on aura les mêmes résultats. Bien sûr on aurait pu choisir d'autres valeurs particulières $a_0 = 1,\ c_0 = 0,\ d_0 = -1,\ \lambda_0 = 0$ puis les premiers 11 et 5 pour démontrer des résultats identiques...

Résumé. Pour $a, c-1, d+1, \lambda \in 15\mathbb{Z}$, ou pour $a-1, c, d+1, \lambda \in 55\mathbb{Z}$ (ce sont des exemples parmi d'autres) le polynôme $f_{\substack{a,c\\d,\lambda}}$ (équation (II.5)) a pour groupe de Galois sur $\mathbb{Q}$ le groupe diédral.

En caractéristique 2.

Dans le cadre plus particulier, la paramétrisation quasi-complète de $\mathcal{V}$ (notation de la propriété II.7.7) est plus simple : en effet la relation (II.4) est réduite à

$$b = \frac{\lambda^3 + ac\lambda + c^2 + a^2 d}{\lambda^2} = \lambda + \frac{a}{\lambda}\frac{c}{\lambda}\lambda + \left(\frac{c}{\lambda}\right)^2 + d\left(\frac{a}{\lambda}\right)^2$$

En effectuant $a \leftarrow \dfrac{a}{\lambda}$ et $c \leftarrow \dfrac{c}{\lambda}$, on obtient $b = \lambda + ac\lambda + c^2 + da^2$.

Finalement, la famille de polynômes obtenus est l'ensemble des polynômes s'écrivant :

$$f_{\substack{a,c \\ d,\lambda}}(T) = T^4 + \lambda a T^3 + (\lambda + ac\lambda + c^2 + da^2)T^2 + \lambda c T + d \tag{II.6}$$

où a, c, d, λ sont des éléments du corps K de caractéristique 2. Notons $\mathcal{W}$ la sous-variété de $\mathcal{V}$ définie par $T = 0$. Nous venons de calculer une paramétrisation de l'ensemble $\mathcal{V} - \mathcal{W}$.

Nous allons maintenant spécialiser $f_{\substack{a,c \\ d,\lambda}}$ afin de trouver un polynôme dont le groupe de Galois soit le groupe diédral. Nous décidons de travailler dans le corps $\mathbb{F}_2$. Posons par exemple $a = 0, c = 1, \lambda = 1$, ce qui donne $f_d = T^4 + T + d \in \mathbb{F}_2(d)$. Montrons que $\mathrm{Gal}_{\mathbb{F}_2(d)} f_d$ est bien D_4 grâce au corollaire II.7.4. Comme d est une indéterminée sur $\mathbb{F}_2$, f_d est clairement irréductible. L'évaluation en $d = 0$ nous prouve que $\mathrm{Gal}_{\mathbb{F}_2(d)} f_d$ contient une transposition : $f_0 = T(T+1)(T^2+T+1)$. Comme $\mathrm{Gal}_{\mathbb{F}_2(d)} f_d$ est inclus dans D_4 (le polynôme f_d est fait pour cela), on conclut qu'il y a égalité.

Ce petit résultat démontre, grâce au théorème II.7.3, que $f_{\substack{a,c \\ d,\lambda}} \in \mathbb{F}_2(a, c, d, \lambda)[T]$ possède un groupe de Galois égal au groupe diédral : en effet son groupe de Galois est inclus dans D_4 (encore une fois, $f_{\substack{a,c \\ d,\lambda}}$ est fait pour cela...), et le groupe de Galois du spécialisé f_d de $f_{\substack{a,c \\ d,\lambda}}$ est D_4...

II.7.d Réduction modulo un idéal premier

Théorème II.7.3 (voir [38] pages 344-345) *Soit R un anneau intégralement clos et K son corps des fractions, $f \in R[X]$ un polynôme unitaire, $\mathfrak{p}$ un idéal premier de R. Si $\overline{f} \in R/\mathfrak{p}[X]$ est un polynôme séparable alors f est séparable et $\mathrm{Gal}_{\mathrm{Frac}(R/\mathfrak{p})} \overline{f}$ s'injecte dans $\mathrm{Gal}_K f$.*

Démonstration Soit θ_i les racines de f dans une clôture algébrique de K. Le groupe de Galois de f, $\mathrm{Gal}_K f$, opère sur $R' = R[\theta_1, \ldots, \theta_n]$. Ce dernier anneau est entier sur R, et l'ensemble des points fixes sous l'action de $\mathrm{Gal}_K f$ est égal à $K \cap R' = R$ car R est intégralement clos.

On est donc en situation du théorème I.1.1 : soit $\mathfrak{p}$ un idéal premier de R et $\mathfrak{p}'$ un idéal premier de R' tel que $\mathfrak{p} = R \cap \mathfrak{p}'$ (il existe toujours un idéal premier $\mathfrak{p}'$ vérifiant cela car R' est entier sur R). Soit k le corps des fractions de $R/\mathfrak{p}$ et k' celui de $R'/\mathfrak{p}'$. Alors k' est une extension normale de k et le morphisme canonique de

$$D(\mathfrak{p}') = \{g \in \mathrm{Gal}_K f \mid g\mathfrak{p}' = \mathfrak{p}'\} \subset \mathrm{Gal}_K f$$

dans le groupe $\mathrm{Aut}_k\, k'$ est surjectif.

En fait ce morphisme est injectif dans l'hypothèse où $\overline{f}$ est séparable : les racines $\overline{\theta_i}$ de $\overline{f}$ sont distinctes, ce qui impose aux racines θ_i de f de l'être. On a $f(T) = \prod_i (T - \theta_i)$, et dans k' on a

$$\overline{f}(T) = \prod_i \left(T - \overline{\theta_i}\right)$$

Les racines θ_i sont en bijection avec les $\overline{\theta_i}$. L'automorphisme $\mathrm{Id} \in \mathrm{Aut}_k\, k'$ se relève obligatoirement en $\mathrm{Id} \in \mathrm{Gal}_K\, f$ car les θ_i sont des générateurs de $\mathrm{Frac}\, R' = K(\theta_1, \ldots, \theta_n)$. Le morphisme canonique de $D(\mathfrak{p}')$ dans $\mathrm{Aut}_k\, k'$ est donc injectif. □

Définition II.7.1 *Précisons les trois notions de "type" suivantes :*

- *Le* ***type de factorisation*** *d'un polynôme est la suite décroissante des degrés des polynômes irréductibles formant sa décomposition en irréductibles.*
- *Le* ***type d'une permutation*** *de $\mathcal{S}_n$ est la suite décroissante des longueurs des cycles formant sa décomposition en cycles à supports disjoints.*
- *Le* ***type d'une partition*** *d'un entier n est une suite finie décroissante d'entiers positifs dont la somme vaut n.*

Propriété II.7.8 *Soit K un corps fini et $f \in K[X]$ séparable. Alors le type de la factorisation de f est le type d'un générateur quelconque de $\mathrm{Gal}_K\, f$ considéré comme une permutation des racines de f.*

Démonstration Le type de la factorisation de f est la suite décroissante des degrés des facteurs irréductibles de sa décomposition. Le degré d'un polynôme irréductible est égal au cardinal de l'orbite d'une de ses racines sous l'action du groupe des automorphismes $\mathrm{Gal}_K\, f$. Or ce dernier est cyclique car K est un corps fini : soit g un générateur de $\mathrm{Gal}_K\, f$, par exemple l'automorphisme de Frobenius $x \mapsto x^{|K|}$. Finalement, l'orbite d'une racine de f correspond à un certain cycle de la décomposition à supports disjoints de g. □

En juxtaposant les deux résultats précédents, on obtient :

Corollaire II.7.4 *Dans le cadre du théorème II.7.3, si de plus $R/\mathfrak{p}$ est un corps fini, alors $\overline{f}$ séparable implique que le type de $\overline{f}$ est le type d'un élément de $\mathrm{Gal}_K\, f \subset \mathcal{S}_n$.*

Chapitre III

Équations résolubles par radicaux

III.1 Un (tout petit) peu d'histoire

La résolubilité des équations polynomiales à l'aide de radicaux fût un problème à l'égal de la quadrature du cercle... Au XVI^e siècle, quelques initiés connaissaient des formules (ou des techniques) permettant de calculer les solutions des équations de degré inférieur à 4. Mais nombre de mathématiciens ont tenté de résoudre par radicaux les équations de degré 5 jusqu'au XVIII^e siècle, bien sûr sans y parvenir...

Références bibliographiques : [21], [26]

Alors que les Babyloniens savaient (grosso-modo) déjà résoudre les équations du second degré, il a fallu attendre l'année 1545 pour qu'enfin Cardan révèle au "grand public" la fameuse formule permettant de résoudre les équations du type $T^3 + aT = b$:

$$\sqrt[3]{\frac{b}{2} + \sqrt{\left(\frac{b}{2}\right)^2 + \left(\frac{a}{3}\right)^3}} + \sqrt[3]{\frac{b}{2} - \sqrt{\left(\frac{b}{2}\right)^2 + \left(\frac{a}{3}\right)^3}}$$

obtenue en fait par del Ferro vers 1500.

Toujours vers le milieu du XVI^e siècle, Ferrari trouve une méthode pour résoudre les équations de degré 4.

Cependant, les équations de degré 5 résistent à toute tentative. Entre 1683 et 1689, Tschirnhaus essaie de transformer une équation polynomiale $P(x) = 0$ en un système d'équations que l'on saurait résoudre : il pose $y = Q(x)$ où Q est un polynôme de degré strictement inférieur à celui de P, et dont les coefficients restent à déterminer pour que y^n soit rationnel. Une fois $y^n = c$ résolue, il suffira de résoudre $y = Q(x)$ par rapport à x, ce que l'on sait faire "par récurrence" puisque $\deg(Q) < \deg(P)$.

Cette méthode de Tschirnhaus est utilisable pour les équations de degré inférieur à 3 (voire 4), mais n'aboutit pas au résultat escompté en degré 5...

Dans les années 1770-1772, Lagrange essaie de comprendre pourquoi les mathématiciens subissent un tel échec. Il commença à étudier les fonctions de plusieurs variables, le nombre de valeurs prises par de telles fonctions lorsque l'on permute leurs arguments : par

exemple, $(x_1 + jx_2 + j^2x_3)^3$ ne prend au plus que deux valeurs si l'on échange x_1, x_2 et x_3 (les x_i sont supposés être les racines d'un polynôme du troisième degré et j représente une racine troisième de l'unité), $y_1y_2 + y_3y_4$ n'en prend que trois (si les y_i sont solutions d'une équation du quatrième degré)...

Ainsi Lagrange donna naissance au groupe symétrique $\mathcal{S}_n$, à la notion de stabilisateur d'une expression à plusieurs variables. Si x_1, x_2, x_3 sont trois indéterminées sur $\mathbb{Q}$, il savait par exemple que les expressions $x_1x_2 + x_3^2$ et $x_1^2 + x_2^2 + 2x_3$ étaient fonctions rationnelles l'une de l'autre puisqu'elles ont le même stabilisateur dans $\mathcal{S}_3$.

Par ses recherches, Lagrange obtint une méthode générale qui lui permettait de passer d'une équation de degré n à une autre de degré $(n-2)!$. Son principe expliquait donc pourquoi il était possible de résoudre les équations jusqu'au degré 4. Malheureusement, pour $n = 5$ Lagrange était ramené à résoudre une équation de degré 6... Il commenca largement à douter de la résolubilité des équations de degré 5.

Son intuition était on ne peut plus raisonnable puisqu'en 1826 Abel démontra qu'il était impossible de les résoudre par radicaux en général. Trois ans plus tard, ce dernier ajouta qu'il était cependant possible de calculer avec des radicaux les racines d'un polynôme si celui-ci possédait, en termes modernes, un groupe de Galois abélien.

En reprenant la voie ouverte par Abel (mort en 1829), Galois développa la théorie des extensions de corps. L'idée géniale de Galois fût de mettre en correspondance le groupe d'une équation et le groupe des automorphismes du corps engendré par toutes les racines de l'équation. Il démontra notamment en 1831 que les équations de degré 5 ne pouvaient pas être résolues de façon générale, et qu'il en était de même pour les degré plus important. Il montra que la nature du corps de base influe sur le groupe des automorphismes, donc sur la possibilité de résoudre une équation par radicaux. Voici sa célèbre réponse définitive au problème de la résolubilité par radicaux :

Théorème III.1.1 (Galois, voir [33] pages 417-432) *Une équation (irréductible) est résoluble par radicaux si et seulement si le groupe de cette équation est résoluble.*

Savoir ce grand théorème de Galois est une chose, mais donner une méthode pour déterminer si ce groupe est résoluble, donner des formules plus ou moins explicites pour obtenir les racines en sont deux autres !

Afin d'obtenir ces formules, nous utiliserons l'algèbre de décomposition universelle qui nous permettra de manipuler les racines de polynômes plus ou moins génériques que nous serons amenés à considérer. Dans le cadre particulier des polynômes génériques, leur algèbre de décomposition universelle représentera le corps de décomposition de ces polynômes (voir chapitre II).

III.2 Équations de degré 3

Dans ce qui suit, on se place sur un corps k de caractéristique différente de 2 et 3. Soit $T^3 + aT^2 + bT + c \in k(a, b, c)[T]$ le polynôme générique de degré 3. Notre but est de calculer ses racines avec des radicaux.

En premier lieu, il s'agit de simplifier l'équation : par exemple on passe de l'équation $T^3 + aT^2 + bT + c = 0$ à l'équation $f = T^3 + pT + q = 0$ en effectuant le changement de variable $T \to T - a/3$. Ceci a pour effet de diminuer le nombre de paramètres, ce qui n'est pas négligeable lorsque le moment d'écrire des formules arrive... Nous noterons x_1, x_2, x_3 les trois racines de f.

Résolution générique

Lagrange avait remarqué à juste titre que l'expression $(x_1 + jx_2 + j^2x_3)^3$ ne prend au plus que deux valeurs lorsque l'on permute les x_i (j représente une racine primitive troisième de l'unité).

Prouvons ce résultat : considérons les corps $K = k(p, q, j)$ où p et q sont des indéterminées, $E = K(x_1, x_2, x_3)$. L'extension E de K est galoisienne et son groupe d'automorphismes est $\mathcal{S}_3$: en effet le polynôme $f = T^3 + pT + q$ est irréductible dans $K[T]$ et son discriminant n'est un carré dans K. Posons maintenant

$$h = x_1 + jx_2 + j^2x_3 \qquad \text{résolvant de Lagrange}$$

Cet élément de E est primitif car nous pouvons exprimer les x_i en comme fonction rationnelle en h :

$$x_1 = R(h), \quad x_2 = R(j^{-1}h), \quad x_3 = R(jh), \quad \text{avec } R(T) = T/3 - pT^{-1}$$

Ces relations sont obtenues en utilisant l'algèbre de décomposition universelle, grâce à une fonction cherchant à lier par combinaison linéaire les vecteurs x_i et les puissances de h sur le corps K.

En fait, h a été construit pour avoir la propriété suivante : soit le 3-cycle $\sigma = (3, 2, 1)$, alors $\sigma h = jh$, si bien que $\sigma(h^3) = (\sigma h)^3 = h^3$. Ceci implique que h^3 est invariant par le groupe engendré par σ que je note C_3.

Ainsi on obtient $h^3 \in E^{C_3}$ et nous nous retrouvons dans cette situation galoisienne :

$$K = E^{\mathcal{S}_3} \xrightarrow{2} E^{C_3} \xrightarrow{3} K(h) = E = K(x_1, x_2, x_3)$$

On voit alors que le degré de h^3 sur K est au plus 2... On peut donc exprimer h^3 avec des radicaux, par suite h, et enfin les x_i.

En effet, le polynôme minimal de h^3 sur K est $\mu_{h^3} = T^2 + 27qT - 27p^3$.

> Remarque. Nous "prouvons" l'exactitude de l'expression de μ_{h^3} en disant simplement que μ_{h^3} a été calculé grâce à la fonction `minimalPolynomial` implantée dans l'algèbre de décomposition universelle de f.

On obtient finalement

$$h = \sqrt[3]{\frac{3}{2}\left(-9q + \sqrt{3}\sqrt{27q^2 + 4p^3}\right)}$$

Le problème des déterminations des racines $\sqrt[n]{\ }$ n'en est pas un : il y a six valeurs possibles pour l'expression ci-dessus en fonction des radicaux, ces six valeurs représentent les six racines du polynôme minimal de h sur K. Aucune distinction n'est à faire entre ces racines. L'écriture "globale" des x_i en fonction de h est indépendante de la détermination par radicaux de h que l'on a choisi : un autre choix de h revient à permuter les x_i.

Spécialisation

Finalement, ces résultats génériques peuvent se spécialiser à n'importe quel polynôme $f = T^3 + pT + q \in k[T]$ si h ne se spécialise pas en 0. Or, il est clair au vu de μ_{h^3} qu'on peut toujours choisir $h \neq 0$ si $f \neq T^3$.

On peut remarquer que si $-\operatorname{dis}(f) = 27q^2 + 4p^3 > 0$ alors f n'a qu'une racine réelle (à savoir x_1 avec les notations précédentes), et que celle-ci s'exprime avec des radicaux réels. En revanche, si f possède trois racines réelles distinctes, ce qui est équivalent à $-\operatorname{dis}(f) = 27q^2 + 4p^3 < 0$, celles-ci ne s'expriment pas avec des radicaux réels.

III.3 Équations de degré 4

Dans ce qui suit, on se place sur un corps k de caractéristique différente de 2 et 3. Notre but est de calculer les racines d'un polynôme de degré 4 avec des radicaux. Effectuons une première simplification classique : à l'aide de la translation $T \mapsto T + \frac{\operatorname{coeff}_{X^3}(f)}{4}$, nous nous ramenons au cas où $f = T^4 + aT^2 + bT + c$.

Résolution générique

Soit $i = \sqrt[4]{1}$ une racine primitive quatrième de 1. Soit $K = k(a, b, c, i)$ où a, b, c sont des indéterminées sur k. Les racines de f dans une clôture algébrique sont notées $x_1, \ldots, x_4$ et le groupe de Galois de f sur K est bien sûr $\mathcal{S}_4$. Considérons les éléments $h_i \in K(x_1, x_2, x_3, x_4)$ suivants :

$$\begin{pmatrix} h_0 \\ h_1 \\ h_2 \\ h_3 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}$$

> Remarque. Le terme particulier h_0 est égal à la somme des racines x_i. Par conséquent, dans notre cadre particulier, $h_0 = 0$ car notre équation $T^4 + aT^2 + bT + c = 0$ n'a pas de terme en T^3.

Les h_i sont nommés les résolvants de Lagrange. Leur intervention est fondamental dans la résolution des équations polynomiales. Par exemple, ils forment un système de Vandermonde composé verticalement et horizontalement des puissances de i. On peut inverser le système afin d'exprimer simplement les x_i en fonctions des h_i :

$$\begin{aligned} x_1 &= (h_0 + h_1 + h_2 + h_3)/4 \\ x_2 &= (h_0 - ih_1 - h_2 + ih_3)/4 \\ x_3 &= (h_0 - h_1 + h_2 - h_3)/4 \\ x_4 &= (h_0 + ih_1 - h_2 - ih_3)/4 \end{aligned}$$

Les expressions des x_i en fonction des h_i sont extrêmement simples, mais il reste à déterminer "les valeurs en radicaux" des h_i pour $i = 2, 3, 4$. En clair, le problème de résolution par radicaux est simplement transporté des x_i sur les h_i.

Nous allons maintenant mettre en évidence une deuxième cause majeure de l'importance des résolvants de Lagrange. Étudions l'action de $D_4 = \langle (4,3,2,1),\ (1,3)\rangle$ sur ces h_i :

$$\begin{array}{lll} (4,3,2,1)h_1 = ih_1 & (4,3,2,1)h_2 = -h_2 & (4,3,2,1)h_3 = -ih_3 \\ (1,3)h_1 = -h_3 & (1,3)h_2 = h_2 & (1,3)h_3 = -h_1 \end{array}$$

On constate facilement que

h_1^2 et h_3^2 sont invariants par $(4,3,2,1)^2 = (1,3)(2,4)$,

h_2 invariant par $S_2 \times S_2 = \langle (1,3),(2,4)\rangle$,

h_1^4, h_3^4, $h_2h_3^2$ et $h_2h_3^2$ invariants par $C_4 = \langle (4,3,2,1)\rangle$,

h_2^2, h_1h_3 et $h_2(h_1^2+h_3^2)$ invariants par D_4 (plus précisément, $h_2(h_1^2+h_3^2)$ appartient à K).

Considérons le diagramme suivant :

$$K = E^{\mathcal{S}_4} \xrightarrow{3} E^{D_4} \xrightarrow{2} E^{S_2\times S_2} \xrightarrow{2} E^{(1,3)(2,4)} \xrightarrow{2} E = K(x_1,x_2,x_3,x_4)$$

Comme chaque étage est de degré 2 ou 3, il semble bien que l'on puisse trouver des formules avec radicaux exprimant les x_i...

Comme nous sommes amenés à calculer des expressions dans E^{D_4}, il est tout à fait naturel d'en calculer un élément primitif sur lequel nous pourrons appuyer nos futurs calculs : soit

$$d = h_2^2/4 \quad \in E^{D_4}$$

On calcule le polynôme minimal de d sur K (avec la fonction `minimalPolynomial`) :

$$\mu_{d:K} = T^3 + 2aT^2 + (a^2-4c)T - b^2$$

ce qui prouve bien que d est un élément primitif de E^{D_4} sur K. Le polynôme minimal de h_2 sur $K(d)$ est bien sûr T^2-4d. Ainsi h_2 est calculable avec des radicaux, et nous avons en particulier $K(h_2) = E^{S_2\times S_2}$. Nous pouvons maintenant connaître le polynôme minimal de h_1^2 sur $K(h_2)$ grâce aux relations (obtenues par calcul dans l'algèbre de décompositoin universelle) :

$$h_1h_3 = -4a - 2d \qquad \text{et} \qquad (h_1^2+h_3^2)h_2 = -16b$$

$$\mu_{h_1^2:K(h_2)} = T^2 - (h_1^2+h_3^2)T + (h_1h_3)^2 = T^2 + 16bh_2^{-1}T + (4a+2d)^2$$

Nous avons alors moyen de calculer par radicaux h_1^2, puis h_1. Enfin, nous pouvons faire de même avec h_3 grâce à $h_3 = (-4a-2d)/h_1$.

Remarquons qu'il y a en tout et pour tout $3.2.2.2 = 24 = |\mathcal{S}_4|$ affectations possibles de h_1 : 3 venant de d, 2 de h_2, 2 de h_1^2 et 2 de h_1. Elles correspondent aux 24 racines du polynôme minimal de h_1 sur K et sont équivalentes pour ce que nous voulons en faire... c'est-à-dire calculer les x_i.

Spécialisation

Finalement, ces résultats génériques peuvent se spécialiser à n'importe quel polynôme $f = T^4 + aT^2 + bT + c \in k[T]$, à condition que h_1 et h_2 ne deviennent pas nuls. Pour cela, supposons que le polynôme f n'est pas bicarré. Nous pouvons alors imposer $d \neq 0$ (pour avoir $h_2 \neq 0$) et $d \neq -2a$ (pour avoir $h_1 \neq 0$) : en effet, $\mu_{d:K} = T^3 + 2aT^2 + (a^2 - 4c)T - b^2$ admet nécessairement une racine (dans une clôture algébrique de k) autre que 0 et $-2a$ si f n'est pas bicarré.

Résumé

On considère un polynôme $f = T^4 + aT^2 + bT + c$ non bicarré. Soit $d \notin \{0, -2a\}$ une racine de $T^3 + 2aT^2 + (a^2 - 4c)T - b^2$, $h_2 = 2\sqrt{d}$ et $h_3 = (-4a - 2d)/h_1$ où

$$h_1 = \sqrt{-8bh_2^{-1} \pm \sqrt{32b^2d^{-1} - (4a + 2d)^2}} \neq 0$$

Alors les racines de f sont

$$x_{k+1} = ((-i)^k h_1 + (-1)^k h_2 + i^k h_3)/4 \qquad k \in \{0, 1, 2, 3\}$$

Une autre stratégie pour résoudre les équations de degré 4 consiste à utiliser la même technique que précédemment avec la tour d'extensions

$$K = E^{\mathcal{S}_4} \xrightarrow{3} E^{D_4} \xrightarrow{2} E^{C_4} \xrightarrow{4} E = K(x_1, x_2, x_3, x_4)$$

où l'on franchit le dernier étage grâce la propriété $h_1^4 \in E^{C_4}$.

Le lecteur pourra trouver une troisième méthode dans [59], page 182.

III.4 Équations de degré 5

III.4.a Équations irréductibles résolubles de degré premier

Soit p un nombre premier. Notons γ le p-cycle canonique dans le groupe $\mathcal{S}_p$ et C_p le sous-groupe de $\mathcal{S}_p$ engendré par γ. On appelle **groupe métacyclique** engendré par γ le normalisateur M_p de C_p dans $\mathcal{S}_p$. Il est bien connu que M_p est l'image du groupe $\mathrm{AGL}_1(\mathbb{F}_p)$ par l'isomorphisme canonique $\mathrm{Perm}(\mathbb{F}_p) \simeq \mathcal{S}_p = \mathrm{Perm}(\{1, \ldots, p\})$, et C_p l'image de $\mathbb{T}_p$.

Rappel. Quel que soit l'anneau R, le groupe des similitudes de R

$$\mathrm{AGL}_1(R) = \{x \mapsto b + ax,\ b \in R, a \in \mathrm{U}(R)\}$$

est isomorphe au produit semi-direct $R \rtimes \mathrm{U}(R)$.

Le cardinal de $\mathrm{AGL}_1(\mathbb{Z}/n\mathbb{Z})$ est donc $n\phi(n)$.

Si p est un nombre premier, tout groupe transitif sur $\mathbb{F}_p$ contient un unique sous-groupe cyclique d'ordre p, isomorphe au groupe des translations sur $\mathbb{F}_p$

$$\mathbb{T}_p = \{x \mapsto b + x,\ b \in \mathbb{F}_p\}$$

Les sous-groupes conjugués de M_p dans $\mathcal{S}_p$ sont appelés **sous-groupes métacycliques principaux**. On vérifie alors que tout sous-groupe de $\mathcal{S}_p$ de cardinal pm avec $m \leq p-1$ est un sous-groupe d'un et un seul sous-groupe métacyclique principal, et en conséquence on a nécessairement $m \mid p-1$. Enfin, on démontre que les sous-groupes résolubles transitifs maximaux de $\mathcal{S}_p$ sont ses sous-groupes métacycliques principaux (voir par exemple [4]).

Considérons un polynôme f à coefficients dans un corps k, de degré p, séparable et irréductible. Les propriétés ci-dessus permettent de caractériser la résolubilité par radicaux de f sur k, i.e. la résolubilité du groupe de Galois de f sur k. Comme $\mathrm{Gal}_k f$ est transitif sur les racines de f (appartenant à une clôture algébrique de k), ce groupe contient un p-cycle. Numérotons les racines de f de 1 à p et identifions naturellement $\mathrm{Gal}_k f$ dans $\mathcal{S}_p$ de telle sorte que C_p soit inclus dans $\mathrm{Gal}_k f$. Alors f est résoluble par radicaux sur k si et seulement si $\mathrm{Gal}_k f \subset M_p$.

Théorème III.4.1 (voir [62], pages 187-188) *Une équation séparable de degré premier p irréductible est résoluble par radicaux si et seulement si son groupe de Galois est contenu dans le groupe métacyclique M_p.*

S'il en est ainsi, un élément du groupe $\mathrm{Gal}_k f$ qui fixe deux racines quelconques de f est nécessairement Id. Par suite, le corps de décomposition de f sur k est engendré par uniquement deux racines quelconques de f.

Réciproquement, si le corps de décomposition de f sur k est engendré par deux racines de f, le groupes de Galois de f est au plus de cardinal $p(p-1)$, donc $\mathrm{Gal}_k f$ est inclus dans un groupe métacyclique principal. Plus précisément, $\mathrm{Gal}_k f \subset M_p$ puisque $C_p \subset \mathrm{Gal}_k f$.

C'est en substance le théorème découvert par Galois (voir [33] page 432), à partir duquel il a inventé le concept de groupe résoluble.

Théorème III.4.2 *Pour qu'une équation de degré premier et irréductible soit résoluble, il faut et il suffit que deux quelconques des racines étant connues, les autres s'en déduisent "rationnellement".*

III.4.b Simplification d'une équation de degré 5

Il est bien connu que le problème de la résolubilité des équations quelconques de degré 5 en caractéristique 0 se ramène au problème "plus simple" qui consiste à résoudre uniquement les équations du type

$$T^5 + pT + q = 0 \qquad \text{forme de Bring Jerrard}$$

Théorème III.4.3 (F. Klein) *Soit $p \geq 5$ un nombre premier et le polynôme*

$$f(T) = T^p + a_1 T^{p-1} + \cdots + a_p \quad \in k[T], \qquad k \subset \mathbb{C}$$

Les racines de f sont notées $x_1, \ldots, x_p$. Il existe alors une extension élémentaire k'/k (en particulier, les éléments de k' sont calculables avec des radicaux), et un polynôme $\phi(T)$

de $k'[T]$ non constant et de degré au plus 4 tel que le polynôme $g(T) = \prod_{i=1}^{p} \big(T - \phi(x_i)\big)$ soit de la forme

$$g(T) = T^p + b_4 T^{p-4} + \cdots + b_p \qquad\qquad b_i \in k'$$

> Rappel. Une extension k'/k est dite **élémentaire** s'il existe des extensions intermédiaires $k_1, \ldots, k_n$
>
> $$k = k_1 \subset k_2 \subset \cdots \subset k_{n-1} \subset k_n = k'$$
>
> telles que le degré de k_{i+1}/k_i soit au plus 4.

Une preuve de ce résultat est donnée dans [2] (pages 22-25). Le passage du polynôme f au polynôme g est communément appelé **transformation de Tschirnhaus**. Remarquer que les coefficients de cette transformation appartiennent à k' et non au corps de base k.

Illustration de ce théorème Nous allons voir comment on peut rendre nuls, par des changements de variable bien choisis, les coefficients en T^4 et T^3 d'une équation de degré 5 irréductible à coefficients dans un corps k. L'élimination du coefficient en T^2 peut théoriquement se faire de manière identique (théorème III.4.3), mais les formules que l'on obtient sont imposantes... trop pour être couchées sur le papier !

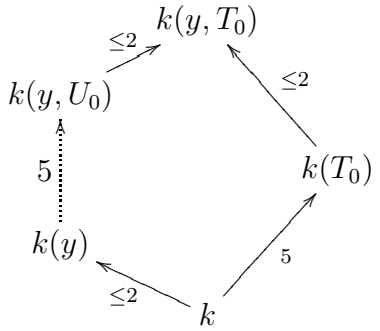
Le lecteur constatera que les changements de variable proposés ci-dessous sont tout-à-fait valables en caractéristique distincte de 2 et 5.

Considérons un polynôme irréductible $f = T^5 + aT^4 + bT^3 + cT^2 + dT + e$. A l'aide de la translation très classique $T \mapsto T + \frac{a}{5}$, on se ramène au cas où $a = 0$, toutes les autres hypothèses restant inchangées.

Maintenant, essayons d'éliminer le coefficient en T^3. Considérons une racine T_0 de $f = T^5 + bT^3 + cT^2 + dT + e$ ainsi que l'élément

$$U_0 = T_0^2 + yT_0 + z \qquad \text{où} \qquad z = \frac{2b}{5} \quad \text{et} \quad y^2 + \frac{3c}{b}y + \frac{10d - 3b^2}{5b} = 0$$

Cet élément U_0 est nécessairement un élément de degré 5 sur $k(y)$ comme le montre le diagramme ci-contre (on rappelle que f est irréductible sur k, donc $\dim_k k(T_0) = 5$). On déduit également l'égalité entre $k(y, T_0)$ et $k(y, U_0)$.



Les éléments z (appartenant à k) et y (de degré 1 ou 2 sur k) ont été choisis pour que le polynôme minimal de U_0 sur k soit un polynôme (unitaire de degré 5) ayant des coefficients nuls en U^4 et U^3. Ce polynôme minimal est donné simplement par

$$P(U) = \mathrm{res}_T(f(T), U - T^2 - yT - z) \quad \in k[U]$$

Si nous réussissons à calculer la racine U_0 de $P(U)$ avec des radicaux, nous pourrons en faire de même avec T_0 : en effet, l'égalité $k(y, T_0) = k(y, U_0)$ nous montre que T_0 est exprimable comme une fraction en y et U_0.

Il reste cependant à connaître explicitement cette relation donnant T_0 en fonction de y et U_0. Tous les sous-résultants (voir chapitre B) des deux polynômes $f(T)$ et $T^2+yT+z-U$ (vus comme des polynômes en T) s'annulent en (T_0, U_0), car ils appartiennent à l'idéal engendré par ces deux polynômes. En particulier le sous-résultant d'indice 1 (de degré 1 en T) nous donne :

$$T_0 = -\frac{(10b - 25U_0)y^3 + (2b^2 + 15U_0b - 50U_0^2)y + 25e + (-10b + 25U_0)c}{25y^4 + (-5b + 75U_0)y^2 - 25cy + 25d - 6b^2 + 5U_0b + 25U_0^2}$$

Le dénominateur de cette fraction ne peut pas être nul car U_0 est de degré 5 sur $k(y)$. Nous venons de retrouver la valeur de T_0 en fonction de U_0 et y.

III.4.c Résolution générique

Dans ce qui suit, on se place sur un corps k de caractéristique différente de 2 et 5. Notre but est de calculer les racines d'un polynôme de degré 5 avec des radicaux lorsque ceci est possible.

Nous allons reprendre la stratégie que nous avons utilisée dans la section III.3 : soit ε une racine cinquième primitive de l'unité, le corps $K = k(p, q, \varepsilon)$ où p, q sont des indéterminées sur k, et le polynôme

$$f = T^5 + pT + q \in k(p, q)$$

Ses racines, dans une clôture algébrique de K, sont notées $x_1, \ldots, x_5$. Son groupe de Galois sur K est $\mathcal{S}_5$.

> Remarque. Pour montrer que le groupe de Galois de f sur $k(p, q)$ est $\mathcal{S}_5$, il suffit d'utiliser les résultats qui suivent dans cette section. On vérifie tout d'abord que f est irréductible dans $k[p, q, t]$ car de degré 1 et unitaire en q. Grâce au théorème III.4.4, le groupe de Galois de f n'est pas inclus dans le groupe métacyclique car la résolvante de Cayley n'a pas de racine dans $k(p, q)$: en effet, si une racine de cette résolvante existait dans $k(p, q)$, son degré en q n'appartiendrait pas à $\mathbb{Z}$, ce qui est absurde...
>
> De même, on montre facilement que le discriminant de f (qui est $5^5q^4 + 2^8p^5$) n'est pas un carré dans $k(p, q)$ car son degré en p n'est un multiple de 2. Ainsi, le groupe de Galois de f n'est pas un groupe pair.
>
> Finalement, il ne reste que $\mathcal{S}_5$ comme seule possibilité !

Considérons les résolvants de Lagrange :

$$h_i = x_1 + \varepsilon^i x_2 + \varepsilon^{2i} x_3 + \varepsilon^{3i} x_4 + \varepsilon^{4i} x_5 \qquad i \in \{0, 1, 2, 3, 4\}$$

Remarquer que dans notre cas, nous avons $h_0 = 0$.
On peut naturellement exprimer les x_i en fonction des h_i comme nous l'avons fait en degré 4 :

$$x_{i+1} = (h_0 + \varepsilon^{-i}h_1 + \varepsilon^{-2i}h_2 + \varepsilon^{-3i}h_3 + \varepsilon^{-4i}h_4)/5 \qquad i \in \{0,1,2,3,4\}$$

Ceci étant, h_i^5 est invariant sous l'action de $\sigma = (5,4,3,2,1)$ car $\sigma h_i = \varepsilon^i h_i$. Considérons le diagramme suivant :

$$K = E^{\mathcal{S}_5} \xrightarrow{6} E^{F_{20}} \xrightarrow{2} E^{D_5} \xrightarrow{2} E^{C_5} \xrightarrow{5} E = K(x_1,x_2,x_3,x_4,x_5)$$

où $C_5 = \langle\sigma\rangle$, D_5 le groupe diédral engendré par C_5 et la permutation $(2,5)(3,4)$, et enfin F_{20} le groupe métacyclique, ou de Frobenius, de cardinal 20 engendré par D_5 et $(2,3,5,4)$.

> Remarque. D.S. Dummit étudie la même tour d'extensions dans [30]. En revanche, dans [3], J.M. Arnaudiès considère le diagramme
>
> $$K = E^{\mathcal{S}_5} \xrightarrow{2} E^{\mathcal{A}_5} \xrightarrow{6} E^{D_5} \xrightarrow{2} E^{C_5} \xrightarrow{5} E = K(x_1,x_2,x_3,x_4,x_5)$$
>
> Cela montre qu'il n'y a pas qu'une seule approche possible du problème...

On remarque que les étages à descendre sont au nombre de 4 : le passage de E à E^{C_5} se fait "classiquement" avec les h_i grâce à $h_i^5 \in E^{C_5}$: les h_i peuvent donc s'exprimer avec des radicaux sur E^{C_5}. Le deuxième étage, de E^{C_5} à E^{D_5}, ne pose pas de problème puisqu'il est de degré 2. Idem pour le suivant : E^{D_5} à $E^{F_{20}}$. Quand au dernier, il ne se franchit pas si le polynôme f n'est pas résoluble !

Le théorème III.4.1 nous montre que le corps de décomposition d'un polynôme irréductible de degré 5 résoluble par radicaux ne peut pas être "très gros", c'est-à-dire au plus de dimension $p(p-1)$, ce qui donne 20 quand $p = 5$.

La première chose à faire est donc de s'assurer que l'on ne cherche pas à résoudre par radicaux une équation qui n'est pas résoluble... Est-il facile de voir si le groupe de Galois d'un polynôme est inclus dans $M_5 \simeq \mathrm{AGL}_1(\mathbb{F}_5) \simeq F_{20}$? La réponse est oui : il s'agit d'un résultat classique de théorie de Galois.

En utilisant la propriété III.5.1 et le corollaire III.5.2, (pages 91 et 94), nous obtenons le théorème suivant :

Théorème III.4.4 *Le groupe de Galois sur un corps K (de caractéristique distincte de 2 et 5) d'un polynôme séparable irréductible $f \in K[T]$ est contenu dans le groupe métacyclique F_{20} si et seulement si la résolvante de Cayley évaluée en les coefficients de ce polynôme possède une racine dans K.*

Pour les polynômes du type $f = T^5 + pT + q$, la "résolvante de Cayley" s'écrit

$$g = \left[T^3 - 5pT^2 + 15p^2T + 5p^3\right]^2 - \mathrm{dis}(f)T$$

Remarque. Le calcul de g peut se faire dans l'algèbre de décomposition universelle. En fait, g est la résolvante associée au résolvant de Cayley divisé par 4,

$$b = \big[(x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_1) - (x_1x_3 + x_3x_5 + x_5x_2 + x_2x_4 + x_4x_1)\big]^2/4$$

car celui-ci donne une résolvante plus "conviviale", i.e. avec des coefficients plus petits que ceux de la résolvante de Cayley classique. Cette résolvante g est le polynôme minimal (en terrain générique) de b sur K. Elle a la très bonne propriété d'être toujours séparable lorsque le polynôme f est irréductible et séparable en caractéristique distincte de 2 et 5 (voir la section III.5).

Dans l'algèbre de décomposition universelle, on remarque aussi que b est égal au résolvant de Serret auquel on a ajouté une constante de k (à savoir $3p$).

Pour résoudre l'équation $f = 0$, il faut donc trouver une racine à cette fameuse résolvante de Cayley g. Elle existe dans $E^{F_{20}}$ puisque le polynôme g provient d'un F_{20}-résolvant : il s'agit de b. Pour résoudre par radicaux l'équation $f = 0$, nous n'allons plus travailler en prenant K comme corps de base, mais plutôt

$$K' = K(b) = k(p, q, \varepsilon, b)$$

Ainsi nous nous retrouvons dans la situation résoluble suivante :

$$K' = E^{F_{20}} \xrightarrow{2} E^{D_5} \xrightarrow{2} E^{C_5} \xrightarrow{5} E = K'(x_1, x_2, x_3, x_4, x_5)$$

Il ne reste plus qu'à trouver un élément primitif de E^{D_5} sur le corps $K' = E^{F_{20}}$ que l'on exprimera avec des radicaux sur K', ensuite nous calculerons les $h_i^5 \in E^{C_5}$ par radicaux, et finalement les racines x_i de f en fonction des h_i.

Soit $d = (2\varepsilon + 2\varepsilon^4 + 1)(x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_1)$.

Remarque. La valeur $2\varepsilon + 2\varepsilon^4 + 1$ n'est autre qu'une racine carrée de 5. Ce facteur n'est là que pour rendre les expressions à venir moins repoussantes...

Cette quantité d est invariante par D_5 et nous avons la relation

$$d^2 = 5b$$

Nous pouvons facilement constater cette dernière car $4b = \left(\dfrac{d - (2,3,5,4).d}{2\varepsilon + 2\varepsilon^4 + 1}\right)^2$ et de plus $d + (2,3,5,4).d = 0$. Peu importe la détermination de d, cela ne fera que permuter les racines x_i. Ainsi d est un élément primitif de E^{D_5} car d n'appartient pas à $K' = E^{F_{20}}$.

Maintenant on peut calculer des polynômes de degré 2 qui ont les h_i^5 pour racines. Pour cela, étudions l'action de F_{20}, c'est-à-dire $\tau = (2,3,5,4)$ et $\sigma = (5,4,3,2,1)$, sur les h_i : on peut facilement vérifier les formules suivantes (avec l'algèbre de décomposition universelle par exemple) :

$$\begin{array}{lllll} \tau h_1 = h_3 & \tau h_3 = h_4 & \tau h_4 = h_2 & \tau h_2 = h_1 & \sigma h_i = \varepsilon^i h_i \\ \tau h_1^5 = h_3^5 & \tau h_4^5 = h_2^5 & h_1h_4 = d & h_2h_3 = -d & \end{array}$$

Nous voyons, entre autre, que les quantités

$$h_1^5+h_4^5 \qquad h_2^5+h_3^5 \qquad h_1h_4 \qquad h_2h_3 \qquad h_2h_1^3+h_3h_4^3 \qquad h_3h_1^2+h_2h_4^2$$

sont invariantes par $D_5=\langle\tau^2,\sigma\rangle$. En particulier

$$h_1h_4=d \qquad \text{et} \qquad h_2h_3=-d$$

Ainsi h_1^5,h_4^5 et h_2^5,h_3^5 sont respectivement racines des polynômes

$$\begin{array}{ll}\mu_{14}=T^2-(h_1^5+h_4^5)T+(h_1h_4)^5=T^2-(u+vd)T+d^5 & u,v\in K'\\ \mu_{23}=T^2-(h_2^5+h_3^5)T+(h_2h_3)^5=T^2-(u-vd)T-d^5 & \end{array}$$

Pour les polynômes de la forme $f=T^5+pT+q$, les scalaires u et v s'écrivent :

$$\begin{array}{l}u=\left(-15625q^4-100p^5+324p^4b-376p^3b^2+184p^2b^3-36pb^4+4b^5\right)/10q^3\\ v=\left(15625q^4+375p^5-840bp^4+695b^2p^3-275b^3p^2+50b^4p-5b^5\right)/2p^3q\end{array}$$

(Ces formules ont été calculées dans l'algèbre de décomposition universelle de f sur le corps $K=k(p,q)$.)

On peut alors déterminer les racines de ces deux polynômes, respectivement :

$$\frac{u+vd\pm\sqrt{(u+vd)^2-4d^5}}{2} \qquad \frac{u-vd\pm\sqrt{(u-vd)^2+4d^5}}{2}$$

Un dernier problème est de savoir comment affecter ces quatre valeurs à h_1^5 et h_4^5 d'une part et h_2^5 et h_3^5 d'autre part. On a cependant une petite tolérance : on peut choisir arbitrairement une affectation parmi ces quatre. Alors les autres seront déterminées de façon unique car les h_i $(i>0)$ sont des éléments primitifs de E : il est facile de constater qu'ils ont 20 conjugués au-dessus de K' (2 venant de d, 2 de h_i^5, 5 de h_i). Il faut donc trouver suffisamment de relations entre les h_i pour savoir comment les affecter judicieusement.

Empressons-nous de fixer arbitrairement h_1. Alors h_4 nous est donné par d/h_1 car $h_1h_2=d$. Il ne reste plus qu'à trouver h_2 et h_3. Alors les relations $h_2h_1^3+h_3h_4^3\in K'(d)$ et $h_3h_1^2+h_2h_4^2\in K'(d)$ nous donnent un système linéaire que nous pouvons résoudre. Pour les polynômes de la forme $f=T^5+pT+q$, nous obtenons :

$$\begin{pmatrix}h_2\\h_3\end{pmatrix}=\frac{1}{h_1^5-h_4^5}\begin{pmatrix}h_1^2 & -h_4^3\\ -h_4^2 & h_1^3\end{pmatrix}\begin{pmatrix}u'\\v'd\end{pmatrix}$$

où

$$\begin{array}{l}u'=\left(3125q^4+50p^5-137p^4b+132p^3b^2-54p^2b^3+10pb^4-b^5\right)d/10p^2q^2\\ \qquad\quad -(125p+15b)/2\\ v'=\left(-3125q^4-25p^5+81p^4b-94p^3b^2+46p^2b^3-9pb^4+b^5\right)/125pq^3\end{array}$$

III.4.d Spécialisation

Les relations étudiées dans le cadre "générique" peuvent se spécialiser sans difficulté jusqu'au moment où l'on calcule les h_i en fonction de h_1. Il faut par exemple que h_1 ne

soit pas nul : si c'est malheureusement le cas, il faut prendre une autre détermination de h. Si aucune d'entre elles ne convient, cela implique que les h_i et x_i sont tous nuls...

Il faut également s'assurer que $h_1^5 - h_4^5$ n'est pas nul. Montrons par l'absurde qu'on ne peut pas avoir simultanément $h_1^5 = h_4^5$ et $h_2^5 = h_3^5$ si le polynôme f est irréductible dans $k[T]$.

Supposons que ce soit effectivement le cas : on a d'une part

$$h_1^5 = (h_1^5 + h_4^5)/2 = (u + vd)/2 \quad \in k(d)$$

et d'autre part

$$h_1^2 = \varepsilon^j h_1 h_4 = \varepsilon^j d \quad \in k(d, \varepsilon)$$

De ces deux appartenances, on déduit $h_1 \in k(d, \varepsilon)$. De même $h_4 \in k(d, \varepsilon)$ et par symétrie h_2 et h_3 appartiennent à $k(d, \varepsilon)$. Ainsi les x_i appartiennent aussi à $k(d, \varepsilon)$ puisqu'ils sont combinaisons linéaires (à coefficients dans $k(\varepsilon)$) des h_i. Or $k(d, \varepsilon)$ est de dimension 1, 2, 4 ou 8 sur k et $k(x_i)$ est de dimension 5 puisque f est irréductible : tout ceci aboutit à une contradiction car 5 ne divise ni 1, ni 2, ni 4, ni 8 !

Ainsi $h_1^5 \neq h_4^5$ ou $h_2^5 \neq h_3^5$: quitte à changer d en $-d$, on peut supposer $h_1^5 \neq h_4^5$.

> Remarque. Ces diverses obstructions au calcul des h_i sont dues à la méthode choisie. Rien ne prouve qu'il s'agisse d'obstructions intrinsèques qu'on rencontrera avec n'importe quelle méthode.

Résumé

Soit k un corps de caractéristique distincte de 2 et 5. On considère un polynôme $f = T^5 + pT + q$ irréductible séparable sur k avec $pq \neq 0$ (on suppose que f est de cette forme assez simple pour écrire des formules explicites). L'équation $f = 0$ est résoluble par radicaux si et seulement si la résolvante

$$\begin{aligned} g = &\quad (T^3 - 5pT^2 + 15p^2T + 5p^3)^2 - (3125q^4 + 256p^5)T \\ = &\quad (T - p)^4(T^2 - 6pT + 25p^2) - 5^5q^4T \end{aligned}$$

admet une racine dans k. Si c'est effectivement le cas, notons b une racine de g. On calcule

$$d = \sqrt{5b} \qquad h_1 = \sqrt[5]{\frac{1}{2}\left(u + vd + \sqrt{(u + vd)^2 - 4d^5}\right)} \qquad h_4 = d/h_1$$

où u et v ont des valeurs exprimées ci-dessus, page 88. On impose $h_1^5 - h_4^5 \neq 0$ quitte à échanger d en $-d$. Puis h_2 et h_3 sont obtenus grâce à :

$$\begin{pmatrix} h_2 \\ h_3 \end{pmatrix} = \frac{1}{h_1^5 - h_4^5} \begin{pmatrix} h_1^2 & -h_4^3 \\ -h_4^2 & h_1^3 \end{pmatrix} \begin{pmatrix} u' \\ v'd \end{pmatrix}$$

où les quantités u' et v' sont explicitées ci-dessus. Enfin les racines de f se calculent par

$$x_{i+1} = (\varepsilon^i h_1 + \varepsilon^{2i} h_2 + \varepsilon^{3i} h_3 + \varepsilon^{4i} h_4)/5 \qquad i \in \{0, 1, 2, 3, 4\}, \qquad \varepsilon = \sqrt[5]{1} \text{ primitive}$$

Exemple

Considérons le polynôme $T^5 - 5T + 12$. Peut-on calculer ses racines par radicaux sur $\mathbb{Q}$, et si oui, quelles sont-elles ?

Le calcul montre que la résolvante "de Cayley" g possède une (unique) racine dans $\mathbb{Q}$ qui est $b = 25$: nous pouvons donc résoudre l'équation $T^5-5T+12 = 0$ avec des radicaux sur $\mathbb{Q}$. Nous obtenons alors les valeurs suivantes :

$$d = 5\sqrt{5} \qquad u = -6250 \qquad v = -500 \qquad u' = 500 + 250\sqrt{5} \qquad v' = 10$$

Comme $\sqrt{5} \notin \mathbb{Q}$, le groupe de Galois de $T^5 - 5T + 12$ ne peut pas être contenu dans le groupe diédral D_5. Nous avons donc

$$\mathrm{Gal}_{\mathbb{Q}}\ \big(T^5 - 5T + 12\big) \simeq \mathrm{AGL}_1(\mathbb{F}_5) \simeq F_{20}$$

Enfin

$$h_1 = \sqrt[5]{-3125 - 1250\sqrt{5} + 375\sqrt{5}\sqrt{11\sqrt{5}+25},} \qquad h_4 = 5\sqrt{5}/h_1$$

$$h_2 = \frac{(2\sqrt{5}+5)h_1^2 - h_4^3}{15\sqrt{11\sqrt{5}+25}}, \qquad h_3 = -\frac{(2\sqrt{5}+5)h_4^2 - h_1^3}{15\sqrt{11\sqrt{5}+25}}$$

Les racines de $T^5-5T+12$ sont données par $(\varepsilon^k h_1+\varepsilon^{2k}h_2+\varepsilon^{3k}h_3+\varepsilon^{4k}h_4)/5$ où $\varepsilon = e^{2i\pi/5}$ et $k \in \{0,1,2,3,4\}$.

III.4.e Paramétrisation des polynômes $T^5 + pT + q$ irréductibles résolubles

On peut noter que mettre le polynôme g sous la forme

$$g = (T-p)^4(T^2 - 6pT + 25p^2) - 5^5q^4T$$

permet de paramétrer l'ensemble des polynômes (irréductibles) $f = T^5 + pT + q$ où p et q sont non nuls, dont le groupe de Galois est inclus dans F_{20} (voir [2] page 32, [57], ou [65] pages 675-676). En effet, la condition $\mathrm{Gal}_k(f) \subset F_{20}$ est équivalente à l'existence d'une racine b de g dans le corps de base (en caractéristique distincte de 2 et 5). De plus, $pq \neq 0$ implique $b \notin \{0, p\}$.

Si nous posons $\quad c = \xi\dfrac{3b-25p}{4b}, \quad e = \xi\dfrac{5q}{2(p-b)}, \quad \xi = \pm 1 \quad$ alors

$$p = \frac{5e^4(3-4\xi c)}{c^2+1} \qquad \text{et} \qquad q = -\frac{4e^5(11\xi+2c)}{c^2+1}$$

La constante $c^2 + 1$ n'est pas nulle car nous sommes en caractéristique autre que 5 : en effet, la condition $c^2+1 = 0$ impose à b d'être racine de $h = (3T-25p)^2+(4T)^2$. Or b est également racine de g, donc le résultant de h et g est nul. Mais $\mathrm{res}(g,h) = 5^{24}p^2q^8 \neq 0$!

Réciproquement, si $\xi = \pm 1$ et c et e sont choisis de façon quelconque avec $c^2 + 1 \neq 0$, alors la résolvante g calculée à partir du polynôme

$$f = T^5 + \frac{5e^4(3 - 4\xi c)}{c^2 + 1}\, T - \frac{4e^5(11\xi + 2c)}{c^2 + 1}$$

admet une racine qui est $\qquad b = \dfrac{125e^4}{c^2 + 1}$.

Ainsi, il est clair que l'on peut exprimer rationnellement le couple (c, e) en fonction du triplet (p, q, b), et surtout réciproquement (p, q, b) en fonction de (c, e).

En particulier, si p et q sont deux indéterminées sur le corps k, alors il est évident que $T^5 + pT + q$ est irréductible sur $k(p, q)$ et $pq \neq 0$. Les éléments p, q et b s'expriment donc rationnellement en fonction de $c, e \in k(p, q, b)$. L'extension $k(p, q, b)$ (algébrique sur $k(p, q)$) est par conséquent une extension pure de k puisqu'elle est égale à $k(c, e)$. Les indéterminées c et e (sur k) sont donc algébriquement indépendantes.

Remarque due à J.-M. Arnaudiès. La surface définie par le polynôme

$$(T - U)^4(T^2 - 6UT + 25U^2) - 5^5V^4T \in k[T, U, V]$$

(où k est le corps de base) est rationnelle sur k. On le voit en posant $V = \lambda(T - U)$, ce qui ramène à $(T^2 - 6UT + 25U^2) - 5^5\lambda T$, et ce dernier polynôme est de degré 2 en (T, U) et admet un point k-rationnel (l'origine), ce qui permet d'achever la rationalisation en posant par exemple $U = \rho T$ (ceci donne $(1 - 6\rho + 25\rho^2)T - 5^5\lambda^4$). L'explication de l'existence de cette paramétrisation des polynômes $T^5 + pT + q$ irréductibles résolubles est là.

III.5 Séparabilité de la résolvante de Cayley

Considérons un polynôme unitaire irréductible de degré 5 et cherchons à savoir si celui-ci est résoluble par radicaux, c'est-à-dire si son groupe de Galois est résoluble ou non, ou encore si celui-ci est inclus dans le sous-groupe métacyclique F_{20} de $\mathcal{S}_5$. Réécrivons le théorème II.6.2 de la page 64 dans le cas particulier où nous nous trouvons :

Propriété III.5.1 *Soit K un corps, $f \in K[T]$ un polynôme unitaire de degré 5 séparable et $g \in K[X]$ une résolvante liée au sous-groupe $F_{20} \subset \mathcal{S}_5$. On suppose que g est séparable. Alors le groupe de Galois de f sur K est inclus dans le sous-groupe métacyclique F_{20} si et seulement si g admet au moins une racine dans K.*

La résolvante de Cayley (de degré 6) est liée au groupe métacyclique de $\mathcal{S}_5$. Ce qui la particularise, c'est le théorème suivant :

Théorème III.5.1 (voir [4]) *Avec les mêmes notations, si* $\mathrm{carac}(K) = 0$ *et f est irréductible alors la résolvante de Cayley g est séparable.*

Ainsi, il est facile de savoir (en caractéristique 0 tout au moins) si l'on peut calculer par radicaux les racines d'un polynôme irréductible de degré 5 :

Corollaire III.5.1 *Avec les mêmes hypothèses (*$\mathrm{carac}(K) = 0$*, f est unitaire irréductible de degré 5), l'équation $f = 0$ est résoluble par radicaux si et seulement si la résolvante de Cayley admet au moins une racine dans K.*

Dans cette section, je propose de caractériser tous les polynômes f pour lesquels la résolvante de Cayley est séparable, avec un minimum d'hypothèses sur la caractéristique de K... Les polynômes ne sont pas tous "bons" : en effet, en caractéristique 0, si f est un polynôme séparable de la forme $T^5 + pT + q$, alors la résolvante de Cayley g est séparable si et seulement si $q \neq 0$. On peut le voir simplement en calculant et factorisant les discriminants de g et de f : $\mathrm{dis}(g) = 2^{60}5^{30}q^{12}\,\mathrm{dis}(f)^3$.

Il faut donc bien avoir en tête que la simple séparabilité de f ne suffit pas, et qu'il faut trouver une autre hypothèse pour obtenir le résultat désiré. Bien entendu, il faudra aussi retrouver le théorème III.5.1 comme cas particulier.

La démonstration qui suit et celle que l'on peut voir dans [4] sont très différentes : celle que nous présentons ici est plus élémentaire et mais aussi plus calculatoire...

Avant de se lancer dans le degré 5, certifions le résultat suivant.

Lemme III.5.1 *Soit K' un corps, $h = T^4 + aT^3 + bT^2 + cT + d \in K'[T]$ dont les racines dans une extension sont y_1, y_2, y_3, y_4. Soit k la résolvante associée à y_1y_2, i.e. le polynôme (de degré 6) dont les racines sont les double-produits des y_i :*

$$K'[T] \ni k = \prod_{\tau \in (\mathcal{S}_4/\mathcal{S}_2\times\mathcal{S}_2)_g} \big(T - y_{\tau(1)}y_{\tau(2)}\big) = \prod_{i<j} \big(T - y_iy_j\big)$$

Alors $\mathrm{dis}(k) = \mathrm{dis}(h)^2d^6(da^2 - c^2)^2$*, si bien que k est séparable si et seulement si h l'est, $d \neq 0$ et $da^2 \neq c^2$.*

Revenons maintenant au degré 5. Considérons les polynômes

$$D = X_1X_2 + X_2X_3 + X_3X_4 + X_4X_5 + X_5X_1 \qquad C = (D - (2,3,5,4).D)^2$$

Le polynôme C est appelé le résolvant de Cayley : son stabilisateur sous l'action de $\mathcal{S}_5$ est le groupe métacyclique F_{20} (le stabilisateur du polynôme D est le groupe diédral D_5). On définit la résolvante de Cayley générique par

$$G = \prod_{\tau \in (S_5/F_{20})_g} \big(T - \tau.C\big) \qquad \in \mathbb{Z}[\sigma_1, \ldots, \sigma_5, T]$$

où σ_i est le polynôme symétrique élémentaire homogène de degré i en $X_1, \ldots, X_5$. En fait G est le polynôme minimal de C sur $\mathbb{Z}[\sigma_1, \ldots, \sigma_5]$ (anneau intégralement clos).

Remarquer que $D + (2,3,5,4).D = \sigma_2$.

Soit K un corps et $f \in K[T]$ un polynôme unitaire de degré 5 dont les racines dans un sur-corps sont x_1, x_2, x_3, x_4, x_5. On note g la spécialisation de G en les racines de f :

$$g = \prod_{\tau \in (S_5/F_{20})_g} \big(T - (\tau.C)(x_1, \ldots, x_5)\big)$$

Le polynôme g est la résolvante de Cayley associée à f.

Théorème III.5.2 *Soit le polynôme* $f(T) = T^5 + aT^4 + bT^3 + cT^2 + dT + e \in K[T]$. *On pose* $P_d = f'$, $P_c = 10T^3 + 6aT^2 + 3bT + c$ *(*$= f''/2$ *si cela a un sens) et* $P_a = 5T + a$ *(*$= f^{(4)}/4!$ *si cela a un sens). La résolvante de Cayley* g *est séparable si et seulement si on a simultanément*

$$\mathrm{carac}(K) \neq 2, \qquad f \text{ est séparable}, \qquad \mathrm{res}(f, P_d P_a^2 - P_c^2) \neq 0$$

Démonstration Pour commencer, si $\mathrm{carac}(K) = 2$ alors $g = (T - \sigma_2(x_1, \ldots, x_5)^2)^6$: le polynôme g est alors loin d'être séparable. De même, si f n'est pas séparable alors g ne peut pas l'être...

Plaçons-nous maintenant en caractéristique différente de 2. Pour alléger les notations, posons $x = (x_1, \ldots, x_5)$. Montrons la contraposée du résultat : si g n'est pas séparable alors deux racines de G deviennent égales après l'évaluation. Par suite

$$(\tau.C)(x) = (\tau'.C)(x)$$

où $\tau \neq \tau' \in (\mathcal{S}_5/F_{20})_g$. Quitte à changer l'ordre des x_i, on peut admettre que $\tau' = \mathrm{Id}$, c'est-à-dire

$$C(x) = (\tau.C)(x)$$

où τ appartient au système de représentants de $(\mathcal{S}_5/F_{20})_g \setminus \{\overline{\mathrm{Id}}\}$ que l'on choisit arbitrairement : $\{(2,3),(2,4),(3,4),(3,5),(4,5)\}$. Posons $\mu = (2,3,5,4) \in F_{20}$.

Nous savons que $C(x) = (D(x) - (\mu.D)(x))^2$, et de même

$$(\tau.C)(x) = ((\tau.D)(x) - (\tau.\mu.D)(x))^2$$

L'égalité $C(x) = (\tau.C)(x)$ nous donne la suivante :

$$D(x) - (\mu.D)(x) = \pm(\tau.D)(x) \mp (\tau.\mu.D)(x)$$

De plus, il est facile de voir que $D + \mu.D = \sigma_2 = \tau.D + \tau.\mu.D$, ce qui donne la relation supplémentaire

$$D(x) + (\mu.D)(x) = (\tau.D)(x) + (\tau.\mu.D)(x)$$

Ainsi, en sommant ces deux égalités (caractéristique différente de 2), deux cas peuvent se présenter :

$$(1) \quad D(x) = (\tau.D)(x) \qquad \text{ou} \qquad D(x) = (\tau.\mu.D)(x) \quad (2)$$

où τ appartient à $\{(2,3),(2,4),(3,4),(3,5),(4,5)\}$ (rappel : $\mu = (2,3,5,4)$).

Le premier cas (1), $D(x) = (\tau.D)(x)$, implique que f n'est pas séparable : par exemple, si $\tau = (2,3)$ alors

$$x_1x_2 + \cancel{x_2x_3} + x_3x_4 + \cancel{x_4x_5} + \cancel{x_5x_1} = x_1x_3 + \cancel{x_3x_2} + x_2x_4 + \cancel{x_4x_5} + \cancel{x_5x_1}$$

ce qui donne après simplification et factorisation $(x_1 - x_4)(x_2 - x_3) = 0$: f n'est pas séparable.

Des calculs identiques pour les autres valeurs possibles de τ amènent au même type d'égalité...

Le second cas (2), $D(x) = (\tau.\mu.D)(x)$, est un peu plus compliqué. Pour rendre plus concrets les calculs, posons $\tau = (2,3)$ et écrivons la relation $D(x) = (\tau.\mu.D)(x)$: on a $\tau.\mu = (3,5,4)$ et

$$\cancel{x_1x_2} + x_2x_3 + \cancel{x_3x_4} + x_4x_5 + x_5x_1 = \cancel{x_1x_2} + x_2x_5 + x_5x_3 + \cancel{x_3x_4} + x_4x_1$$

Cette dernière égalité est équivalente à $(x_1 - x_5)(x_4 - x_5) = (x_2 - x_5)(x_3 - x_5)$ (merci à Noël Fraisseix pour cette factorisation.). Si l'on fait les calculs pour les autres valeurs possibles de τ, là encore, on obtient le même type d'égalité.

C'est maintenant que le lemme III.5.1 va nous servir : soit x une racine de f telle que $(x_i - x)(x_j - x) = (x_m - x)(x_n - x)$ (dans l'exemple ci-dessus, il s'agit de x_5). Notons K' l'extension de K engendrée par x, et posons $h(T) = T^{-1}f(T + x)$: un simple calcul nous donne, avec les notations du théorème III.5.2,

$$h = T^4 + P_a(x)T^3 + (10x^2 + 4ax + b)T^2 + P_c(x)T + P_d(x)$$

Les racines de h dans K' sont $y_i = x_i - x$, $y_j = x_j - x$, etc. On peut alors utiliser judicieusement le lemme puisque nous avons la relation $y_iy_j = y_my_n$: (la résolvante k, notation du lemme, n'est pas séparable) : $\mathrm{dis}(k) = 0$. Ainsi nous avons $\mathrm{dis}(h) = 0$, ou $P_d(x) = 0$, ou encore $P_d(x)P_a(x)^2 - P_c(x)^2 = 0$.

On rappelle que x est une racine de f. Comme $h(T).T = f(T+x)$, il est clair que $\mathrm{dis}(h)$ divise $\mathrm{dis}(f)$ (dans K'). Ainsi, nous obtenons finalement

$$\mathrm{dis}(f) = 0 \quad \text{ou} \quad \mathrm{res}(f, P_d) = 0 \quad \text{ou} \quad \mathrm{res}(f, P_dP_a^2 - P_c^2) = 0$$

Pour démontrer la réciproque du résultat, i.e. $\mathrm{res}(f, P_dP_a^2 - P_c^2) = 0$ implique g non séparable, il suffit de choisir une numérotation adéquate des x_i pour avoir par exemple $(x_1 - x_5)(x_4 - x_5) = (x_2 - x_5)(x_3 - x_5)$, ce qui implique la non séparabilité de g. □

Prenons l'exemple d'un polynôme séparable f s'écrivant $T^5 + pT + q$: la résolvante de Cayley qui lui est associée est séparable si et seulement si $q \neq 0$ en caractéristique distincte de 5 (on peut le voir simplement en calculant et factorisant les discriminants de f et de la résolvante de Cayley). On retrouve ce résultat avec le théorème III.5.2 car $P_a = 5T$, $P_c = 10T^3$, $P_d = 5T^4 + p$ et $P_dP_a^2 - P_c^2 = 25T(f - q)$: $\mathrm{res}(f, 25T(f - q)) = 0$ si et seulement si $f(0) = 0$ ou $q = 0$ (ce qui revient au même).

On peut aussi obtenir le théorème III.5.1 comme corollaire du théorème III.5.2 :

Corollaire III.5.2 *Soit K un corps de caractéristique distincte de 2 et 5, f un polynôme irréductible séparable unitaire de degré 5 de $K[T]$, alors la résolvante de Cayley qui lui est associée est séparable.*

Démonstration Posons $f = T^5 + aT^4 + bT^3 + cT^2 + dT + e$. En premier lieu, on peut supposer que a est nul : en effet les conditions du théorème III.5.2 sont invariantes par les translations du genre $T \mapsto T + a/5$.

Maintenant, $\mathrm{res}(f, P_dP_a^2 - P_c^2) = \mathrm{res}(f, R)$ où R est le reste de la division unitaire euclidienne de $P_dP_a^2 - P_c^2$ par f.

$$R = -10bT^4 + 5cT^3 - 9b^2T^2 - (25e + 6bc)T - c^2$$

Or $\mathrm{res}(f, R) = 0$ est équivalent à $R = 0$ car f est irréductible de degré 5. Mais pour avoir $R = 0$, il faut avoir obligatoirement $b = c = e = 0$. Sous ces conditions, $f = T^5 + dT$ ce qui contredit le fait que f est irréductible.

Ainsi $\mathrm{res}(f, R) = \mathrm{res}(f, P_d P_a^2 - P_c^2)$ ne peut pas être nul : la résolvante de Cayley liée à f est donc séparable dans tous les cas. □

Remarque. En caractéristique 5, la résolvante de Cayley liée à un polynôme f unitaire séparable irréductible est toujours séparable sauf dans le cas où

$$f = T^5 + pT + q$$

(un polynôme que l'on a déjà vu quelque part !).

Chapitre IV

Réalisation régulière explicite de groupes élémentaires

Notre but, dans ce chapitre, est de construire des polynômes de degré n à coefficients dans $k[t]$ (k est un corps) réalisant régulièrement sur k certains groupes : par exemple les groupes cycliques, diédraux, abéliens finis, ou encore les sous-groupes $\mathbb{Z}/n\mathbb{Z} \rtimes \Gamma$ des groupes affines linéaires $\mathrm{AGL}_1(\mathbb{Z}/n\mathbb{Z}) = \mathbb{Z}/n\mathbb{Z} \rtimes \mathrm{U}(\mathbb{Z}/n\mathbb{Z})$... Par "réaliser régulièrement sur k", nous entendons que les corps de décomposition des polynômes sur $k(t)$ sont des extensions régulières sur k.

Pour cela, après de brefs rappels sur les extensions régulières et la théorie de Kummer, nous avons choisi de traiter en premier lieu la réalisation régulière des extensions cycliques et abéliennes. Le fait que tout groupe abélien soit groupe de Galois d'une extension régulière de $\mathbb{Q}(t)$ n'est bien sûr pas nouveau : J.P. Serre, dans [53] (pages 689-03), fait référence à D.J. Saltman [50]. Il en donne plus tard une autre démonstration dans [54], pages 36-37. Dans [55], G.W. Smith explicite la construction de polynômes réguliers (à plusieurs paramètres) de groupe de Galois $\mathbb{Z}/n\mathbb{Z}$ avec n impair ; la construction de G.W. Smith est basée sur la cyclicité du groupe $\mathrm{U}(\mathbb{Z}/p^\alpha\mathbb{Z})$ pour $p \neq 2$. Elle est reprise et généralisée par R. Dentzer dans [24] pour un groupe cyclique quelconque avec des polynômes à 1 paramètre. Cette amélioration, de nature plutôt calculatoire, est également mentionnée dans [43], addendum du chapitre III. Enfin, H. Volklein, à la suite des travaux de M. Fried, D. Harbater, Q. Liu et B.H. Matzat, explicite (dans [64] page 236) une construction particulièrement simple d'une extension cyclique de $\mathbb{Q}(t)$ contenue dans le corps des séries formelles $\mathbb{Q}((t))$ (donc régulière sur $\mathbb{Q}$).

On généralise ici la construction fournie dans [64] en lui assurant un fondement à l'aide de la théorie de Kummer. Cette méthode a plusieurs avantages : tout d'abord la simplicité, l'efficacité en machine, et enfin le contrôle des extensions construites : par exemple, pour un n fixé, chaque extension E est réalisée par le simple choix du polynôme minimal μ d'un générateur de $k(\mathbb{U}_n)/k$ ($\mathbb{U}_n$ désigne l'ensemble des racines n-ièmes de l'unité). Si $k = \mathbb{Q}$ et $n > 2$ alors la seule valuation de $\mathbb{Q}(t)$ (triviale sur $\mathbb{Q}$) ramifiée dans E est celle correspondant au polynôme réciproque de $\mu(-t)$. Cette valuation est d'ailleurs totalement ramifiée dans E. De plus, E est construite dans $\mathbb{Q}((t))$, si bien que

le premier t y est totalement décomposé (existence d'un point rationnel non ramifié). D'une part ce contrôle permet la réutilisation de ces extensions, et d'autre part il est indispensable pour la réalisation régulière de tout groupe fini sur $\mathbb{Q}_p(t)$ (voir [25] et [41]).

Ensuite, nous nous intéressons aux extensions diédrales, puis finalement et de manière plus générale à tout produit semi-direct $A \rtimes \Gamma_0$ à noyau A abélien. Dans [60], J.G. Thomson a montré que, si Γ_0 est réalisé régulièrement sur $\mathbb{Q}(t)$, il en est de même de $A \rtimes \Gamma_0$ (voir également [54] page 37, ou [64] page 140). On rend explicite une telle réalisation ; à noter qu'ici, contrairement aux méthodes de [31], (section 3.4 Produits semi-directs), nous sommes assurés à l'avance, par des moyens théoriques, de la régularité des extensions.

Notre but étant de réaliser certains groupes élémentaires en calculant des polynômes à coefficients dans $k(t)$ (plus précisément dans $k[t]$), nous ferons en sorte que les degrés de ces polynômes soient les plus petits possible : en effet, il y est clair que l'on peut réaliser le groupe symétrique $\mathcal{S}_n$ avec un polynôme de degré $n!$... Il est quand même plus intéressant de trouver un polynôme de degré n.

Cette contrainte supplémentaire portant sur les degrés complique encore notre tâche. Par exemple, pour réaliser un produit semi-direct $\mathbb{Z}/n\mathbb{Z} \rtimes \Gamma$ où Γ opère fidèlement sur $\mathbb{Z}/n\mathbb{Z}$, nous calculerons un polynôme de degré n. En revanche, pour les groupes abéliens, les polynômes que nous coucherons sur le papier aurons des degrés égaux aux cardinaux des groupes abéliens : les polynômes abéliens sont nécessairement galoisiens.

IV.1 Extensions régulières, polynômes réguliers

IV.1.a Définitions et exemples

La notion d'extension régulière est liée aux notions suivantes : extensions linéairement (ou algébriquement) disjointes, extension (de type fini) séparable, sous-corps algébriquement fermé (voir [38], pages 360-368). Rappelons brièvement la définition (une définition possible...) d'une extension régulière.

Définition IV.1.1

- *Une extension K/k de type fini admet une* ***base de transcendance $\mathcal{B}$ séparante*** *s'il existe un ensemble $\mathcal{B} \subset K$ d'éléments algébriquement indépendants sur k tel que $K/k(\mathcal{B})$ soit une extension de dimension finie (algébrique) séparable.*
- *Une extension E/k est dite* ***séparable*** *si, pour toute sous-extension $K \subset E$ de type fini sur k, il existe une base de transcendance $\mathcal{B}$ séparante de K/k. Si E/k est de type fini, alors il faut et il suffit qu'il existe une base de transcendance séparante de E/k.*

Exemple classique : *si t est une indéterminée sur un corps k de caractéristique $p > 0$, alors considérons la k-extension $E = \bigcup_{n\in\mathbb{N}} k\big(t^{\frac{1}{p^n}}\big)$. Cette extension est de degré de transcendance 1 car elle est algébrique sur $k(t)$. Elle ne possède pas de base de transcendance séparante sur k. Malgré cela, elle est séparable car toute k-extension intermédiaire de type fini sur k est contenue dans $k(t^{\frac{1}{p^n}})$ (pure sur k) pour un certain $n \in \mathbb{N}$. En utilisant le théorème de Lurôth, on prouve que cette k-extension intermédiaire s'écrit $k(f)$ (pure sur k) où f est une fraction rationnelle en $t^{\frac{1}{p^n}}$.*

• *Une extension K/k est dite* ***régulière*** *si elle satisfait l'une des deux assertions équivalentes suivantes (voir [38], page 367) :*

REG 1 *k est algébriquement fermé dans K, et K est séparable sur k ;*

REG 2 *K est linéairement disjoint de Ω (une clôture algébrique de k) sur k.*

Exemple : l'extension engendrée par une racine d'un polynôme d'Eisenstein

Soit t une indéterminée sur k, et f_t un polynôme à coefficients dans $k[t]$ d'Eisenstein pour un premier $\pi \in k[t]$ séparable. Si x est une racine de f_t dans une extension de $k(t)$, alors $k(t,x)$ est régulière sur k. En effet, soit Ω une clôture algébrique de k. Dans $\Omega[t]$, π se factorise en produit de polynômes irréductibles distincts de degré 1, $\pi_1 \cdots \pi_m \in \Omega[t]$. Comme f_t est d'Eisenstein pour π, il l'est aussi pour chaque π_i si l'on considère f_t comme un polynôme à coefficients dans $\Omega[t]$. Donc le polynôme f_t reste irréductible sur $\Omega(t)$, autrement dit $[\Omega(t,x) \ : \ \Omega(t)] = [k(t,x) \ : \ k(t)]$, ou encore $\Omega(t)$ et $k(t,x)$ sont linéairement disjointes sur $k(t)$. Enfin Ω et $k(t,x)$ sont linéairement disjointes sur k, ce qui prouve que $k(t,x)$ est régulière sur k.

Contre-exemple : importance de la séparabilité de π dans l'exemple ci-dessus

Si la caractéristique de k est $p > 0$, $a \in k \setminus k^p$ et x une racine de $f_t = X^p - (t^p - a)$, polynôme d'Eisenstein pour $t^p - a$ irréductible (non séparable) de $k[t]$, alors $k(t,x)$ n'est pas régulière sur k. En effet, cette extension contient l'élément $t - x$, n'appartenant pas à k, mais algébrique sur k car $(t-x)^p = t^p - x^p = a$. On pourrait ajouter que le polynôme f_t ne reste pas irréductible sur $\Omega(t)$ car $f_t = (X-x)^p$.

Merci à Pierre Dèbes pour avoir donné ces exemple et contre-exemple.

Autre exemple : le corps des séries formelles

Si k est un corps alors le corps des séries formelles $k((t))$ est régulier sur k. En effet, soit $\mathfrak{b} = \{b_i \mid i = 1, \ldots, n\}$ une famille d'éléments algébriques sur k (disons $b_i \in \Omega$ où Ω une clôture algébrique de k). Nous allons raisonner dans $\Omega((t))$. Une relation de dépendance linéaire non triviale de la famille $\mathfrak{b}$ à coefficients dans le corps $k((t)) \subset \Omega((t))$ s'écrit

$$0 = \sum_{i=1}^{n} \frac{f_i}{g_i} b_i \qquad \text{avec} \qquad f_i, g_i \in k[[t]]$$

En multipliant par $\prod_i g_i$, nous obtenons une relation de dépendance linéaire non triviale à coefficients dans $k[[t]]$:

$$0 = \sum_{i=1}^{n} p_i b_i \qquad \text{avec} \qquad p_i \in k[[t]]$$

Par hypothèse, il existe au moins un p_i non nul. Quitte à diviser par une puissance convenable de l'indéterminée t, on peut supposer qu'il existe au moins un p_i dont le terme constant est non nul. Finalement, en évaluant cette relation en $t \mapsto 0$, on obtient une relation de dépendance linéaire non triviale de la famille $\mathfrak{b}$. Par contraposée, une famille libre d'éléments algébriques sur k reste libre sur $k((t))$.

Nous venons de montrer REG 2 rapidement. L'intérêt de cet exemple est de prouver qu'il est parfois plus facile de prouver une linéaire disjonction (résultat "fort") que de démontrer qu'il n'y a pas d'éléments algébriques non triviaux (résultat "faible", première partie de REG 1). Les deux critères REG 1 et REG 2 offrent des visions totalement différentes des extensions régulières. Aucune d'entre elles ne peut être négligée.

Définition IV.1.2 *Soit k un corps et t une indéterminée sur k. On dira qu'un élément $f \in k(t)[X]$ est* ***polynôme régulier*** *sur un corps k et de groupe de Galois G si f est séparable et son corps de décomposition (qui est une extension galoisienne sur $k(t)$) est une extension régulière sur k de groupe de Galois G sur $k(t)$.*

La définition d'un polynôme régulier est cohérente avec celle d'une extension régulière : la base $\mathcal{B}$ est dans ce cas particulier réduite au singleton formé par l'indéterminée t. Avant d'entrer dans le vif du sujet, voici quelques exemples classiques de polynômes réguliers pour les groupes cycliques.

• Le polynôme $X^n - t$ est régulier sur $k = \mathbb{Q}(\mathbb{U}_n)$ de groupe $\mathbb{Z}/n\mathbb{Z}$ ($\mathbb{U}_n$ est l'ensemble des racines n-ièmes de l'unité). En effet, celui-ci est irréductible car de degré 1 et primitif en tant que polynôme en t à coefficients dans $\mathbb{Q}[\mathbb{U}_n, X]$. Dans une clôture algébrique de $\mathbb{Q}(\mathbb{U}_n, t)$, ses racines x_i sont liées par les relations $x_i = x_0\epsilon^i$ où ϵ est une racine primitive n-ième de 1. De plus, son corps de décomposition sur $k(t)$ est $k(\sqrt[n]{t})$, extension évidemment régulière (pure) sur k.

Ces polynômes relativement simples jouent un rôle fondamental dans la théorie de Kummer comme nous le verrons dans la section IV.2.

• Le polynôme $X^p - X - t$ est régulier sur $\mathbb{F}_p$ (corps fini d'ordre p) et son groupe de Galois sur $\mathbb{F}_p(t)$ est isomorphe au groupe $\mathbb{Z}/p\mathbb{Z}$. En effet, si x_0 est une racine de ce polynôme, alors pour tout $i \in \mathbb{F}_p$, $x_i = x_0 + i$ en est également une racine.

$$x_i^p - x_i - t = x_0^p + i^p - x_0 - i - t = 0$$

Il est clair que $f = X^p - X - t \in \mathbb{F}_p[t, X]$ est irréductible car $-f$ est un polynôme en t unitaire et de degré 1. Vu la relation de dépendance $x_1 = x_0 + 1$, son groupe de Galois ne peut être que cyclique : il existe $\sigma \in \mathrm{Gal}_{\mathbb{F}_p(t)} f$ tel que $\sigma(x_0) = x_1 = x_0 + 1 \neq x_0$. Alors $\sigma^k(x_0) = x_0 + k = x_k$ pour k parcourant $\{0, \ldots, p-1\}$, si bien que tous les x_i sont σ-conjugués.

Enfin, le corps de décomposition de f sur $\mathbb{F}_p(t)$ est particulièrement régulier sur $\mathbb{F}_p$ (pur en fait) car il est égal à $\mathbb{F}_p(x_0, t) = \mathbb{F}_p(x_0)$ (rappel : $t = x_0^p - x_0$).

Ces polynômes particuliers interviennent dans la théorie d'Artin-Schreier. Ce sont en fait des polynômes **génériques** (voir [55]) en caractéristique p pour le groupe cyclique $\mathbb{Z}/p\mathbb{Z}$. Ils ont par exemple la propriété suivante : pour toute extension cyclique K/k en caractéristique $p \neq 0$ de groupe $\mathbb{Z}/p\mathbb{Z}$, il existe un élément x_0 de K dont le polynôme minimal sur k est $X^p - X - t_0$. En effet, soit σ un générateur de $\mathrm{Gal}_k K$. Il est clair que $k = \ker(\sigma - \mathrm{Id}_K)$ et que $\sigma - \mathrm{Id}_K$ est un endomorphisme de k-espace vectoriel nilpotent d'indice p. Or $p = \dim_k K > 1$, donc le noyau de $\sigma - \mathrm{Id}_K$ est inclus dans l'image de

$\sigma - \mathrm{Id}_K$. Ainsi $k \subset \mathrm{im}(\sigma - \mathrm{Id}_K)$, et pour tout $t \in k$ il existe $x \in K$ tel que $\sigma(x) - x = t$. En particulier il existe $x_0 \in K$ tel que $\sigma(x_0) = x_0 + 1$. Alors le polynôme minimal de x_0 sur k est $X^p - X - t_0$ car $x_0 \notin k$ (donc x_0 est degré p) et

$$\sigma(x_0^p - x_0) = \sigma(x_0)^p - \sigma(x_0) = (x_0^p + 1) - (x_0 + 1) = x_0^p - x_0$$

donc $x_0^p - x_0$ appartient à k.

• Le polynôme $f = X^3 - tX^2 - (3+t)X - 1$ est régulier sur $\mathbb{Q}$ de groupe $\mathcal{A}_3$ (le groupe alterné). En effet, f est irréductible sur $\mathbb{Z}[t]$ (donc sur $\mathbb{Q}(t)$) et son discriminant est $(t^2 + 3t + 9)^2$.

En réalité, ce polynôme est générique (en particulier régulier) car pour toute extension K/k de caractéristique distincte de 2, cyclique de degré 3, il existe un élément primitif de K/k dont le polynôme minimal est un spécialisé de f en un certain $t_0 \in k$. Essayons d'expliciter un élément primitif y et la valeur t_0 qui correspond à son polynôme minimal. En tout premier lieu, si l'on veut trouver un élément y racine d'un spécialisé de f, il est obligatoire que cet y soit de norme égale à $(-1)^3 f(0) = 1$. Grâce au théorème 90 de Hilbert, cet élément est de la forme $\frac{z}{\sigma(z)}$ où σ est un générateur de $\mathrm{Gal}_k K$.

Soit x_1 un élément primitif de K/k. Ses conjugués sont notés x_2, x_3 et son polynôme minimal

$$X^3 - a_1 X^2 + a_2 X - a_3$$

Soit $d = (x_1 - x_2)(x_2 - x_3)(x_3 - x_1)$. Cette quantité d appartient à k car le groupe de groupe de Galois est $\mathcal{A}_3$ ($d^2 = \mathrm{dis}(f)$).

En supposant que $y = \frac{x_1}{x_2}$ soit un élément primitif de K/k, le polynôme minimal de y s'écrit

$$X^3 - \left(\frac{a_1 a_2 + d}{2a_3} - \frac{3}{2}\right) X^2 - \left(\frac{-a_1 a_2 + d}{2a_3} + \frac{3}{2}\right) X - 1$$

(Ces calculs sont réalisés avec l'algèbre de décomposition universelle.) Nous constatons que si le produit $a_1 a_2$ est nul, alors en posant

$$t_0 = \frac{d}{2a_3} - \frac{3}{2} \quad \in k$$

le polynôme minimal de y est bien le spécialisé de f en t_0.

Il reste à montrer maintenant que toutes les hypothèses faites ci-dessus sont réalisables. Il est légitime de supposer que x_1 est de trace nulle car on peut toujours s'y ramener en considérant $x_1 - x_2$ ou $x_1^2 - x_2^2$. Comme $[K : k] = 3$, il suffit de ne pas appartenir à k pour être un élément primitif de K/k. Or les deux éléments $x_1 - x_2$ et $x_1^2 - x_2^2 = (x_1 - x_2)(x_1 + x_2)$ de K ne peuvent appartenir simultanément à k, si bien que l'un d'entre eux (voire les deux) est primitif.

Enfin, si x_1 est un élément primitif de trace nulle alors $\frac{x_1}{x_2}$ est un élément primitif de K/k recherché, sauf si $\frac{x_1}{x_2} = \lambda$ appartient à k. Dans ce cas pathologique, λ est une racine primitive troisième de 1 et x_1 est racine de $X^3 - c \in k[X]$, si bien que $x_1^2 + x_1$ est encore un élément primitif de trace nulle (car x_1^2 est de trace nulle), et l'on peut prendre $y = \frac{x_1^2 + x_1}{x_2^2 + x_2} = \frac{x_1^2 + x_1}{\lambda^{-2} x_1^2 + \lambda^{-1} x_1} \notin k$.

Propriété IV.1.1 *Un polynôme f de degré n, à coefficients dans $k[t]$, d'Eisenstein pour un premier p séparable, ayant un groupe de Galois d'ordre n sur $k(t)$, est un polynôme régulier sur k.*

Démonstration En effet, ce polynôme f reste d'Eisenstein (donc irréductible) sur $\Omega[t]$ pour un facteur irréductible quelconque de p dans $\Omega[t]$ (Ω représente une clôture algébrique de k). De plus, son groupe de Galois sur $\Omega(t)$ s'injecte dans son groupe de Galois sur $k(t)$ par le morphisme de translation (selon Bourbaki)

$$\begin{array}{ccc} \mathrm{Gal}_{\Omega(t)} f & \longrightarrow & \mathrm{Gal}_{k(t)} f \\ \sigma & \longmapsto & \sigma \end{array}$$

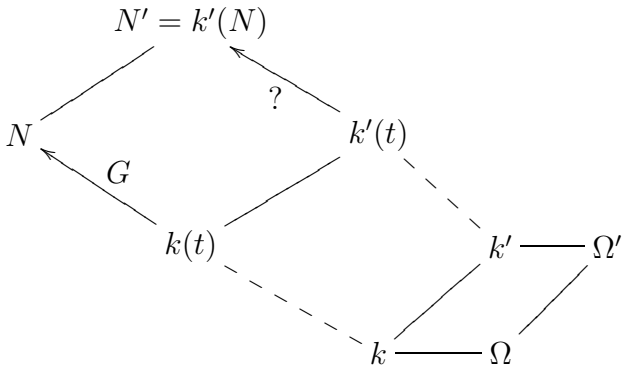
Or $|\mathrm{Gal}_{\Omega(t)} f| \geq n$ car f est irréductible sur $\Omega(t)$ et $|\mathrm{Gal}_{k(t)} f| = n$, d'où l'égalité $\mathrm{Gal}_{\Omega(t)} f = \mathrm{Gal}_{k(t)} f$. Finalement, le corps de décomposition de f sur $k(t)$ et $\Omega(t)$ sont linéairement disjoints sur $k(t)$, lui-même linéairement disjoint de Ω sur k : conclusion, le corps de décomposition de f sur $k(t)$ et Ω sont k-linéairement disjoints. Le polynôme f est bien un polynôme régulier. □

IV.1.b Propriétés essentielles des polynômes réguliers

L'intérêt particulier des polynômes réguliers vient en partie de la propriété suivante :

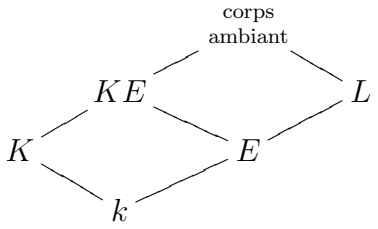
Propriété IV.1.2 *Soit k'/k une extension quelconque et t une indéterminée sur k'. Si $f \in k(t)[X]$ est régulier sur un corps k et de groupe de Galois G, alors f est régulier sur k' de groupe de Galois G.*

Démonstration Soit N le corps de décomposition de f sur $k(t)$. Considérons aussi les k'-extensions $k'(t)$ et $N' = k'(N)$ (compositum de N et k'). Le corps N' est galoisien sur $k'(t)$ car il s'agit du corps de décomposition du polynôme f sur $k'(t)$. Soit Ω' une clôture algébrique de k' et Ω la clôture algébrique de k dans Ω'. Le corps Ω est algébriquement clos.



Etant donné que t reste une indéterminée sur k', donc sur Ω', l'extension N est algébriquement indépendante de Ω' sur k. Or N est une extension régulière sur k, donc N est linéairement disjointe de Ω' sur k (voir [38], page 367, théorème 4.12). Utilisons à présent ce petit lemme de "transitivité" très classique :

Lemme IV.1.1 *Considérons le diagramme ci-contre : pour que K et L soient linéairement disjointes sur k, il faut et il suffit que K, E le soient sur k et KE, L le soient sur E.*



Ainsi, en posant $K = N, \quad E = k', \quad KE = k'N = N', \quad L = \Omega'$ dans le corps ambiant $\Omega' N$, nous constatons entre autres que N' et Ω' sont linéairement disjointes sur k'. Autrement dit N'/k' est bien une extension régulière.

De plus, N et k' sont linéairement disjointes sur k car N et Ω' le sont. En utilisant à nouveau le lemme IV.1.1 avec $K = k', \quad E = k(t), \quad KE = k'(t), \quad L = N$, dans l'ambiant N', nous constatons cette fois-ci que N et $k'(t)$ sont linéairement disjointes sur $k(t)$. Nous avons par conséquent $[N' : k'(t)] = [N : k(t)]$. Le groupe de Galois de $N'/k'(t)$ s'injecte dans celui de $N/k(t)$ par le morphisme de translation

$$\begin{array}{ccc} \mathrm{Gal}_{k'(t)} N' & \longrightarrow & G = \mathrm{Gal}_{k(t)} N \\ \sigma & \longmapsto & \sigma_{||_N} \end{array}$$

L'égalité des degrés $[N' : k'(t)] = [N : k(t)]$ implique l'égalité des groupes $\mathrm{Gal}_{k'(t)} N' = G$. Finalement, $f \in k'(t)[X]$ reste un polynôme régulier sur k' et de groupe de Galois G. □

Une conséquence directe de cette propriété est qu'il suffit de trouver un polynôme régulier sur un corps premier ($\mathbb{Q}$ ou $\mathbb{F}_p$ avec $p \in \mathbb{N}$ premier) pour avoir un polynôme régulier sur tout corps de même caractéristique.

Cependant, plus le corps k est gros, plus il facile de construire des polynômes réguliers. Par exemple, si k est algébriquement clos alors tout polynôme séparable à coefficients dans $k(t)$ est régulier. En effet toute extension E d'un corps k algébriquement clos est séparable (car k est en particulier parfait) et k est algébriquement fermé dans E : l'extension E est donc régulière sur k par définition.

Propriété IV.1.3 *Soit k un corps et t une indéterminée sur k. Soit N une extension algébrique séparable de $k(t)$ (par exemple le corps de décomposition d'un polynôme séparable à coefficients dans $k(t)$). Pour que N soit régulière sur k, il est nécessaire et suffisant que l'une des propriétés suivantes soit vérifiée :*

- *$\Omega(t)$ et N sont linéairement disjointes sur $k(t)$, où Ω est une clôture algébrique de k ;*
- *$\Omega(t) \cap N = k(t)$;*
- *k est algébriquement fermé dans N.*

Démonstration Si N est régulière sur k, c'est-à-dire N et Ω linéairement disjointes sur k (REG 2), alors N et $\Omega(t)$ sont linéairement disjointes sur $k(t)$ (lemme IV.1.1).

Si N et $\Omega(t)$ sont linéairement disjointes sur $k(t)$, alors $N \cap \Omega(t) = k(t)$. En effet, l'existence d'une famille $\{x, y\} \subset \Omega(t) \cap N$ libre sur $k(t)$ contredirait l'hypothèse de linéaire disjonction entre N et $\Omega(t)$ sur $k(t)$ ($yx - xy = 0$). La dimension de $N \cap \Omega(t)$ sur $k(t)$ est donc 1.

Si $\Omega(t) \cap N = k(t)$ alors $\Omega \cap N = \Omega \cap k(t) = k$, autrement dit k est algébriquement fermé dans N.

Finalement si k est algébriquement fermé dans N alors N régulière sur k (REG 1) car $\{t\}$ est une base de transcendance séparante de N/k. □

IV.2 Théorie de Kummer

La théorie de Kummer étudie très concrètement les extensions E abéliennes et d'exposant n d'un corps L contenant n racines n-ièmes de l'unité (leur ensemble est noté $\mathbb{U}_n$). La caractéristique de ce corps est nécessairement étrangère à n. Cette théorie met en bijection les trois données suivantes :

• l'extension galoisienne $E = L\big((b_g^{\frac{1}{n}})_g\big)$ où $(b_g)_g$ est une famille finie de L^* et $b_g^{\frac{1}{n}}$ une racine n-ième quelconque de b_g dans une clôture algébrique Ω de L. L'extension E/L est alors abélienne.

• le sous-groupe $B \subset L^*$ engendré par les $(b_g)_g$ et L^{*n} (l'ensemble des puissances n-ièmes des éléments de L^*). On possède une bijection explicite entre l'ensemble des extensions E/L finies abéliennes et l'ensemble des sous-groupes $B \subset L^*$ contenant L^{*n} et de type fini sur L^{*n} :

$$B = E^n \cap L^* \qquad \text{et} \qquad E = L(B^{\frac{1}{n}})$$

où $B^{\frac{1}{n}} = \{y \in \Omega \mid y^n \in B\} \supset \{b_g^{\frac{1}{n}}\}$.

• le groupe-quotient (fini et abélien) $B/L^{*n} = \big\langle (\overline{b_g})_g \big\rangle$ où $\overline{b_g}$ désigne la classe $b_g \mod L^{*n}$. Le groupe de Galois de E/L est isomorphe à B/L^{*n}, ou plus canoniquement au dual de B/L^{*n}, i.e. $(B/L^{*n})^\bullet = \mathrm{Hom}(B/L^{*n}, \mathbb{U}_n)$.

> Rappel. Par définition, le dual d'un groupe abélien G d'exposant m est le groupe des morphismes $\mathrm{Hom}(G, \mathbb{U}_m)$ (voir [38] pages 46-49). Plus généralement, le dual d'un groupe abélien G est formé par le groupe des morphismes de G dans l'ensemble des racines de l'unité $\mathbb{U}_\infty$.

En effet, ce dernier isomorphisme provient de l'application bi-multiplicative :

$$\begin{array}{rcl} \mathrm{Gal}_L E \times B & \longrightarrow & \mathbb{U}_n \\ (\sigma, b) & \longmapsto & \frac{\sigma(b^{\frac{1}{n}})}{b^{\frac{1}{n}}} \end{array}$$

Le noyau à gauche de ce morphisme surjectif est $\{\mathrm{Id}\}$ et son noyau à droite est L^{*n}, si bien que l'on obtient deux isomorphismes :

$$\begin{array}{rcl} \mathrm{Gal}_L E & \longrightarrow & (B/L^{*n})^\bullet \\ \sigma & \longmapsto & \left(b \mapsto \frac{\sigma(b^{\frac{1}{n}})}{b^{\frac{1}{n}}} \right) \end{array} \qquad \begin{array}{rcl} B/L^{*n} & \longrightarrow & (\mathrm{Gal}_L E)^\bullet \\ \overline{b} & \longmapsto & \left(\sigma \mapsto \frac{\sigma(b^{\frac{1}{n}})}{b^{\frac{1}{n}}} \right) \end{array}$$

Ainsi le groupe de Galois $\mathrm{Gal}_L E$ est isomorphe au dual $(B/L^{*n})^\bullet$, lui-même isomorphe à B/L^{*n} car ce dernier est un groupe abélien fini.

Cet isomorphisme est d'autant plus intéressant s'il est facile de connaître B/L^{*n}. C'est là un point fort de la théorie de Kummer : lier le problème "externe" à L qui est d'identifier le groupe de Galois de E/L et celui "interne" qui est d'identifier B/L^{*n}. Les éléments de B sont de la forme

$$\prod_g b_g^{\mathbb{Z}}\ L^{*n} = \prod_g b_g^{[0,n_g[}\ L^{*n} \quad \subset L^*$$

où n_g est l'ordre de b_g modulo L^{*n}. Par exemple, si les $(b_g)_g$ sont L^{*n}-indépendants (i.e. le produit $\prod_g \langle \overline{b_g} \rangle$ est direct dans L^*/L^{*n}), alors le cardinal de $\mathrm{Gal}_L E$ est égal au produit des n_g.

De plus, la théorie de Kummer permet de connaître une base de E/L : si $S \subset B$ est un système représentatif du quotient B/L^{*n}, alors $(s^{\frac{1}{n}})_{s\in S}$ forme une base de E/L. Nous profiterons de cette propriété pour justifier, entre autre, des indépendances L-linéaires entre certains éléments de E.

Théorème IV.2.1 (voir [14], pages 84-87) *Soit L un corps de caractéristique ne divisant pas n. On suppose que L contient n racines n-ièmes de l'unité. On identifie les sous-groupes B de L^* contenant L^{*n} et ceux de L^*/L^{*n} (L^{*n} désigne l'ensemble des puissances n-ièmes de L).*

1. *L'application $B \mapsto L(B^{\frac{1}{n}})$ est une bijection croissante de l'ensemble des sous-groupes finis $B/L^{*n} \subset L^*/L^{*n}$ sur l'ensemble des sous-extensions abéliennes de Ω (une clôture algébrique de L) d'exposant divisant n.*
   L'application réciproque est $E \mapsto E^n \cap L^*$.

2. *Pour tout sous-groupe fini B/L^{*n} de L^*/L^{*n}, l'homomorphisme*

$$\begin{array}{ccc} \mathrm{Gal}_L L(B^{\frac{1}{n}}) & \longrightarrow & \mathrm{Hom}(B/L^{*n},\ \mathbb{U}_n) \\ \sigma & \longmapsto & \left(\overline{b} \mapsto \dfrac{\sigma(b^{\frac{1}{n}})}{b^{\frac{1}{n}}}\right) \end{array}$$

   est bijectif. En particulier

$$[L(B^{\frac{1}{n}}) : L] = (B : L^{*n})$$

3. *Soit B/L^{*n} un sous-groupe fini de L^*/L^{*n}. Pour chaque $a \in B/L^{*n}$, soit Θ_a un élément de $L(B^{\frac{1}{n}})$ tel que Θ_a^n soit congru à a modulo L^{*n}. Alors les $(\Theta_a)_{a\in B/L^{*n}}$ forment une base du L-espace vectoriel $L(B^{\frac{1}{n}})$.*

Propriété IV.2.1 *Soit L un corps contenant n racines n-ièmes de l'unité. Soit B_1/L^{*n} et B_2/L^{*n} deux sous-groupes finis de L^*/L^{*n}, et les extensions de Kummer associées $E_1 = L(B_1^{\frac{1}{n}})$ et $E_2 = L(B_2^{\frac{1}{n}})$. Alors il y a équivalence entre les deux assertions suivantes :*

1. *les sous-groupes B_1/L^{*n} et B_2/L^{*n} sont en produit direct ;*

2. *les extensions E_1/L et E_2/L sont linéairement disjointes.*

Cette propriété peut facilement être généralisée à plusieurs sous-groupes de L^*/L^{*n} et extensions E/L. On obtient ainsi l'équivalence entre les deux assertions suivantes (I est un ensemble fini) :

"Les sous-groupes $\left(B_i/L^{*n}\right)_{i\in I}$ sont en produit direct."

"Les extensions $\left(E_i/L\right)_{i\in I}$ sont linéairement disjointes dans leur ensemble."

Par abus de langage, des extensions sont **linéairement disjointes dans leur ensemble** si chacune d'entre elles est linéairement disjointe du compositum des autres.

IV.3 Réalisation régulière des groupes cycliques

Dans cette section, notre objectif est de réaliser régulièrement tout groupe cyclique sur un corps k dont la caractéristique ne divise pas le cardinal du groupe cyclique. Plus précisément, nous allons réaliser les groupes cycliques sur $k(t)$ par une extension galoisienne F incluse dans le corps des séries formelles $k((t))$. Comme $k((t))$ est une extension régulière de k, il en sera bien évidemment de même pour F sur k.

Dire seulement que nous réaliserons régulièrement tous les groupes cycliques $\mathbb{Z}/n\mathbb{Z}$ (en caractéristique étrangère à n) serait réducteur. Pour chaque $n \in \mathbb{N}^*$, nous serons capables de produire toute une gamme d'extensions cycliques "bien contrôlées" : chaque extension cyclique réalisant $\mathbb{Z}/n\mathbb{Z}$ sera attachée au polynôme minimal d'un élément primitif de l'extension $k(\mathbb{U}_n)/k$. A partir de deux polynômes minimaux distincts, nous construirons deux extensions cycliques linéairement disjointes l'une de l'autre sur $k(t)$.

La technique que nous allons employer dans cette section et les suivantes peut se résumer ainsi : afin de réaliser une extension cyclique (ou abélienne) de $k(t)$, nous ajouterons au corps de base k les racines n-ièmes de l'unité : $l = k(\mathbb{U}_n)$. Cela nous permettra d'utiliser la théorie de Kummer et de contrôler facilement les groupes de Galois de certaines extensions, etc. Puis nous "rétracterons" les extensions cycliques (ou abéliennes) en prenant leurs points invariants sous l'action du groupe $\Gamma = \mathrm{Gal}_k\, l$. Disons que nous utiliserons une certaine réciprocité entre les notions "d'extension des scalaires" et de "rétraction aux points invariants", cette réciprocité provenant de la correspondance biunivoque entre les extensions de k dans $k((t))$ et celles de l dans $l((t))$ stables par l'action de $\Gamma = \mathrm{Gal}_k\, l$, correspondance biunivoque décrite par :

$$\left\{ \begin{array}{c} \text{extensions de } k \\ \text{incluses dans } k((t)) \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{extensions de } l = k(\mathbb{U}_n) \\ \text{incluses dans } l((t)),\ \text{stables par } \Gamma \end{array} \right\}$$

$$\begin{array}{rcl} F & \longmapsto & F(\mathbb{U}_n) = l(F) \\ k((t)) \cap E = E^\Gamma & \longleftarrow\!\shortmid & E \end{array}$$

On peut apporter sur cette correspondance les précisions suivantes :

$$\left\{\begin{array}{c}\text{extensions de } k(t)\\ \text{incluses dans } k((t))\end{array}\right\} \longleftrightarrow \left\{\begin{array}{l}\text{extensions de } l(t)\\ \text{incluses dans } l((t)), \text{ stables par } \Gamma\end{array}\right\}$$

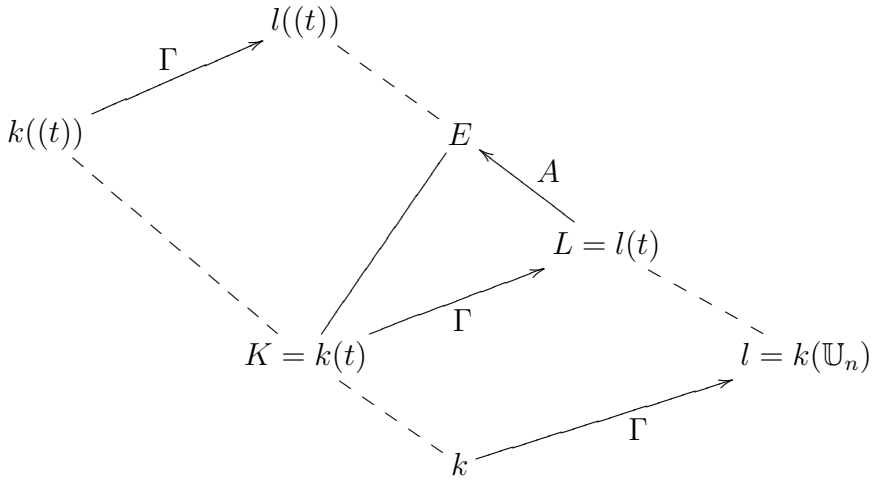
$$\begin{array}{c}F_1,\ F_2 \text{ linéairement}\\ \text{disjointes sur } k(t)=F\end{array} \longmapsto \begin{array}{c}F_1(\mathbb{U}_n),\ F_2(\mathbb{U}_n) \text{ linéairement}\\ \text{disjointes sur } l(t)=F(\mathbb{U}_n)\end{array}$$

$$\begin{array}{c}E_1^\Gamma,\ E_2^\Gamma \text{ linéairement}\\ \text{disjointes sur } k(t)=E^\Gamma\end{array} \longmapsto \begin{array}{c}E_1,\ E_2 \text{ linéairement}\\ \text{disjointes sur } l(t)=E\end{array}$$

IV.3.a Cadre de travail

Considérons donc le diagramme ci-dessous où l est une extension galoisienne de k contenant $\mathbb{U}_n$ (l'ensemble des racines n-ièmes de l'unité). Par la suite, nous poserons plus particulièrement $l = k(\mathbb{U}_n)$. Soit t une indéterminée sur l et E une extension abélienne de $L = l(t)$ contenue dans le corps des séries formelles $l((t))$.

Les automorphismes de l'extension galoisienne l/k se prolongent canoniquement en des $k(t)$-automorphismes du corps des fractions rationnelles $l(t)$. De même, ces automorphismes se prolongent (toujours canoniquement) en des $k((t))$-automorphismes du corps des séries formelles $l((t))$.



Les flèches $\rightarrow$ désignent des extensions galoisiennes dont les groupes de Galois sont précisés : par définition, $A = \mathrm{Gal}_L E$ et $\Gamma = \mathrm{Gal}_k l$.

Si le corps E est stable sous l'action du groupe Γ alors Γ s'injecte dans les K-automorphismes de E. La suite définie par les groupes d'automorphismes des extensions E/L, E/K, et L/K est par conséquent scindée (donc exacte) :

$$1 \longrightarrow A = \mathrm{Gal}_L E \longrightarrow \mathrm{Aut}_K E \underset{\longleftarrow}{\longrightarrow} \Gamma = \mathrm{Gal}_K L \longrightarrow 1$$

Dans ces conditions (existence d'une section dans cette suite exacte), le groupe $\mathrm{Aut}_K E$ est obligatoirement isomorphe au produit semi-direct $A \rtimes \Gamma$ où l'action de Γ sur A est la conjugaison intérieure dans $\mathrm{Aut}_K E$ (voir [11], pages 64-65). Finalement, comme le

cardinal de $A \rtimes \Gamma \simeq \mathrm{Aut}_K E$ est égal au degré $[E : K]$, l'extension E est galoisienne sur K de groupe $A \rtimes \Gamma$.

> Remarque due à A.C. Movahhedi. Une façon plus directe de prouver que l'extension E/K est galoisienne consiste à considérer le sous-groupe G de $\mathrm{Aut}(E)$ engendré par Γ et A. Il est clair que K est inclus dans E^G, donc G est un groupe fini de cardinal inférieur à $[E : K]$. De plus E^G est inclus dans $(E^A)^\Gamma = K$, si bien que nous avons finalement $K = E^G$ où G est un sous-groupe fini (engendré par A et Γ) de $\mathrm{Aut}(E)$.

IV.3.b Construction effective d'une extension cyclique sur $k(t)$

On suppose que la caractéristique de k ne divise pas n. On note toujours Γ le groupe des k-automorphismes de $l = k(\mathbb{U}_n)$. Chaque élément $\gamma \in \Gamma$ opère sur les racines n-ièmes de l'unité par une élévation à la puissance $i(\gamma)$ inversible modulo n. Définissons les deux applications suivantes :

$$\begin{array}{rcl} i \ : \ \Gamma \subset \mathrm{Aut}(\mathbb{U}_n) & \longrightarrow & \mathrm{U}(\mathbb{Z}/n\mathbb{Z}) \\ (w \to w^j) & \longmapsto & j \end{array} \qquad \begin{array}{rcl} \langle\ \rangle \ : \ \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \{0, \ldots, n-1\} \\ j \bmod n & \longmapsto & j \end{array}$$

Remarquer que i est un morphisme injectif de groupes commutatifs car c'est la restriction à Γ d'un isomorphisme de groupes entre $\mathrm{Aut}(\mathbb{U}_n)$ et $\mathrm{U}(\mathbb{Z}/n\mathbb{Z})$.

Soit x un élément primitif de $l = k(\mathbb{U}_n)$ sur k. Considérons l'élément de $l[t]$

$$d = \prod_{\gamma \in \Gamma} \gamma(y)^{\langle i(\gamma^{-1}) \rangle} \qquad \text{avec} \qquad y = 1 + xt \qquad \text{(voir [64], page 236)}$$

Nous verrons dans la section IV.8 (page 144) pourquoi nous imposons un tel d. Ce qui est important, ce n'est pas la valeur de d en elle-même, mais surtout la classe de d dans le quotient L^*/L^{*n} où $L = l(t)$.

$$d \equiv \prod_{\gamma \in \Gamma} \gamma(y)^{i(\gamma^{-1})} \mod L^{*n} \qquad \text{avec} \qquad y = 1 + xt$$

Pour justifier la plupart des propriétés de d, nous ferons des petits calculs dans le quotient L^*/L^{*n} : sa forme en produit et l'exposant de $\gamma(y)$ sont quasiment indispensables pour obtenir la stabilité de $E = L(d^{\frac{1}{n}})$ sous l'action de Γ et la commutation de Γ et $\mathrm{Gal}_L E$. En revanche, un bon choix de y est important pour contrôler l'ordre de la classe de d dans L^*/L^{*n}.

Dans l'anneau des séries formelles, si n est inversible (et c'est vrai dans notre cas), il existe une notion de racine n-ième canonique pour une série formelle dont le terme constant est égal à 1 : la racine n-ième d'une série formelle $f(t)$ où $f(0) = 1$ est la série $g(t)$ telle que $g^n = f$ et $g(0) = 1$. Nous donnons ainsi naissance à la racine n-ième canonique de d dans $l[[t]]$ par :

$$e = d^{\frac{1}{n}}$$

Grâce à la théorie de Kummer, nous savons que l'extension $E = L(e)$ de L est cyclique. De plus son degré est égal au degré du polynôme minimal de e sur L. Or celui-ci n'est autre que $T^n - d$ car ce dernier est irréductible : il vérifie le critère d'Eisenstein pour le premier $1 + xt$ de $l[t]$ (les éléments $\gamma(x)$ sont distincts 2 à 2 lorsque γ parcourt Γ). L'extension E/L a donc pour groupe de Galois $\mathbb{Z}/n\mathbb{Z}$. Essayons de "rétracter" l'extension E/L dans le corps $k((t))$.

Pour cela, calculons $\gamma(d) \in L^*/L^{*n}$ où γ appartient à Γ :

$$\gamma(d) \equiv \prod_{\tau\in\Gamma} \gamma\tau(y)^{i(\tau^{-1})} \equiv \prod_{\mu\in\Gamma} \mu(y)^{i(\gamma\mu^{-1})} \equiv \prod_{\mu\in\Gamma} \mu(y)^{i(\mu^{-1})i(\gamma)} \equiv d^{i(\gamma)} \qquad \mod\ L^{*n}$$

Grâce à ce calcul, nous pouvons faire le constat de trois résultats importants :

- Le corps $E = L(e) = L(d^{\frac{1}{n}})$ est stable sous l'action canonique de Γ car

$$\frac{\gamma(e)}{e^{i(\gamma)}} \equiv \left(\frac{\gamma(d)}{d^{i(\gamma)}}\right)^{\frac{1}{n}} \equiv 1 \quad \mod\ L^*$$

$$\gamma(e) = e^{i(\gamma)} q_\gamma \qquad \text{où} \qquad q_\gamma \in L^*$$

Ainsi Γ s'injecte dans les K-automorphismes de E, et comme nous l'avons vu ci-dessus (section IV.3.a), l'extension E/K est galoisienne de groupe isomorphe à $\mathbb{Z}/n\mathbb{Z} \rtimes \Gamma$.

- En réalité, ce produit semi-direct est un produit direct : les éléments de Γ commutent avec ceux de $\mathrm{Gal}_L E$. Faisons opérer ces derniers sur l'élément générateur e de E/L. Soit $\gamma \in \Gamma$ et $g \in \mathrm{Gal}_L E$:

$$\begin{aligned} \gamma \circ g(e) &= \gamma\big(w(g)e\big) = w(g)^{i(\gamma)} e^{\langle i(\gamma)\rangle} q_\gamma \\ g \circ \gamma(e) &= g(e^{\langle i(\gamma)\rangle} q_\gamma) = \big(w(g)e\big)^{\langle i(\gamma)\rangle} q_\gamma \end{aligned} \qquad \text{où } w(g) = \frac{g(e)}{e} \in \mathbb{U}_n$$

Le fait que q_γ appartienne à L et que l'exposant de e dans l'écriture de $\gamma(e)$ soit $i(\gamma)$ est primordial, voire impératif, pour obtenir la commutation de γ et g.

Ainsi l'action de Γ sur $\mathrm{Gal}_L E$ par conjugaison dans $\mathrm{Gal}_K E$ est triviale, si bien que le groupe de Galois de E sur K est le produit direct $\mathrm{Gal}_K E \simeq \mathbb{Z}/n\mathbb{Z} \times \Gamma$.

Par suite, l'extension E^Γ est galoisienne sur $K = k(t)$ de groupe de Galois $\mathbb{Z}/n\mathbb{Z}$. De plus cette dernière est incluse dans le corps des séries formelles $k((t))$, elle est donc clairement régulière sur k.

- Comme i est (un morphisme) injectif, les classes dans L^*/L^{*n} des Γ-conjugués de d sont distinctes. En utilisant une fois de plus la théorie de Kummer, ou plus simplement le fait que $X^n - d$ est le polynôme minimal de e sur L, nous savons que les éléments $\big(\gamma(e)\big)_{\gamma\in\Gamma}$ forment une famille libre sur L.

Ceci nous permet de calculer un élément primitif de E^Γ sur K. Pour cela, introduisons la trace de e sur E^Γ :

$$r = \mathrm{tr}_{E/E^\Gamma}(e) = \sum_{\gamma\in\Gamma} \gamma(e)$$

Alors r est un élément primitif de E/L. En effet, les conjugués de r sous l'action de $\mathrm{Gal}_L E$ sont en nombre maximum : si $g \in \mathrm{Gal}_L E$, alors

$$g(r) = \sum_{\gamma\in\Gamma} g\gamma(e) = \sum_{\gamma\in\Gamma} w(g)^{i(\gamma)}\gamma(e)$$

L'égalité $r = g(r)$ implique $1 = w(g)^{i(\gamma)}$ pour tout $\gamma \in \Gamma$ car les $\gamma(e)$ forment une famille libre sur L. En particulier, pour $\gamma = \mathrm{Id}$, nous obtenons $w(g) = 1$, ce qui finit par donner $g = \mathrm{Id}$. Nous concluons que r est un élément primitif de E/L (et par conséquent de E^Γ/K).

Remarquer que L et E^Γ sont des K-extensions linéairement disjointes (plutôt deux fois qu'une) : l'élément $r \in E^\Gamma$ est à la fois un élément primitif de E^Γ/K et de E/L, ou plus simplement encore $k((t)) \supset E^\Gamma$ et $L = K(\mathbb{U}_n)$ sont linéairement disjointes sur K.

Théorème IV.3.1 *Soit k un corps de caractéristique étrangère à $n \geq 2$, l/k l'extension abélienne engendrée par les racines n-ièmes de l'unité dont le groupe de Galois est noté Γ, x un élément primitif de l/k, et enfin e l'élément du corps des séries formelles $l((t))$*

$$e = \prod_{\gamma\in\Gamma} \big(1 + \gamma(x)t\big)^{\frac{\langle i(\gamma^{-1})\rangle}{n}}$$

où le morphisme $i : \Gamma \hookrightarrow \mathrm{U}(\mathbb{Z}/n\mathbb{Z})$ est défini par $\gamma(w) = w^{i(\gamma)}$ pour tout $w \in \mathbb{U}_n$, $\gamma \in \Gamma$.

Alors le polynôme minimal de $r = \sum_{\gamma\in\Gamma} \gamma(e)$ sur $k(t)$ est un polynôme régulier sur k de groupe $\mathbb{Z}/n\mathbb{Z}$, ayant un corps de décomposition inclus dans le corps des séries formelles $k((t))$ (voir [64], pages 236-237). De plus, le polynôme minimal de r est un polynôme d'Eisenstein pour le premier $p = \prod_{\gamma\in\Gamma} \big(1 + \gamma(x)t\big)$ de $k[t]$.

On peut ajouter que $p(-t)$ est le polynôme réciproque du polynôme minimal de x sur k. Choisir x revient en quelque sorte à choisir p.

Démonstration Tous les résultats ont été prouvés ci dessus, mis à part le fait que le polynôme minimal obtenu est un polynôme d'Eisenstein pour p.

Tout d'abord, p est bien irréductible dans $k[t]$ car l'idéal qu'il engendre est la trace sur $k[t]$ de l'idéal engendré par le polynôme irréductible $1 + xt$ dans $l[t]$.

En second lieu, l'idéal $(1 + xt)$ de $l[t]$ est totalement ramifié dans l'extension E, car celle-ci est engendrée par une racine e d'un polynôme $X^n - d$ d'Eisenstein pour $1 + xt$ (voir [52], pages 28-31). Soit $\mathcal{P}$ l'idéal de E au-dessus de $1 + xt$ et $v_\mathcal{P}$ la valuation qui lui est associée. Si l'on restreint la valution $v_\mathcal{P}$ au corps $K = k(t)$, alors nous obtenons la relation

$$v_p = \frac{1}{n} v_{\mathcal{P}|K}$$

Pour montrer que le polynôme minimal de r sur K est un polynôme d'Eisenstein pour p, il suffit alors de montrer que $\mathcal{P}$ divise tous les coefficients du polynôme minimal et que la valuation en $\mathcal{P}$ du terme constant est exactement n.

On vérifie alors aisément que pour $\gamma \in \Gamma$, on a $v_{\mathcal{P}}(\gamma(e)) = \langle i(\gamma) \rangle$, puis

$$v_{\mathcal{P}}(r) = v_{\mathcal{P}}\left(\sum_{\gamma\in\Gamma} \gamma(e)\right) = 1$$

car les $\gamma(e)$ ont des valuations distinctes. Enfin, pour tout $g \in \mathrm{Gal}_L E$, on a $v_{\mathcal{P}}(g(r)) = 1$ car $g.\mathcal{P} = \mathcal{P}$, et donc

$$v_{\mathcal{P}}\left(\prod_{g\in\mathrm{Gal}_L E} g(r)\right) = n$$

ce qui démontre le résultat désiré : le polynôme minimal de r est un polynôme d'Eisenstein pour le premier $p \in k[t]$. □

Corollaire IV.3.1 *Soit un nombre fini d'extensions cycliques $(F_i)_{i\in I}$ de $k(t)$ construites à partir du théorème IV.3.1 (les degrés des extensions $F_i/k(t)$ peuvent être égaux ou pas). Chacune d'entre elles est liée à un polynôme irréductible de $k[t]$, noté respectivement p_i. Si les polynômes $(p_i)_{i\in I}$ sont distincts (donc premiers entre eux 2 à 2) alors les extensions $(F_i)_{i\in I}$ sont linéairement disjointes dans leur ensemble sur $k(t)$.*

Démonstration Voir la section IV.4. Par abus de langage, des extensions sont **linéairement disjointes dans leur ensemble** si chacune d'entre elles est linéairement disjointe du compositum des autres. □

Corollaire IV.3.2 *En conservant les notations du théorème IV.3.1, dans le cas particulier où $k = \mathbb{Q}$, la seule valuation (triviale sur $\mathbb{Q}$) de $\mathbb{Q}(t)$ ramifiée dans l'extension cyclique $F = \mathbb{Q}(t, r)$ est la valuation liée au polynôme irréductible $p \in \mathbb{Q}[t]$. Celle-ci est d'ailleurs totalement ramifiée dans F. Exception : pour $n = 2$, la valuation à l'infini de $\mathbb{Q}(t)$ est également ramifiée (totalement) dans F.*

De plus, comme F est incluse dans $\mathbb{Q}((t))$, la valuation en $t \in \mathbb{Q}[t]$ est totalement décomposée dans F.

Démonstration En premier lieu, le polynôme minimal de r sur $\mathbb{Q}(t)$ étant un polynôme d'Eisenstein pour le premier $p \in \mathbb{Q}[t]$, ce dernier est totalement ramifié dans F (voir [52], pages 28-31). La valuation en p de $\mathbb{Q}(t)$ est donc totalement ramifiée dans F.

Montrons maintenant qu'il n'y a pas d'autre valuation ramifiée (sauf pour $n = 2$). Comme $F = \mathbb{Q}(t, r)$ est une extension de $\mathbb{Q}(t)$ régulière sur $\mathbb{Q}$, la structure de ramification de $F/\mathbb{Q}(t)$ est liée à celle de $\overline{\mathbb{Q}}(F)/\overline{\mathbb{Q}}(t)$ où $\overline{\mathbb{Q}}$ est une clôture algébrique de $\mathbb{Q}$. Or l'extension $\overline{\mathbb{Q}}(F)/\overline{\mathbb{Q}}(t)$ est engendrée par r mais aussi par e (notations du théorème IV.3.1). Le polynôme minimal de e sur $\overline{\mathbb{Q}}(t)$ est

$$X^n - d = X^n - \prod_{\gamma\in\Gamma} \left(1 + \gamma(x)t\right)^{\langle i(\gamma^{-1})\rangle} \qquad \Gamma = \mathrm{Gal}_{\mathbb{Q}}\, \mathbb{Q}(\mathbb{U}_n) \simeq \mathrm{U}(\mathbb{Z}/n\mathbb{Z})$$

Il est facile de voir que les premiers de $\overline{\mathbb{Q}}[t]$ qui ne sont pas des facteurs irréductibles de

$$p = \prod_{\gamma\in\Gamma} \big(1+\gamma(x)t\big)$$

ne sont pas ramifiés car ils ne divisent pas le discriminant de $X^n - d$ qui est $(-1)^{\frac{n(n-1)}{2}} n^n d^{n-1}$. Les valuations de $F/\mathbb{Q}(t)$ liées aux premiers de $\mathbb{Q}[t]$ étrangers à p ne sont donc pas ramifiées dans F. Il reste finalement à prouver que la valuation liée à t^{-1} n'est pas ramifiée sauf pour $n = 2$.

Si $n > 2$, alors nous nous plaçons sur $\overline{\mathbb{Q}}$. Effectuons le changement de variable $t = u^{-1}$. Comme la somme $\sum_{\gamma\in\Gamma} i(\gamma^{-1}) = 0 \in \mathbb{Z}/n\mathbb{Z}$, nous poserons

$$\lambda n = \sum_{\gamma\in\Gamma} \big\langle i(\gamma^{-1}\big\rangle$$

Le polynôme minimal de $u^\lambda e$ sur $\overline{\mathbb{Q}}(t)$ s'écrit alors

$$X^n - \prod_{\gamma\in\Gamma} \big(u+\gamma(x)\big)^{\langle i(\gamma^{-1})\rangle}$$

Comme u ne divise pas son discriminant, u n'est pas ramifié dans $\overline{\mathbb{Q}}(F)$. La valuation à l'infini de $k(t)$ n'est donc pas ramifiée dans F.

Dans le cas pathologique où $n = 2$, l'extension $F/\mathbb{Q}(t)$ est donnée par le polynôme du second degré $X^2 + t - 1$ dont r est une racine. Par suite, le polynôme minimal de $\frac{r}{t}$ est

$$X^2 + u(1-u) \qquad\qquad u = \frac{1}{t}$$

Ce polynôme vérifie le critère d'Eisenstein avec le premier $u \in \mathbb{Q}[u]$. Ce premier est donc totalement ramifié dans F. En conclusion, la valuation à l'infini de $\mathbb{Q}(t)$ est totalement ramifiée dans F.

Pour démontrer que t est totalement décomposé dans F, deux raisons simples peuvent être évoquées :

1) Le premier $t \in k[t]$ n'est pas ramifié dans F et le degré résiduel de tout premier de F au-dessus de t est égal à 1 car $F \subset k((t))$;

2) Le corps $k((t))$ est le complété de $k(t)$ pour la valuation liée au premier t. La factorisation du polynôme minimal de r (notation du théorème IV.3.1) dans $k((t))[X]$ reflète la factorisation de t dans $k(t,r) = F$. □

IV.3.c Résultats numériques sur $\mathbb{Q}$

Il suffit maintenant de mettre en œuvre ce théorème en machine pour obtenir une série de polynômes f_n réalisant régulièrement le groupe cyclique $\mathbb{Z}/n\mathbb{Z}$...

Nous avons mené les calculs sur le corps $\mathbb{Q}$ pour ne pas avoir de difficulté liée à la caractéristique, en choisissant une racine primitive n-ième de l'unité comme élément

primitif x de l'extension cyclotomique $\mathbb{Q}(\mathbb{U}_n)/\mathbb{Q}$. Nous obtenons ainsi des polynômes d'Eisenstein pour les premiers $\Phi_n(-t) \in \mathbb{Q}[t]$.

Les polynômes obtenus sont très proches de ceux de R. Dentzer dans [24], ou de Y. Eichenlaub dans [31] pour les polynômes f_9 et f_{11}. En revanche, le temps d'obtention de ces polynômes est nettement moindre que celui donné par R. Dentzer. En effet, il lui faut moins d'un jour pour obtenir l'un des f_i pour $i \leq 16$ ou $i \in \{18, 20\}$. Pour $i = 17$, il escompte un temps de calcul d'un an ! Avec la méthode que nous employons, il faut à peine une nuit pour obtenir tous les f_i où $i \leq 18$ et $i = 20$... Ceci n'est pas dû aux logiciels de calcul formel différents, mais à la manière dont les calculs ont été menés : l'utilisation des séries formelles est apparemment nettement plus efficace.

$$f_2 = X^2 + t - 1$$

$$\begin{aligned} f_3 = \ & X^3 - 3\ p\ X + (t-2)\ p \\ & \text{avec} \\ & p = t^2 - t + 1 \end{aligned}$$

$$\begin{aligned} f_4 = \ & X^4 - 4\ p\ X^2 + 4\ t^2\ p \\ & \text{avec} \\ & p = t^2 + 1 \end{aligned}$$

$$\begin{aligned} f_5 = \ & X^5 - 10\ p\ X^3 + 5\ (t^2 + 2\ t - 4)\ p\ X^2 + 5\ (t+1)\ (2\ t^3 - 4\ t^2 + 6\ t - 3)\ p\ X \\ & + p\ (t^6 - 9\ t^5 + 10\ t^4 - 10\ t^3 + 5\ t^2 + 6\ t - 4) \\ & \text{avec} \\ & p = t^4 - t^3 + t^2 - t + 1 \end{aligned}$$

$$\begin{aligned} f_6 = \ & X^6 - 6\ p\ X^4 + 9\ p^2\ X^2 - (t^2 - 2\ t - 2)^2\ p \\ & \text{avec} \\ & p = t^2 + t + 1 \end{aligned}$$

$$\begin{aligned} f_7 = \ & X^7 - 21\ p\ X^5 - 7\ (3\ t^3 - 5\ t^2 - 5\ t + 10)\ p\ X^4 \\ & + 7\ p\ (13\ t^6 - 6\ t^5 + 13\ t^4 - 27\ t^3 + 20\ t^2 + 15\ t - 15)\ X^3 \\ & + 7\ p\ (16\ t^9 - 31\ t^8 + 2\ t^7 + 35\ t^6 - 14\ t^5 + 35\ t^4 - 63\ t^3 + 30\ t^2 + 18\ t - 12)\ X^2 \\ & - 7\ (t+1)\ p\ (12\ t^{11} - 8\ t^{10} + 30\ t^9 - 113\ t^8 + 166\ t^7 - 126\ t^6 \\ & \qquad + 91\ t^5 - 93\ t^4 + 62\ t^3 - 5\ t^2 - 15\ t + 5)\ X \\ & - p\ (97\ t^{15} - 29\ t^{14} - 189\ t^{13} + 175\ t^{12} + 84\ t^{11} + 126\ t^{10} - 427\ t^9 + 131\ t^8 \\ & \qquad + 271\ t^7 - 91\ t^6 - 70\ t^5 - 63\ t^4 + 126\ t^3 - 35\ t^2 - 15\ t + 6) \\ & \text{avec} \\ & p = t^6 - t^5 + t^4 - t^3 + t^2 - t + 1 \end{aligned}$$

$$f_8 = X^8 - 16\,p\,X^6 + 32\,t^2\,(t^2+4)\,p\,X^4 - 256\,t^4\,(t^2+1)\,p\,X^2 + 256\,t^8\,p$$
avec
$p = t^4 + 1$

$$\begin{aligned} f_9 = {} & X^9 - 27\,p\,X^7 + 54\,(t-1)\,(t+1)\,p\,X^6 + 243\,t^2\,(t^4 - t^2 - t + 2)\,p\,X^5 \\ & -243\,(t-1)\,t^2\,(t+1)\,(3\,t^4 - t^3 - t^2 - 2\,t + 4)\,p\,X^4 \\ & -81\,t^4\,p\,(10\,t^8 + 3\,t^7 - 36\,t^6 - 16\,t^5 + 69\,t^4 + 6\,t^3 - 26\,t^2 - 33\,t + 33)\,X^3 \\ & +2187\,(t-1)\,t^4\,(t+1)\,p\,(t^8 - t^6 - 3\,t^5 + 4\,t^4 + t^3 - t^2 - 2\,t + 2)\,X^2 \\ & +729\,t^6\,(t^3-2)\,p\,(t^9 + t^8 - 9\,t^7 - t^6 + 17\,t^5 - 14\,t^3 - 2\,t^2 + 9\,t - 3)\,X \\ & +243\,t^8\,p\,(t^{13} - 3\,t^{12} - 15\,t^{11} + 21\,t^{10} + 54\,t^9 - 36\,t^8 - 87t^7 \\ & \qquad -9\,t^6 + 81\,t^5 + 64\,t^4 - 30\,t^3 - 60\,t^2 - 18\,t + 36) \end{aligned}$$
avec
$p = t^6 - t^3 + 1$

$$\begin{aligned} f_{10} = {} & X^{10} - 20\,p\,X^8 + 10\,p\,(12\,t^4 + 17\,t^3 + 17\,t^2 + 7\,t + 7)\,X^6 \\ & -25\,p\,(9\,t^8 + 38\,t^7 + 67\,t^6 + 46\,t^5 + 25\,t^4 + 16\,t^3 + 12\,t^2 + 8\,t + 4)\,X^4 \\ & +5\,p\,(18\,t^{12} + 164\,t^{11} + 613\,t^{10} + 1125\,t^9 + 1050\,t^8 + 214\,t^7 \\ & \qquad -453\,t^6 - 376\,t^5 - 125\,t^4 - 50\,t^3 + 18\,t^2 + 39\,t + 13)\,X^2 \\ & -p\,(t^8 - 3\,t^7 - 32\,t^6 - 36\,t^5 + 10\,t^4 + 34\,t^3 + 13\,t^2 - 8\,t - 4)^2 \end{aligned}$$
avec
$p = t^4 + t^3 + t^2 + t + 1$

f_{11} énorme... voir [31], pages 85-86.

$$\begin{aligned} f_{12} = {} & X^{12} - 24\,p\,X^{10} + 72\,p\,(2\,t^4 - t^2 + 2)\,X^8 \\ & -16\,p\,(4\,t^8 + 31\,t^6 - 6\,t^4 + 10\,t^2 + 16)\,X^6 \\ & +48\,t^2\,p\,(8\,t^8 - 17\,t^6 + 61\,t^4 - 53\,t^2 + 32)\,X^4 \\ & -576\,t^4\,(t^2-2)^2\,p^2\,X^2 + 64\,t^6\,(t^2-2)^4\,p \end{aligned}$$
avec
$p = t^4 - t^2 + 1$

$\vdots$

IV.3.d Résultats numériques en caractéristique non nulle

Ces polynômes $f_n \in \mathbb{Z}[t][X]$ ont été calculés pour réaliser régulièrement les groupes cycliques $\mathbb{U}_n$ sur $\mathbb{Q}(t)$. En réalité...

Propriété IV.3.1 *Quel que soit le corps k de caractéristique q étrangère à n et sur lequel t reste une indéterminée, ces polynômes f_n sont toujours réguliers sur k et de groupe de Galois $\mathbb{U}_n$ sur $k(t)$.*

Démonstration La propriété IV.1.2 permet de nous convaincre de ce fait si nous le prouvons seulement pour les corps premiers. Pour $k = \mathbb{Q}$ c'est clair, et pour $k = \mathbb{F}_q$ où q

est un nombre premier ne divisant pas n, nous le démontrons maintenant. Notons avec une barre $\bar{}$ les éléments de $\mathbb{Z}[t,X]$ que nous réduirons modulo q dans $\mathbb{F}_q[t,X]$.

Le polynôme $f_n \in \mathbb{Z}[t][X]$ est un polynôme d'Eisenstein pour $\Phi_n(-t)$. Comme q (la caractéristique de $\mathbb{F}_q$) ne divise pas n, le polynôme cyclotomique $\overline{\Phi_n(-t)}$ est séparable dans $\mathbb{F}_q[t]$ et $\overline{f_n} \in \mathbb{F}_q[t,X]$ reste un polynôme d'Eisenstein (irréductible) pour n'importe quel facteur premier de $\overline{\Phi_n(-t)}$ dans $\mathbb{F}_q[t]$.

De plus, $\overline{f_n}$ est séparable dans $\mathbb{F}_q[t][X]$: en effet, un polynôme irréductible est séparable si et seulement si sa dérivée n'est pas nulle. Ici, $\overline{f_n}'$ n'est pas nulle car son monôme dominant est $\overline{nX^{n-1}} \neq 0$ (q ne divise pas n). Autrement dit $\overline{f_n}$ est irréductible séparable.

Montrons à présent que le groupe de Galois de $\overline{f_n}$ sur $\mathbb{F}_q(t)$ est cyclique. Par suite, la propriété IV.1.1 justifiera qu'il est régulier sur $\mathbb{F}_q$. Soit $x_1,\dots,x_n$ les n racines de f_n dans une clôture algébrique de $\mathbb{Q}(t)$ et $d \in \mathbb{Z}[t]$ son discriminant. Considérons l'algèbre $A = \mathbb{Z}[t,d^{-1},x_1,\dots,x_n]$ sur l'anneau intégralement clos $R = \mathbb{Z}[t,d^{-1}]$. Celle-ci vérifie les hypothèses du théorème I.1.1 car $A^{\mathbb{U}_n} = R$.

> Remarque. En réalité A est une R-algèbre galoisienne (de groupe de Galois $\mathbb{U}_n$) car A est un quotient de l'algèbre de décomposition universelle $\mathbb{D}^{f_n}_{\mathbb{Z}[t,d^{-1}]}$. Cette dernière est galoisienne sur $\mathbb{Z}[t,d^{-1}]$ car $d = \operatorname{dis}(f_n)$ est inversible dans $\mathbb{Z}[t,d^{-1}]$.

Comme $\overline{f_n}$ est séparable sur $\mathbb{F}_q[t]$, le discriminant $d \in \mathbb{Z}[t]$ de f_n ne devient pas nul modulo q. Dit de façon différente, l'idéal premier engendré par q dans $\mathbb{Z}[t]$ ne rencontre pas les puissances de d. Ainsi q est premier dans R, et $R/qR = \mathbb{F}_q[t,\overline{d^{-1}}]$. Soit $\mathcal{P}$ un idéal premier au-dessus de q dans la R-algèbre A. Posons

$$k = \operatorname{Frac} R/qR = \mathbb{F}_q(t) \qquad k' = \operatorname{Frac} A/\mathcal{P} = \mathbb{F}_q(t,\overline{x_1},\dots,\overline{x_n})$$

où $\overline{x_i}$ désigne la classe de x_i modulo $\mathcal{P}$.

L'extension k'/k est galoisienne et le théorème I.1.1 prouve que le sous-groupe $\operatorname{Stab}_{\mathbb{U}_n}(\mathcal{P})$ "se surjecte" sur $\operatorname{Gal}_k k'$. Or $|\operatorname{Gal}_k k'| \geq n$ car $\overline{f_n}$ est irréductible, donc $\operatorname{Gal}_k k' = \mathbb{U}_n$. Finalement $\overline{f_n}$ est un polynôme d'Eisenstein dont le groupe de Galois sur $\mathbb{F}_q(t)$ est cyclique d'ordre n. Il est par conséquent régulier sur $\mathbb{F}_q$. □

Dans cette démonstration, nous aurions pu utiliser le théorème II.7.3, page 74. De façon plus générale, en utilisant le chapitre I, nous avons également le résultat qui suit :

Propriété IV.3.2 *Soit A une algèbre galoisienne sur R de groupe G, et $\mathcal{P}$ un idéal premier de A au-dessus de l'idéal $\mathfrak{p} \subset R$. Si $R/\mathfrak{p}$ est intégralement clos alors $A/\mathcal{P}$ est une algèbre galoisienne sur $R/\mathfrak{p}$ de groupe $D(\mathcal{P}) = \{g \in G \mid g.\mathcal{P} = \mathcal{P}\}$.*

IV.4 Réalisation régulière des groupes abéliens finis

Dans cette section, notre objectif est de réaliser régulièrement tout groupe abélien A fini sur un corps k dont la caractéristique est étrangère à l'exposant du groupe abélien A. Il revient au même de supposer que le cardinal de A n'est pas divisible par la caractéristique de k.

Plus précisément, nous allons réaliser le groupe abélien A sur $k(t)$ par une extension galoisienne F incluse dans le corps des séries formelles $k((t))$. Comme $k((t))$ est une extension régulière de k, il en sera bien évidemment de même pour F sur k. Les résultats acquis dans la section précédente nous serviront d'appui : un groupe abélien fini est un $\mathbb{Z}$-module fini, autrement dit, il se décompose en somme directe finie

$$A \simeq \bigoplus_{j\in J} \mathbb{Z}/n_j\mathbb{Z}$$

Étant donné que nous savons déjà réaliser tous les groupes cycliques régulièrement dans le corps des séries formelles $k((t))$, il suffit à présent d'en "regrouper" quelques uns pour obtenir une réalisation régulière de A sur k.

IV.4.a Construction effective d'une extension abélienne

Soit $l = k(\mathbb{U}_n)$ l'extension galoisienne de k engendrée par les racines n-ièmes de l'unité (n est l'exposant du groupe abélien A). Notons Γ son groupe de Galois.

Nous allons maintenant reprendre rapidement la section IV.3 pour chaque n_j. Nous avons considéré x_j un élément primitif de l'extension galoisienne $l_j = k(\mathbb{U}_{n_j}) \subset l$ de k (dont le groupe de Galois est Γ_j) donnant naissance au polynôme $d_j \in l_j[t]$:

$$d_j = \prod_{\gamma\in\Gamma_j} \gamma(y_j)^{\left\langle i(\gamma^{-1})\right\rangle_j} \qquad \text{avec} \qquad y_j = 1 + x_j t$$

où l'application i est définie par $\gamma(w) = w^{i(\gamma)}$ pour tout $w \in \mathbb{U}_n$, et $\langle\lambda\rangle_j$ est un relèvement dans l'ensemble $\{0, \ldots, n_j - 1\}$ de λ mod n_j. Nous avons introduit ensuite sa racine n_j-ième canonique dans l'algèbre des séries formelles

$$e_j = (d_j)^{\frac{1}{n_j}} = \left(d_j^{\frac{n}{n_j}}\right)^{\frac{1}{n}}$$

Alors l'extension $L_j(e_j)$ de $L_j = l_j(t)$ est une extension cyclique de groupe $\mathbb{Z}/n_j\mathbb{Z}$.

Regardons à présent les x_j comme des éléments de l et supposons qu'ils soient non conjugués 2 à 2 sur k. Considérons les polynômes de $l[t]$

$$d'_j = (d_j)^{\frac{n}{n_j}} = \prod_{\gamma\in\Gamma_j} \gamma(y_j)^{\frac{n}{n_j}\left\langle i(\gamma^{-1})\right\rangle_j} \qquad \text{avec} \qquad y_j = 1 + x_j t$$

Ces polynômes d'_j sont deux à deux étrangers, si bien que le groupe qu'ils engendrent dans le quotient L^*/L^{*n} est égal au produit direct des groupes que chacun d'entre eux engendre dans L^*/L^{*n}.

Enfin, l'ordre du groupe engendré par d'_j modulo L^{*n} est exactement n_j : il suffit pour s'en persuader de considérer la valuation de d'_j en le premier $(1 + x_j t)$ de $l[t]$. Le lecteur pourra constater qu'elle est égale à $\frac{n}{n_j}$. Finalement, nous obtenons :

$$\left\langle (d'_j)_{j\in J}, L^{*n}\right\rangle / L^{*n} = \prod_{j\in J} \left\langle d'_j, L^{*n}\right\rangle / L^{*n} \simeq \bigoplus_{j\in J} \mathbb{Z}/n_j\mathbb{Z}$$

où $\langle X, L^{*n}\rangle$ désigne le sous-groupe de L^* engendré par X et L^{*n}.

Autrement dit, en termes d'extensions de $L = l(t)$, les extensions $E_j = L(e_j)$ sont linéairement disjointes sur L dans leur ensemble et le groupe de Galois sur L de leur compositum $E \subset l((t))$ est le produit direct des groupes $\mathrm{Gal}_L E_j$. Ainsi, et toujours par la théorie de Kummer, le groupe de Galois de E/L est isomorphe au groupe abélien A.

Nous venons de construire une extension abélienne E sur le corps $L = l(t)$ en considérant des extensions cycliques E_j linéairement disjointes sur L. Cette extension E est incluse dans le corps $l((t))$ régulier sur l. Il nous faut maintenant rétracter cette extension dans $k((t))$.

Dans la section précédente, quel que soit $j \in J$, nous avons montré que l'élément de $k((t))$

$$r_j = \sum_{y \in \Gamma.e_j} y$$

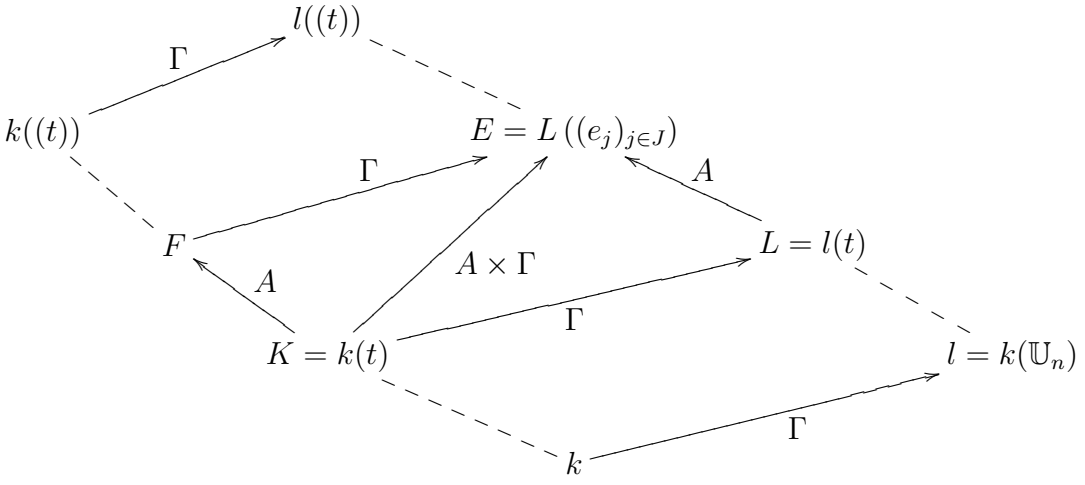
est un élément primitif d'une K-extension cyclique F_j de groupe $\mathbb{Z}/n_j\mathbb{Z}$. De plus, cet élément r_j a la propriété d'engendrer sur $L_j = k(\mathbb{U}_{n_j}, t)$ le même corps que e_j. A fortiori, nous avons l'égalité $L(e_j) = L(r_j)$. Nous possédons alors un nouveau système de générateurs de l'extension $E = \prod_j L(e_j)$ sur L :

$$E = L\big((r_j)_{j\in J}\big)$$

Soit $F = \prod_j F_j$ le compositum des extensions $F_j = K(r_j)$ de K. Cette extension F est abélienne sur K car les F_j sont galoisiennes cycliques sur K. Elle est de plus linéairement disjointe de L sur K car le corps F est inclus dans $k((t))$. Ainsi nous obtenons directement

$$\mathrm{Gal}_K F = \mathrm{Gal}_L F.L = \mathrm{Gal}_L E \simeq A$$

Il est alors facile de se convaincre que les K-extensions $(F_j)_{j\in J}$ sont linéairement disjointes dans leur ensemble puisque leur compositum sur K possède un groupe de Galois de cardinal maximal, i.e. le produit des cardinaux des groupes $\mathrm{Gal}_K F_j$.



Lemme IV.4.1 *Soit $F_j = K(r_j)$ des extensions galoisiennes d'un corps K de groupes de Galois respectifs G_j. Si les extensions F_j sont linéairement disjointes "dans leur ensemble" sur K, alors leur compositum $F = \prod_j F_j$ est une extension galoisienne de K de groupe Galois le produit direct $G = \prod_j G_j$.*

De plus, si l'on suppose que la caractéristique de K ne divise le cardinal d'aucun groupe G_j, alors l'élément $r = \sum_j r_j$ est un élément primitif de F/K.

Démonstration La première partie du lemme est classique. Attachons-nous à démontrer la dernière ligne. Quel est le nombre de G-conjugués de r ?

Soit $a \in G$. Analysons l'égalité $a(r) = r$. Celle-ci est équivalente à

$$a(r_i) - r_i = \sum_{j \neq i} r_j - a(r_j)$$

Ainsi, $a(r_i) - r_i$ appartient à $F_i \cap \prod_{j \neq i} F_j$. Or l'extension $F_i = K(r_i)$ et le compositum $\prod_{j \neq i} F_j$ sont linéairement disjoints sur K (traduction de "les K-extensions F_j pour $j \in J$ sont linéairement disjointes dans leur ensemble"). Donc $a(r_i) - r_i$ est égal à une certaine constante λ_i du corps de base K. Or la trace sur K de $a(r_i) - r_i$ est nulle, celle de λ_i est $|G|\lambda_i$. Ainsi on obtient $|G|\lambda_i = 0$, ou encore $\lambda_i = 0$ car le cardinal de G est étranger à la caractéristique. Conclusion :

$$a(r_i) = r_i \qquad \text{quel que soit } i$$

L'automorphisme a est donc l'identité de $F = K\big((r_j)_j\big)$. L'élément $r \in F$ possède le nombre maximum de conjugués, il s'agit donc d'un élément générateur de F/K. □

Théorème IV.4.1 *Soit k un corps de caractéristique étrangère à n, l/k l'extension abélienne engendrée par les racines n-ièmes de l'unité dont le groupe de Galois est noté Γ. On se fixe des entiers n_j dont le p.p.c.m. est exactement n, des éléments x_j primitifs de $k(\mathbb{U}_{n_j})/k$ non 2 à 2 conjugués sur k, et enfin les éléments e_j, puis r_j, définis dans le théorème IV.3.1 (page 110) et appartenant respectivement aux algèbres de séries formelles $l[[t]]$ et $k[[t]]$. Les extensions $k(t, r_j)$ de $k(t)$ sont linéairement disjointes dans leur ensemble (car les x_j sont non conjugués 2 à 2 sur k).*

Alors la somme $r = \sum_j r_j$ engendre sur $k(t)$ une extension abélienne de groupe de Galois $A \simeq \oplus_j \mathbb{Z}/n_j\mathbb{Z}$, incluse dans $k((t))$. Le polynôme minimal de r sur $k(t)$ est par conséquent un polynôme régulier sur k réalisant le groupe abélien A.

Corollaire IV.4.1 *En conservant les notations du théorème IV.4.1, dans le cas particulier où $k = \mathbb{Q}$, les seules valuations (triviales sur $\mathbb{Q}$) de $\mathbb{Q}(t)$ ramifiées dans l'extension abélienne $F = \mathbb{Q}(t, r)$ sont les valuations liées aux polynômes irréductibles $p_j = \prod_{y \in \Gamma . x_j} (1 + yt) \in \mathbb{Q}[t]$, et la valuation à l'infini si $2 \in \{n_j \mid j \in J\}$.*

Démonstration Dans le compositum $F = \prod_j F_j$, une valuation de $\mathbb{Q}(t)$ est ramifiée si et seulement si elle l'est dans l'une des extensions F_j. □

IV.4.b Résultats numériques sur $\mathbb{Q}$

Voici à présent des polynômes obtenus par le théorème IV.4.1 réalisant les groupes abéliens finis non cycliques.

Nous avons mené les calculs sur $\mathbb{Q}$ à la fois pour des raisons de caractéristique, mais aussi de liberté dans le choix des générateurs de $\mathbb{Q}(\mathbb{U}_n)$. Nous avons choisi, pour les x_j, des multiples de racines primitives n_j-ièmes de l'unité. Ainsi les polynômes calculés dans la section IV.3 nous serviront à volonté : $f_{n_j}(t,X)$ et $f_{n_j}(2t,X)$ correspondent respectivement aux polynômes minimaux de $r(x)$ et $r(2x)$ si x est une racine primitive n_j-ième de 1. Pour s'en convaincre, il suffit de regarder les expressions de $d(x)$ et de $e(x)$, page 108. Autrement dit, $f_{n_j}(t,X)$ et $f_{n_j}(2t,X)$ réalisent régulièrement le même groupe cyclique dans $k((t))$ sur $k(t)$, mais leurs corps de décomposition sont linéairement disjoints sur $k(t)$.

> Remarque. Les corps de décomposition des deux polynômes $f_{n_j}(t,X)$ et $f_{n_j}(2t,X)$ sont inclus dans $\mathbb{Q}((t))$: en effet, ce fait est déjà établi pour $f_{n_j}(t,X)$. Ainsi, $f_{n_j}(2t,X)$ se décompose totalement dans $\mathbb{Q}((2t))$. Or $\mathbb{Q}((2t)) = \mathbb{Q}((t))$... Alors que $\mathbb{Q}((t+1)) \neq \mathbb{Q}((t))$. C'est pour cela que nous ne considérons pas $f_{n_j}(t+1,X)$.

Le théorème IV.4.1 nous donne un élément $r = \sum_j r_j$ engendrant une extension abélienne. Or nous connaissons les polynômes minimaux des éléments r_j : il s'agit bien sûr des f_{n_j}. Pour obtenir le polynôme minimal de $r = \sum_j r_j$, on peut par exemple calculer le polynôme caractéristique de $\sum_j \overline{Y_j}$ dans l'algèbre

$$\mathbb{Q}[t,(Y_j)_{j\in J}]/\left\langle f_{n_j}(Y_j) \mid j\in J\right\rangle \simeq \bigotimes_{j\in J}{}_{\mathbb{Q}[t]}\ \mathbb{Q}[t,Y_j]/\left\langle f_{n_j}(Y_j)\right\rangle$$

Comme tout polynôme caractéristique dans une tour d'algèbres monogènes, celui-ci se calcule via une succession de résultants du type suivant : si f et g sont deux polynômes unitaires alors le résultant en Y

$$\mathrm{res}_Y(f(Y), g(X-Y))$$

est un polynôme unitaire en X dont les racines sont les sommes des racines de f et de g (avec multiplicité si f ou g ne sont pas séparables).

Enfin, sachant que les extensions $\mathbb{Q}(t,r_j)$ sont linéairement disjointes "dans leur ensemble" sur $\mathbb{Q}(t)$ et que r est un élément primitif de leur compositum

$$F = \mathbb{Q}(t,r) = \mathbb{Q}\big(t,(r_j)_{j\in J}\big) \simeq \mathrm{Frac}\left(\bigotimes_{j\in J}{}_{\mathbb{Q}[t]}\ \mathbb{Q}[t,Y_j]/\left\langle f_{n_j}(Y_j)\right\rangle\right)$$

le polynôme minimal de r sur $\mathbb{Q}(t)$ est exactement son polynôme caractéristique dans l'extension $F/\mathbb{Q}(t)$. Nous calculons ainsi très facilement des polynômes abéliens à partir des f_{n_j}.

$\big(\mathbb{Z}/2\mathbb{Z}\big)^2$: $X^4 - 4\,X^2 + 4\,t^2$
en choisissant $f_2(t,X)$ et $f_2(-t,X)$.

$\big(\mathbb{Z}/2\mathbb{Z}\big)^3$: $X^8 - 4\,(2\,t+3)\,X^6 + 2\,(16\,t^2+20\,t+15)\,X^4 + 4\,(16\,t^3-14\,t-7)\,X^2$
$+(8\,t^2-4\,t-3)^2$
en choisissant $f_2(t,X)$, $f_2(-t,X)$, et $f_2(2t,X)$.

$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$: $X^8 - 4\,(2\,t^2-t+3)\,X^6 + 2\,(12\,t^4-4\,t^3+27\,t^2-10\,t+15)\,X^4$
$-4\,(8\,t^6+4\,t^5+10\,t^4-t^3+11\,t^2-7\,t+7)\,X^2$
$+(4\,t^4+4\,t^3+t^2+2\,t-3)^2$
en choisissant $f_2(t,X)$ et $f_4(t,X)$.

$\big(\mathbb{Z}/3\mathbb{Z}\big)^2$: $X^9 - 18\,(t^2+1)\,X^7 - 6\,(3\,t^2+2)\,X^6 + 27\,(3\,t^4+7\,t^2+3)\,X^5$
$+36\,(3\,t^4+7\,t^2+1)\,X^4 - 3\,(27\,t^6+135\,t^4+123\,t^2+56)\,X^3$
$-216\,t^2\,(3\,t^2+2)\,X^2 + 36\,(9\,t^6-3\,t^4+7\,t^2+4)\,X + 8\,(27\,t^6+18\,t^2-8)$
en choisissant $f_3(t,X)$ et $f_3(-t,X)$.

$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$: $X^{12} - 6\,(2\,t^2-3\,t+3)\,X^{10} + 3\,(18\,t^4-48\,t^3+83\,t^2-70\,t+35)\,X^8$
$-2\,(55\,t^6-195\,t^5+441\,t^4-608\,t^3+594\,t^2-348\,t+116)\,X^6$
$+3\,(31\,t^8-126\,t^7+426\,t^6-848\,t^5+1092\,t^4$
$\quad -936\,t^3+536\,t^2-192\,t+48)\,X^4$
$-6\,t^2\,(3\,t^8-12\,t^7+116\,t^6-352\,t^5+584\,t^4$
$\quad -624\,t^3+432\,t^2-192\,t+48)\,X^2$
$+t^4\,(t^4+12\,t^3-24\,t^2+24\,t-12)^2$
en choisissant $f_2(t,X)$ et $f_6(t,X)$.

$\big(\mathbb{Z}/2\mathbb{Z}\big)^4$: $X^{16} - 32\,X^{14} + 16\,(5\,t^2+22)\,X^{12} - 128\,(5\,t^2+14)\,X^{10}$
$-32\,(197\,t^4-120\,t^2-136)\,X^8 + 512\,(105\,t^4-40\,t^2-8)\,X^6$
$+256\,t^2\,(685\,t^4-602\,t^2+160)\,X^4 + 18432\,t^4\,(5\,t^2-2)\,X^2 + 20736\,t^8$
en choisissant $f_2(t,X)$, $f_2(-t,X)$, $f_2(2t,X)$ et $f_2(-2t,X)$.

$\big(\mathbb{Z}/2\mathbb{Z}\big)^2\times\mathbb{Z}/4\mathbb{Z}$: $X^{16} - 16\,(t^2+2)\,X^{14} + 16\,(7\,t^4+24\,t^2+22)\,X^{12}$
$-64\,(7\,t^6+26\,t^4+46\,t^2+28)\,X^{10}$
$+32\,(35\,t^8+96\,t^6+232\,t^4+320\,t^2+136)\,X^8$
$-256\,(7\,t^{10}+6\,t^8+8\,t^6+64\,t^4+72\,t^2+16)\,X^6$
$+256\,t^2\,(7\,t^{10}-8\,t^8+6\,t^6+48\,t^2+64)\,X^4$
$-1024\,t^6\,(t^8-2\,t^6-14\,t^4+4\,t^2+16)\,X^2 + 256\,t^{16}$
en choisissant $f_2(t,X)$, $f_2(-t,X)$ et $f_4(t,X)$.

$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}$: un peu trop volumineux...

en choisissant $f_2(t,X)$ et $f_8(t,X)$.

$$\begin{aligned}\left(\mathbb{Z}/4\mathbb{Z}\right)^2 \ : \ & X^{16} - 16\,(5\,t^2+2)\,X^{14} + 16\,(159\,t^4+115\,t^2+22)\,X^{12} \\ & -64\,(635\,t^6+611\,t^4+220\,t^2+28)\,X^{10} \\ & +32\,(10643\,t^8+11610\,t^6+5983\,t^4+1480\,t^2+136)\,X^8 \\ & -256\,(5715\,t^{10}+5812\,t^8+4015\,t^6+1590\,t^4+280\,t^2+16)\,X^6 \\ & +256\,t^2\,(12879\,t^{10}+6525\,t^8+6595\,t^6+4755\,t^4+1470\,t^2+160)\,X^4 \\ & -9216\,t^4\,(405\,t^{10}-225\,t^8+115\,t^6+225\,t^4+60\,t^2+4)\,X^2 \\ & +20736\,t^8\,(9\,t^4-10\,t^2-3)^2\end{aligned}$$

en choisissant $f_4(t,X)$ et $f_4(2t,X)$ (car $f_4(t,X) = f_4(-t,X)$).

$\vdots$

IV.5 Réalisation régulière du groupe diédral de tout groupe abélien fini

Dans cette section, notre objectif est de réaliser régulièrement le groupe diédral D_A de tout groupe abélien fini A sur un corps k dont la caractéristique ne divise pas le cardinal de D_A, c'est-à-dire $2|A|$. On rappelle que $D_A = A \rtimes \mathbb{U}_2$ où $\mathbb{U}_2 = \{1,-1\}$ opère sur A (abélien) par simple exponentiation par $-1 : a \mapsto a^{-1}$.

Plus précisément, nous allons réaliser les groupes diédraux sur $k(t)$ par une extension galoisienne F incluse dans le corps des séries formelles $k((t^{\frac{1}{2}}))$. Comme $k((t^{\frac{1}{2}}))$ est une extension régulière de k, il en sera bien évidemment de même pour F sur k.

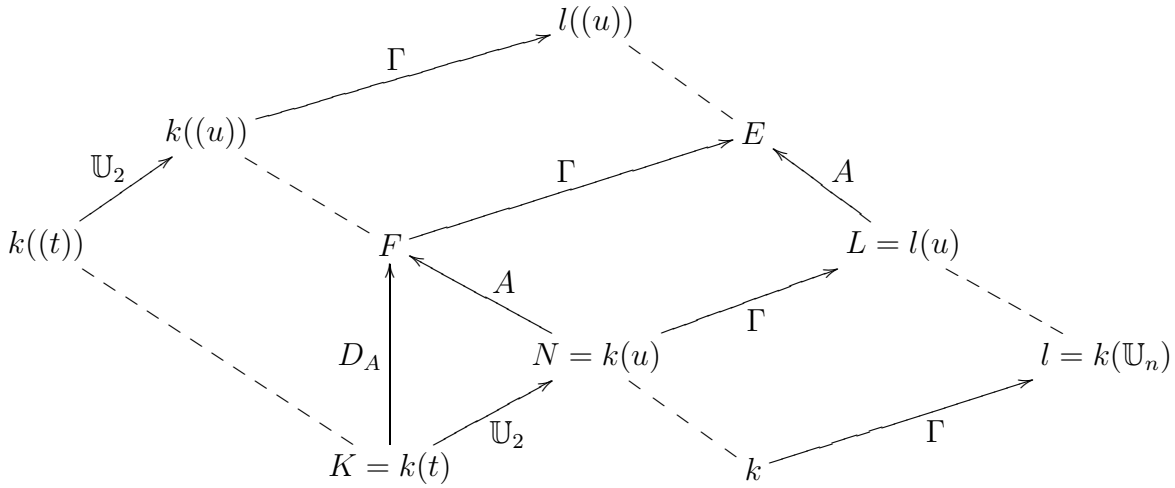
IV.5.a Construction d'une extension abélienne "convenable"

Avant de réaliser le groupe diédral D_A dans $k((t^{\frac{1}{2}}))$, il paraît assez logique de construire une extension abélienne de groupe A. Or, la section IV.4 nous montre comment on peut s'y prendre. Soit u une racine carrée de t.

$$u = \sqrt{t}$$

Nous constatons facilement que le corps engendré par u sur $k(t)$ est égal à $k(u)$ car $u^2 = t$... Considérons donc u comme une indéterminée sur k.

Voici le cadre que nous allons essayer d'obtenir afin de réaliser le groupe diédral D_A :



où n est l'exposant du groupe fini abélien A.

L'obstacle que nous devons franchir dans cette section IV.5 est la construction d'une extension abélienne F/N qui soit stable par l'action du groupe $\mathrm{Gal}_K N$, isomorphe à $\mathbb{U}_2$ si l'on considère l'action de $\mathrm{Gal}_K N$ sur $\{u, -u\}$. Alors l'extension F de K sera galoisienne. Il faudra de plus que l'action de $\mathbb{U}_2$ sur $\mathrm{Gal}_N F$ soit isomorphe à celle de $\mathbb{U}_2$ sur A dans le groupe diédral D_A. Celles que nous avons obtenues dans la section IV.4 n'ont pas a priori ces qualités. (A posteriori non plus d'ailleurs...)

Une extension abélienne $F \subset k((u))$ sur $k(u)$ se transporte très bien par compositum sur $L = k(\mathbb{U}_n, u)$ en une extension abélienne $E = F.L$ de même groupe. Là, en utilisant la théorie de Kummer, on associe l'extension n-abélienne E/L à un sous-groupe fini B/L^{*n} de L^*/L^{*n}. Il s'agit maintenant de construire un groupe B qui possède les propriétés que nous désirons donner à l'extension E/L, puis par "rétraction", à l'extension F/N.

Reprenons encore une fois la stratégie utilisée jusqu'à présent. Décomposons A en somme directe de groupes cycliques

$$A = \bigoplus_{j \in J} \mathbb{Z}/n_j\mathbb{Z}$$

Soit Γ le groupe des automorphismes de $l = k(\mathbb{U}_n)$ sur k où n est l'exposant de A. Un élément $\gamma \in \Gamma$ opère sur les racines n-ièmes de l'unité par élévation à la puissance $i(\gamma)$ appartenant à $\mathrm{U}(\mathbb{Z}/n\mathbb{Z})$.

$$\gamma(w) = w^{i(\gamma)} \qquad \gamma \in \Gamma,\ w \in \mathbb{U}_n$$

Soit x_j un élément primitif de $l_j = k(\mathbb{U}_{n_j})$ sur k. Nous noterons Γ_j le groupe des k-automorphismes de l_j. Considérons le polynôme de $l_j[t]$

$$d_j = \prod_{\gamma \in \Gamma_j} \big(1 + \gamma(x)u\big)^{\left\langle i(\gamma^{-1})\right\rangle_j} \big(1 - \gamma(x)u\big)^{\left\langle -i(\gamma^{-1})\right\rangle_j}$$

où les crochets $\langle\lambda\rangle_j$ représente un relevé dans $\{0,\dots,n_j-1\}$ de $\lambda \mod n_j$. Nous verrons dans la section IV.8 (page 144) pourquoi nous imposons un tel d_j.

Comme nous l'avons déjà précisé dans la section IV.3, plus que la valeur de d_j, c'est sa classe dans L^*/L^{*n_j} qui est importante.

$$d_j \equiv \prod_{\gamma\in\Gamma_j} \gamma(y)^{i(\gamma^{-1})} \mod L^{*n_j} \qquad \text{avec} \qquad y=\frac{1+xu}{1-xu}$$

Ces d_j sont de la même espèce que le d qui nous a servi pour réaliser les groupes cycliques : en quelque sorte, nous avons simplement remplacé le terme $y=1+xt$ de la page 108 par $y=\frac{1+xu}{1-xu}$.

Nous notons comme d'habitude e_j la racine n_j-ième de d_j

$$e_j=(d'_j)^{\frac{1}{n}} \qquad\qquad d'_j=(d_j)^{\frac{n}{n_j}}$$

Nous supposons à présent que les $(x_j)_{j\in J}$ sont choisis dans les corps $(l_j)_{j\in J}$ de telle sorte que **les éléments de la liste** $\big(\gamma(x_j),\ -\gamma(x_j)\ \mid j\in J,\gamma\in\Gamma\big)$ **soient tous distincts**.

Le lecteur pourra vérifier (de la même manière que nous l'avons fait dans les sections IV.3 et IV.4) que chaque d'_j engendre dans L^*/L^{*n} un groupe d'ordre n_j et que le groupe engendré par tous les d'_j dans L^*/L^{*n} est isomorphe à A.

Nous laissons toujours aux soins du lecteur de constater que E est une extension galoisienne de N de groupe isomorphe à $A\times\Gamma$ (E est stable sous l'action de Γ et Γ commute à $\mathrm{Gal}_L E\simeq A$).

Ensuite, l'extension $F=E^\Gamma$ est une extension abélienne de N de groupe de Galois isomorphe à A. Nous en connaissons en particulier un élément primitif

$$r=\sum_{j\in J} r_j \qquad \text{avec} \qquad r_j=\sum_{y\in\Gamma.e_j} y$$

Plus conceptuellement, nous savons que F est le compositum d'extensions cycliques $N(r_j)=L(e_j)^\Gamma$ où $j\in J$, linéairement disjointes "dans leur ensemble" sur N car modulo L^{*n}, les $(e_j^n)_j$ engendrent des groupes en produit direct.

Vérifions enfin que le corps F est bien galoisien sur K et que son groupe de Galois est bien le groupe diédral D_A. Pour cela, nommons τ le K-automorphisme de N échangeant u et $-u$ (i.e. $\mathrm{Gal}_K N=\{\tau,\mathrm{Id}\}$). Cet automorphisme τ se prolonge canoniquement en un automorphisme de $l((u))$. Nous avons par exemple pour tout $j\in J$

$$\begin{aligned}
\tau(d_j) &\equiv \prod_{\gamma\in\Gamma_j}\left(\frac{1+\gamma(x)\tau(u)}{1-\gamma(x)\tau(u)}\right)^{i(\gamma^{-1})} \mod L^{*n_j}\\
&\equiv \prod_{\gamma\in\Gamma_j}\left(\frac{1-\gamma(x)u}{1+\gamma(x)u}\right)^{i(\gamma^{-1})} \mod L^{*n_j}\\
&\equiv d_j^{-1} \mod L^{*n_j}
\end{aligned}$$

Remarque. Regardons uniquement la première ligne de ce calcul : si Γ_j est réduit à $\{\mathrm{Id}\}$ (i.e. $k = k(\mathbb{U}_{n_j})$), alors le polynôme $\tau(d_j)$ est différent de d_j dans $l[t]$, sauf pour $n_j = 2$. En revanche, si Γ_j n'est pas réduit à $\{\mathrm{Id}\}$, alors il existe $\gamma_0 \in \Gamma_j$ tel que $i(\gamma_0) = -1$, et par suite, nous obtenons $\tau(d_j) = \gamma_0(d_j)$. Cet automorphisme γ_0 correspond à l'automorphisme de conjugaison complexe.

On voit alors

$$\tau(d_j) \in d_j^{-1} L^{*n_j}, \qquad \text{puis} \qquad \tau(e_j) \in e_j^{-1} L^*$$

Ainsi il est clair que $L(e_j)$ est stable sous l'action de τ. Soit $g \in \mathrm{Gal}_L L(e_j)$. Constatons l'action de τ sur g :

$$\begin{aligned} \tau \circ g \circ \tau^{-1}(e_j) &= \tau \circ g(e_j^{-1} q_j) && \text{avec } q_j \in L^* \\ &= \tau\big((w_j(g) e_j)^{-1} q_j\big) && \text{où } w_j(g) = \frac{g(e_j)}{e_j} \in \mathbb{U}_{n_j} \\ &= w_j(g)^{-1} e_j = w_j(g^{-1}) e_j = g^{-1}.e_j \end{aligned}$$

Par ce petit calcul, nous confirmons que l'action de τ sur $\mathrm{Gal}_L L(e_j)$ est bien l'action diédrale.

Comme le groupe de Galois A de E/L est le produit direct des groupes de Galois de $L(e_j)/L$ pour $j \in J$, l'action de τ sur A est bien l'action diédrale.

D'autre part, $F = E^\Gamma = E \cap k((u))$ est stable par l'action de τ puisque E et $k((u))$ le sont. Cette extension abélienne F/N est finalement convenable : F est galoisienne sur K, l'homomorphisme τ est un K-automorphisme de F, et enfin $\mathrm{Gal}_K F \simeq A \rtimes \langle\tau\rangle = D_A$.

Théorème IV.5.1 *Soit k un corps de caractéristique étrangère à $2n$, l/k l'extension abélienne engendrée par les racines n-ièmes de l'unité dont le groupe de Galois est noté Γ. On se fixe des entiers n_j dont le p.p.c.m. est exactement n, des éléments primitifs $(x_j)_{j\in J}$ de $k(\mathbb{U}_{n_j})/k$ tels que les termes de la liste $\big(\gamma(x_j),\ -\gamma(x_j) \ \mid j \in J, \gamma \in \Gamma\big)$ soient tous distincts. Enfin considérons les éléments d_j, e_j, puis r_j et r, appartenant respectivement à $l(t^{\frac12})$, $l((t^{\frac12}))$ et $k((t^{\frac12}))$, définis par*

$$d_j = \prod_{\substack{\gamma\in\Gamma_j \\ \epsilon=\pm1}} \big(1 + \epsilon\ \gamma(x_j)\ t^{\frac12}\big)^{\langle \epsilon\ i(\gamma^{-1})\rangle_j} \qquad e_j = d_j^{\frac{1}{n_j}} \qquad r_j = \sum_{\gamma\in\Gamma_j} \gamma(e_j) \qquad r = \sum_{j\in J} r_j$$

où $\Gamma_j = \mathrm{Gal}_k k(\mathbb{U}_{n_j})$.

Alors $F = k(t^{\frac12}, r)$ est une extension galoisienne de $k(t)$, incluse dans $k((t^{\frac12}))$, dont le groupe de Galois est le groupe diédral D_A du groupe abélien $A \simeq \oplus_j \mathbb{Z}/n_j\mathbb{Z}$. En particulier, l'extension $F/k(t^{\frac12})$ est abélienne de groupe de Galois A.

Corollaire IV.5.1 *En particulier, pour $n > 2$ (correspondant au cas où $\mathbb{U}_2$ n'est pas distingué dans $D_A \simeq A \rtimes \mathbb{U}_2$), et $k = \mathbb{Q}$, alors r appartient à $\mathbb{Q}[[t]]$. Son polynôme minimal sur $\mathbb{Q}(t^{\frac12})$ est à coefficients dans $\mathbb{Q}[t]$ et de degré $|A|$. C'est un polynôme régulier sur $\mathbb{Q}$, réalisant le groupe diédral D_A sur $\mathbb{Q}(t)$. Son corps de décomposition est contenu dans le corps des séries formelles $\mathbb{Q}((t^{\frac12}))$.*

Démonstration Nous savons que r appartient à $\mathbb{Q}[[t^{\frac{1}{2}}]]$ grâce au théorème IV.5.1. Nous allons montrer que r est invariant par le groupe $\{\tau, \mathrm{Id}\} = \mathrm{Gal}_K N$ en posant $K = \mathbb{Q}(t)$ et $N = \mathbb{Q}(t^{\frac{1}{2}})$.

Grâce à la remarque faite page 124, en reprenant les mêmes notations, nous voyons que pour chaque d_j, l'automorphisme τ envoie d_j sur un de ses Γ_j-conjugués, car $\mathbb{Q}$ ne contient pas de racines de l'unité autre que 1 et -1. Ainsi la Γ_j-orbite de d_j, est globalement invariante par τ. Par suite, il en est de même pour la Γ_j-orbite de $e_j = d_j^{\frac{1}{n_j}}$. Par conséquent, l'élément $r_j = \sum_{\gamma \in \Gamma_j} \gamma(e_j)$ est invariant par τ. Pour tout j, nous voyons bien que r_j appartient à $\mathbb{Q}[[t]] = \mathbb{Q}[[t^{\frac{1}{2}}]]^{\langle \tau \rangle}$. Finalement, r appartient à $\mathbb{Q}[[t]]$.

Enfin, $\mathbb{Q}((t))$ et N sont linéairement disjointes sur K, si bien que le polynôme minimal de r sur K reste irréductible sur N. Les coefficients du polynôme minimal de r sur N appartiennent donc à $K = \mathbb{Q}(t)$, plus précisément à $\mathbb{Q}[t]$ car r est entier sur $\mathbb{Q}[t]$.

Le corps de décomposition du polynôme minimal de r est bien F : en effet, $K(r)$ est égal à $F^{\mathbb{U}_2}$ et la clôture galoisienne dans F de l'extension $K(r)/K$ est F^H où H est le plus gros sous-groupe de $\mathbb{U}_2$ distingué dans $D_A = \mathrm{Gal}_K F$, c'est-à-dire l'intersection des conjugués de $\mathbb{U}_2$ dans D_A. Comme $\mathbb{U}_2$ n'est pas normal dans D_A, le sous-groupe H est obligatoirement réduit à $\{\mathrm{Id}\}$. □

IV.5.b Résultats numériques sur $\mathbb{Q}$

Groupe diédral d'un groupe cyclique

Il suffit maintenant de mettre en œuvre le théorème IV.5.1 en machine pour obtenir une série de polynômes g_n réalisant régulièrement le groupe diédral $D_n = \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{U}_2$. Nous avons mené les calculs sur le corps $\mathbb{Q}$ pour ne pas avoir de difficulté liée à la caractéristique. Dans ces conditions, nous pouvons également utiliser le corollaire IV.5.1. Nous avons besoin d'un élément primitif x de $\mathbb{Q}(\mathbb{U}_n)/\mathbb{Q}$ tel que ses conjugués ne soient pas opposés les uns aux autres.

Propriété IV.5.1 *Pour un entier $n \in \mathbb{N}^*$ fixé, il y a équivalence entre les deux assertions suivantes :*

1) n est divisible par 4

2) si ϵ est une racine primitive n-ième de l'unité alors $-\epsilon$ l'est également.

Ainsi, lorsque n n'est pas divisible par 4, nous avons choisi tout simplement une racine primitive n-ième de l'unité ϵ comme élément primitif x de l'extension cyclotomique $\mathbb{Q}(\mathbb{U}_n)$ de $\mathbb{Q}$.

Lorsque n est divisible par 4, nous avons choisi $\epsilon + 1$ comme élément primitif x de l'extension cyclotomique $\mathbb{Q}(\mathbb{U}_n)/\mathbb{Q}$, afin de certifier que des conjugués de x et de $-x$ ne soient pas égaux.

Le lecteur remarquera que les polynômes obtenus sont des polynômes d'Eisenstein pour le premier $\prod_{\gamma \in \Gamma} (1 - \gamma(x)^2 t)$ de $\mathbb{Z}[t]$ où $\Gamma = \mathrm{Gal}_{\mathbb{Q}} \mathbb{Q}(\mathbb{U}_n) \simeq \mathrm{U}(\mathbb{Z}/n\mathbb{Z})$. La preuve de ce phénomène est identique à celle donnée après le théorème IV.3.1, page 110.

$$g_3 = X^3 - 3\,p\,X + 2\,(t-1)\,p$$
avec
$p = t^2 + t + 1$

$$g_4 = X^4 - 4\,p\,X^2 + 16\,t\,p$$
avec
$p = 4\,t^2 + 1$

$$g_5 = X^5 - 10\,p\,X^3 - 20\,(t-1)^2\,p\,X^2 - 5\,p\,(3\,t^4 - 17\,t^3 + 3\,t^2 - 17\,t + 3)\,X$$
$$-4\,(t-1)^2\,(t^4 - 9\,t^3 - 9\,t^2 - 9\,t + 1)\,p$$
avec
$p = t^4 + t^3 + t^2 + t + 1$

$$g_6 = X^6 - 6\,p\,X^4 + 9\,p^2\,X^2 - 4\,(t^2 - 5\,t + 1)^2\,p$$
avec
$p = t^2 + t + 1$

$$g_7 = X^7 - 21\,p\,X^5 + 70\,(t-1)^3\,p\,X^4$$
$$-7\,p\,(15\,t^6 - 125\,t^5 + 183\,t^4 - 293\,t^3 + 183\,t^2 - 125\,t + 15)\,X^3$$
$$+28\,(t-1)^3\,p\,(3\,t^6 - 39\,t^5 + 31\,t^4 - 39\,t^3 + 31\,t^2 - 39\,t + 3)\,X^2$$
$$-7\,p\,(5\,t^{12} - 130\,t^{11} + 827\,t^{10} - 2724\,t^9 + 6857\,t^8 - 8958\,t^7 + 10647\,t^6$$
$$-8958\,t^5 + 6857\,t^4 - 2724\,t^3 + 827\,t^2 - 130\,t + 5)\,X$$
$$+2\,(t-1)^3\,p\,(3\,t^{12} - 106\,t^{11} + 905\,t^{10} - 4748\,t^9 + 18999\,t^8 - 21878\,t^7$$
$$+29085\,t^6 - 21878\,t^5 + 18999\,t^4 - 4748\,t^3 + 905\,t^2 - 106\,t + 3)$$
avec
$p = t^6 + t^5 + t^4 + t^3 + t^2 + t + 1$

$$g_8 = X^8 - 16\,p\,X^6 + 256\,t\,(9\,t^2 - 7\,t + 2)\,p\,X^4$$
$$-4096\,t^2\,(2\,t-1)^2\,(6\,t^2 - 2\,t + 1)\,p\,X^2 + 65536\,t^5\,(2\,t-1)^4\,p$$
avec
$p = 4\,t^4 + 8\,t^3 + 8\,t^2 - 4\,t + 1$

$$g_9 = X^9 - 27\,p\,X^7 + 54\,(t-1)\,(t^2 - 3\,t + 1)\,p\,X^6 + 1944\,(t-1)^2\,t\,(t^2 - t + 1)\,p\,X^5$$
$$-3888\,(t-1)^3\,t\,(t^4 - 3\,t^3 + 3\,t^2 - 3\,t + 1)\,p\,X^4$$
$$-1296\,(t-1)^4\,t^2\,(33\,t^4 - 59\,t^3 + 79\,t^2 - 59\,t + 33)\,p\,X^3$$
$$+69984\,(t-1)^5\,t^2\,(t^2 - t + 1)\,(t^4 - 3\,t^3 + 3\,t^2 - 3\,t + 1)\,p\,X^2$$
$$+46656\,(t-1)^8\,t^3\,(2\,t^2 - t + 2)\,(3\,t^2 - t + 3)\,p\,X$$
$$+31104\,(t-1)^9\,t^4\,(3\,t^2 - t + 3)^2\,p$$
avec
$p = t^6 + t^3 + 1$

$$
\begin{aligned}
g_{10} = \; & X^{10} - 20\,p\,X^8 + 10\,p\,(7\,t^4 + 47\,t^3 - 73\,t^2 + 47\,t + 7)\,X^6 \\
& -100\,p\,(t^8 + 2\,t^7 + 23\,t^6 - 76\,t^5 + 125\,t^4 - 76\,t^3 + 23\,t^2 + 2\,t + 1)\,X^4 \\
& +5\,p\,(13\,t^{12} - 201\,t^{11} + 238\,t^{10} + 9250\,t^9 - 44125\,t^8 + 92874\,t^7 \\
& \qquad -114473\,t^6 + 92874\,t^5 - 44125\,t^4 + 9250\,t^3 + 238\,t^2 - 201\,t + 13)\,X^2 \\
& -16\,p\,(t^8 - 23\,t^7 + 158\,t^6 - 366\,t^5 + 435\,t^4 - 366\,t^3 + 158\,t^2 - 23\,t + 1)^2 \\
& \text{avec} \\
& p = t^4 + t^3 + t^2 + t + 1
\end{aligned}
$$

g_{11} énorme...

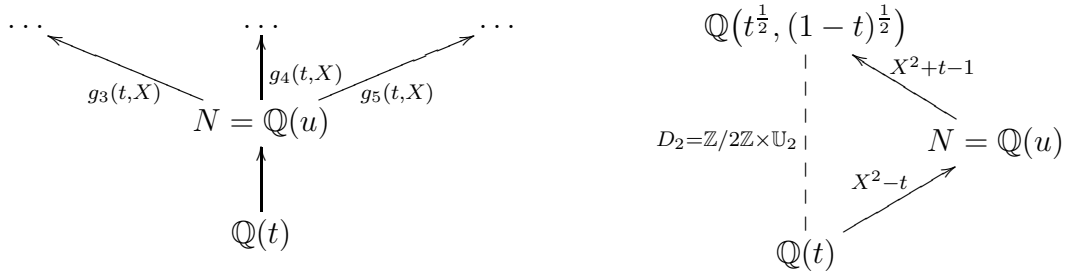
$$
\begin{aligned}
g_{12} = \; & X^{12} - 24\,p\,X^{10} + 144\,p\,(t^4 + 14\,t^3 + 3\,t^2 - 4\,t + 1)\,X^8 \\
& -128\,p\,(2\,t^8 + 84\,t^7 + 680\,t^6 + 129\,t^5 - 984\,t^4 + 555\,t^3 - 94\,t^2 - 3\,t + 2)\,X^6 \\
& +768\,t\,(2\,t-1)^2\,p\,(8\,t^8 + 44\,t^7 + 876\,t^6 - 633\,t^5 + 494\,t^4 \\
& \qquad -627\,t^3 + 354\,t^2 - 85\,t + 8)\,X^4 \\
& -36864\,t^2\,(2\,t-1)^4\,(t^2 - 3\,t + 1)^2\,p^2\,X^2 + 65536\,t^3\,(2\,t-1)^6\,(t^2 - 3\,t + 1)^4\,p \\
& \text{avec} \\
& p = t^4 + 6\,t^3 + 11\,t^2 - 6\,t + 1
\end{aligned}
$$

$\vdots$

Groupe diédral $D(A)$ d'un groupe abélien fini A

Voici à présent des polynômes obtenus par le théorème IV.5.1 réalisant le groupe diédral d'un groupe abélien fini quelconque.

Nous avons mené les calculs sur $\mathbb{Q}$ à la fois pour des raisons de caractéristique, mais aussi de liberté dans le choix des générateurs de $\mathbb{Q}(\mathbb{U}_n)$. Nous utilisons les polynômes g_i calculés dans le paragraphe ci-dessus. Ceux-ci réalisent (régulièrement) les groupes diédraux $D_i = D(\mathbb{Z}/i\mathbb{Z})$ sur $\mathbb{Q}(t)$, mais aussi $\mathbb{Z}/i\mathbb{Z}$ sur $N = \mathbb{Q}(u)$ avec $u = t^{\frac{1}{2}}$.



Si nous ajoutons à cette liste le polynôme $g_2 = X^2 + t - 1 = X^2 + u^2 - 1$ qui réalise régulièrement $\mathbb{Z}/2\mathbb{Z}$ sur N, nous sommes capables, par simple "composition" des g_i, de construire tout groupe abélien A sur N, puis son groupe diédral D_A sur $\mathbb{Q}(t)$ si l'exposant de A est strictement supérieur à 2. En effet, les corps de décomposition des polynômes g_i sur N sont linéairement disjoints "dans leur ensemble". Nous agissons par conséquent de façon similaire à la section IV.4.b.

Remarque. Si l'exposant de A est 2, alors l'action "diédrale" de $\mathbb{U}_2$ sur A est triviale,

si bien que le groupe $D(A) = A \rtimes \mathbb{U}_2 = A \times \mathbb{U}_2$ est abélien. La réalisation d'un tel groupe est traitée dans la section IV.4.

$D(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z})$: $X^8 - 4\,(8\,t^2 - t + 3)\,X^6 + 2\,(128\,t^4 + 48\,t^3 + 83\,t^2 + 6\,t + 15)\,X^4$
$-4\,(384\,t^5 + 312\,t^4 + 15\,t^3 + 105\,t^2 - 23\,t + 7)\,X^2$
$+(80\,t^3 - 15\,t^2 + 18\,t - 3)^2$
en choisissant $g_2(u^2, X)$ et $g_4(u^2, X)$ avec $u^2 = t$.

$D\big((\mathbb{Z}/3\mathbb{Z})^2\big)$: $X^9 - 9\,(17\,t^2 + 5\,t + 2)\,X^7 + 6\,(65\,t^3 - 2)\,X^6$
$+81\,(91\,t^4 + 50\,t^3 + 24\,t^2 + 5\,t + 1)\,X^5$
$-18\,(1970\,t^5 + 446\,t^4 + 65\,t^3 - 17\,t^2 - 5\,t - 2)\,X^4$
$-3\,(24725\,t^6 + 31455\,t^5 + 18279\,t^4 + 4865\,t^3 + 1674\,t^2 + 270\,t + 56)\,X^3$
$+486\,t^2\,(5\,t + 1)^2\,(65\,t^3 - 2)\,X^2$
$-9\,(192500\,t^8 - 22000\,t^7 - 76921\,t^6 - 31255\,t^5$
$-7444\,t^4 - 175\,t^3 - 217\,t^2 - 40\,t - 16)\,X$
$+2\,(612500\,t^9 - 607500\,t^8 - 579555\,t^7 - 172599\,t^6 + 55890\,t^5$
$+28431\,t^4 + 9195\,t^3 + 486\,t^2 - 32)$
en choisissant $g_3(u^2, X)$ et $g_3((2u)^2, X)$ avec $u^2 = t$.

$D(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z})$: $X^{12} - 6(2\,t^2 + t + 3)\,X^{10} + 3\,(18\,t^4 + 24\,t^3 + 59\,t^2 + 26\,t + 35)\,X^8$
$-4\,(29\,t^6 + 45\,t^5 + 186\,t^4 + 174\,t^3 + 231\,t^2 + 60\,t + 58)\,X^6$
$+3\,(43\,t^8 - 16\,t^7 - 30\,t^6 + 1668\,t^5$
$+714\,t^4 + 1128\,t^3 - 520\,t^2 + 448\,t + 48)\,X^4$
$-6\,t\,(12\,t^9 - 63\,t^8 - 475\,t^7 + 668\,t^6 + 1682\,t^5$
$+1408\,t^4 + 100\,t^3 - 656\,t^2 + 48\,t + 192)\,X^2$
$+t^2\,(4\,t^5 - 27\,t^4 + 87\,t^3 + 32\,t^2 + 60\,t - 48)^2$
en choisissant $g_2(u^2, X)$ et $g_6(u^2, X)$ avec $u^2 = t$.

$D\big((\mathbb{Z}/4\mathbb{Z})^2\big)$: un peu trop volumineux...
en choisissant $g_4(u^2, X)$ et $g_4((2u)^2, X)$ avec $u^2 = t$.

$D\big((\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/4\mathbb{Z}\big)$: un peu trop volumineux...
en choisissant $g_2(u^2, X)$, $g_2((2u)^2, X)$ et $g_4(u^2, X)$ avec $u^2 = t$.

$D(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z})$: nettement trop volumineux...
en choisissant $g_2(u^2, X)$ et $g_8(u^2, X)$ avec $u^2 = t$.

$\vdots$

IV.5.c Autres produits semi-directs $\mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{U}_2$

Dans la section IV.3.c, pour n multiple de 4, le polynôme $f_n \in \mathbb{Q}[t, X]$, réalisant régulièrement le groupe cyclique $\mathbb{Z}/n\mathbb{Z}$, est un polynôme en t^2. Ceci vient du fait que, pour n multiple de 4, si $x = \epsilon$ est une racine primitive n-ième de l'unité, alors $-\epsilon$ l'est également.

Ainsi, le polynôme $f_n(t^{\frac{1}{2}}, X) \in \mathbb{Q}[t, X]$ (régulier sur $\mathbb{Q}$) possède un groupe de Galois sur $\mathbb{Q}(t)$ d'ordre $2n$. Plus précisément, son groupe de Galois est un produit semi-direct $\mathbb{Z}/n\mathbb{Z} \rtimes \{\mathrm{Id}, \tau\}$ où $\{\mathrm{Id}, \tau\} = \mathrm{Gal}_{\mathbb{Q}(t)}\, \mathbb{Q}(t^{\frac{1}{2}})$. On pourrait s'attendre à rencontrer le groupe diédral. Mais il n'en n'est rien. En effet, l'action de τ sur $\mathbb{Z}/n\mathbb{Z}$ n'est pas l'action "diédrale". En reprenant les notations de la section IV.3, d'une part,

$$\tau(d) = \gamma(d)$$

où γ désigne l'automorphisme de l'extension $\mathbb{Q}(\mathbb{U}_n)/\mathbb{Q}$ donné par $\epsilon \mapsto -\epsilon$ où ϵ est une racine primitive n-ième de l'unité quelconque. D'autre part, pour $g \in \mathrm{Gal}_L\, L(e)$,

$$\tau g \tau^{-1}(e) = \tau g \gamma(e) = \tau(w(g)^{i(\gamma)} \gamma e) = w(g)^{i(\gamma)} e = g^{i(\gamma)}.e$$

Or $i(\gamma) \equiv \frac{n}{2} + 1 \mod n$, si bien que

$$\tau.g = g^{\frac{n}{2}+1}$$

L'action de τ sur g n'est pas l'action "diédrale" (sauf pour $n = 4$). Pour les entiers n congrus à $0 \mod 4$, nous récupérons donc quelques réalisations régulières sur $\mathbb{Q}$ de groupes formés par le produit semi-direct $\mathbb{Z}/n\mathbb{Z} \rtimes \langle j \rangle \subset \mathbb{Z}/n\mathbb{Z} \rtimes \mathrm{U}(\mathbb{Z}/n\mathbb{Z})$, où l'action de j sur $\mathbb{Z}/n\mathbb{Z}$ est la multiplication par l'élément j de $\mathrm{U}(\mathbb{Z}/n\mathbb{Z})$:

$$\mathbb{Z}/4\mathbb{Z} \rtimes \langle -1 \rangle = D_4 \ : \ X^4 - 4\ p\ X^2 + 4\ t\ p$$
avec
$$p = t + 1$$

$$\mathbb{Z}/8\mathbb{Z} \rtimes \langle -3 \rangle \ : \ X^8 - 16\ p\ X^6 + 32\ t\ (t+4)\ p\ X^4 - 256\ t^2\ (t+1)p\ X^2 + 256\ t^4 p$$
avec
$$p = t^2 + 1$$

$$\begin{aligned}\mathbb{Z}/12\mathbb{Z} \rtimes \langle -5 \rangle \ : \ & X^{12} - 24\ p\ X^{10} + 72\ p\ (2\ t^2 - t + 2)\ X^8 \\ & -16\ p\ (4\ t^4 + 31\ t^3 - 6\ t^2 + 10\ t + 16)\ X^6 \\ & +48\ t\ p\ (8\ t^4 - 17\ t^3 + 61\ t^2 - 53\ t + 32)\ X^4 \\ & -576\ t^2\ (t-2)^2\ p^2\ X^2 + 64\ t^3\ (t-2)^4\ p \\ & \text{avec} \\ & p = t^2 - t + 1\end{aligned}$$

$\vdots$

Nous pouvons en fait très facilement réaliser tous les produits semi-directs $\mathbb{Z}/n\mathbb{Z} \rtimes \langle j \rangle$ où j est un élément d'ordre 2 dans $\mathrm{U}(\mathbb{Z}/n\mathbb{Z})$. En reprenant les notations de la section IV.5.a, il suffit de choisir

$$d \equiv \prod_{\gamma \in \Gamma} \left(1 + \gamma(x) t^{\frac{1}{2}}\right)^{i(\gamma^{-1})} \left(1 - \gamma(x) t^{\frac{1}{2}}\right)^{ji(\gamma^{-1})} \qquad \mod\ L^{*n}$$

On prouve aisément, comme nous l'avons fait pour le groupe diédral, que l'action de $\tau\ :\ t^{\frac{1}{2}} \mapsto -t^{\frac{1}{2}}$ sur le groupe de Galois de l'extension $L(d^{\frac{1}{n}})/L$ est isomorphe à l'action de multiplication par j dans $\mathbb{Z}/n\mathbb{Z}$:

$$\tau(d) \in d^j L^{*n} \qquad\qquad \tau g \tau^{-1} = g^j \qquad \forall\ g \in \mathrm{Gal}_L\, L(d^{\frac{1}{n}})$$

Rappel. Lorsque n est divisible par 4, nous choisissons $\epsilon{+}1$ comme élément primitif x de l'extension cyclotomique $\mathbb{Q}(\mathbb{U}_n)/\mathbb{Q}$, afin de certifier que des conjugués de x et de $-x$ ne soient pas égaux.

$\mathbb{Z}/8\mathbb{Z} \rtimes \langle 3 \rangle$:
$$X^8 - 16\ p\ X^6 + 256\ t^2\ (t^2 + t + 2)\ p\ X^4 - 4096\ t^4\ (2\ t^2 + 2\ t + 1)\ p\ X^2 + 65536\ t^7\ p$$
avec
$$p = 4\ t^4 + 8\ t^3 + 8\ t^2 - 4\ t + 1$$

$\mathbb{Z}/12\mathbb{Z} \rtimes \langle 5 \rangle$:
$$\begin{aligned} &X^{12} - 24\ p\ X^{10} + 144\ p\ (t^4 + 6\ t^3 + 13\ t^2 - 6\ t + 1)\ X^8 \\ &-128\ p\ (2\ t^8 - 7\ t^6 + 174\ t^5 + 477\ t^4 - 390\ t^3 + 137\ t^2 - 24\ t + 2)\ X^6 \\ &+768\ t^2\ p\ (8\ t^8 - 101\ t^6 + 162\ t^5 \\ &\qquad +1105\ t^4 - 1122\ t^3 + 475\ t^2 - 96\ t + 8)\ X^4 \\ &-36864\ t^4\ (t^2 - 3\ t + 1)^2\ p^2\ X^2 + 65536\ t^6\ (t^2 - 3\ t + 1)^4\ p \end{aligned}$$
avec
$$p = t^4 + 6\ t^3 + 11\ t^2 - 6\ t + 1$$

$\vdots$

IV.6 Rappels élémentaires sur les G-modules

Définition IV.6.1 *Soit G un groupe opérant sur un groupe abélien M. Ce groupe M est alors muni d'une structure de $\mathbb{Z}[G]$-module où $\mathbb{Z}[G]$ est l'algèbre du groupe G sur $\mathbb{Z}$. Nous dirons alors que M est un G-**module**.*

L'algèbre $\mathbb{Z}[G]$ est bien sûr un G-module où l'opération de G est la multiplication à gauche.

Notation : Dans ce qui suit, un groupe abélien M pourra être considéré parfois comme étant muni d'une structure de G-module et parfois sans cette structure. Afin de ne faire aucune imprécision, nous porterons un indice sur M de tel sorte que M_0 représentera M vu comme **groupe abélien "nu"** et M_ρ un **G-module** où l'opération de G sur M est donnée par le morphisme $\rho : G \to \mathrm{Aut}(M)$. (En fait, M_0 est un G-module où l'action de G sur M est triviale.)

Convention : Lorsque M_ρ et $M'_{\rho'}$ sont deux G-modules, le groupe des $\mathbb{Z}$-homomorphismes de M_ρ dans $M'_{\rho'}$, noté $\mathrm{Hom}_{\mathbb{Z}}(M_\rho, M'_{\rho'})$, est canoniquement muni d'une structure de G-module par

$$\begin{array}{rccc} G \ni g \ : & \mathrm{Hom}_{\mathbb{Z}}(M_\rho, M'_{\rho'}) & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}}(M_\rho, M'_{\rho'}) \\ & f & \longmapsto & \rho'(g) \circ f \circ \rho(g^{-1}) \end{array}$$

De même, leur produit tensoriel $M_\rho \otimes_{\mathbb{Z}} M'_{\rho'}$ est muni canoniquement de la structure de G-module suivante :

$$\begin{array}{rccc} G \ni g \ : & M_\rho \otimes_{\mathbb{Z}} M'_{\rho'} & \longrightarrow & M_\rho \otimes_{\mathbb{Z}} M'_{\rho'} \\ & m \otimes m' & \longmapsto & \rho(g).m \otimes \rho'(g).m' \end{array}$$

Par exemple, si nous désirons travailler avec ce produit tensoriel démuni de structure de G-module, nous le noterons $M_0 \otimes_{\mathbb{Z}} M'_0$. L'action de G sur le module $M_\rho \otimes_{\mathbb{Z}} M'_0$ sera triviale à droite et non à gauche.

Enfin pour ne pas surcharger les notations, nous éviterons dans la mesure du possible d'écrire $\rho(g) \circ f$ ou $\rho(g).m$. Nous utiliserons la notation $g \circ f$ et $g.m$ si cela ne peut créer de confusion.

Rappel : si A, B et C sont trois modules, alors les trois modules suivants sont isomorphes :

$$\begin{array}{ccccc} \mathrm{Hom}_{\mathbb{Z}}(A, \mathrm{Hom}_{\mathbb{Z}}(B, C)) & \longleftrightarrow & \mathrm{Hom}_{\mathbb{Z}}(A \otimes_{\mathbb{Z}} B, C) & \longleftrightarrow & \mathrm{Hom}_{\mathbb{Z}}(B, \mathrm{Hom}(A, C)) \\ [a \mapsto f(a \otimes \bullet)] & \longleftarrow & f & \longmapsto & [b \mapsto f(\bullet \otimes b)] \end{array}$$

Ces isomorphismes de modules deviennent des G-isomorphismes lorsque A, B et C sont trois G-modules.

IV.6.a G-modules induits

Définition IV.6.2 *Un G-module M' sera dit **induit par** le groupe abélien M_0 s'il est isomorphe au G-module $\mathbb{Z}[G] \otimes_{\mathbb{Z}} M_0$. Il revient au même de dire que M' est égal à la somme directe $\bigoplus_{g \in G} g\ M_0$ de $|G|$ modules isomorphes à M_0.*

Cette définition est légèrement différente de la définition classique (voir [52], page 118). D'habitude, le groupe M_0 n'est pas précisé lorsque l'on désigne M' : "Soit M un G-module induit". Dans l'intention de contrôler les objets au cours des constructions successives, nous retiendrons le module de base M_0.

Propriété IV.6.1 (voir [52], page 118) *Si M_ρ est un G-module alors il existe un isomorphisme canonique de G-modules entre $\mathbb{Z}[G] \otimes_{\mathbb{Z}} M_0$ et $\mathbb{Z}[G] \otimes_{\mathbb{Z}} M_\rho$, à savoir :*

$$\begin{array}{ccc} \mathbb{Z}[G] \otimes_{\mathbb{Z}} M_0 & \overset{G}{\longleftrightarrow} & \mathbb{Z}[G] \otimes_{\mathbb{Z}} M_\rho \\ g \otimes a & \longmapsto & g \otimes g.a \end{array}$$

En particulier, le G-module M_ρ est un quotient canonique du G-module induit par M_0.

$$\begin{array}{ccc} \mathbb{Z}[G] \otimes_{\mathbb{Z}} M_0 & \overset{G}{\longrightarrow} & M_\rho \\ g \otimes a & \longmapsto & g.a \end{array} \qquad \begin{array}{ccc} \mathbb{Z}[G] \otimes_{\mathbb{Z}} M_\rho & \overset{G}{\longrightarrow} & M_\rho \\ g \otimes a & \longmapsto & a \end{array}$$

Grâce à cette propriété, si le besoin s'en fait sentir, nous pourrons considérer indifféremment l'un ou l'autre G-modules $\mathbb{Z}[G] \otimes_{\mathbb{Z}} M_0$ et $\mathbb{Z}[G] \otimes_{\mathbb{Z}} M_\rho$.

Remarque. Ouvrons une petite parenthèse sur le produit régulier en couronne.

Définition IV.6.3 (cf. [58], pages 268-270) *Deux groupes A, G étant donnés, le produit semi-direct $A^G \rtimes G$ où l'action de $g \in G$ sur A^G est simplement la permutation des coordonnées $g.(a_h)_{h\in G} = (a_{g^{-1}h})_{h\in G}$, est appelé* ***produit régulier en couronne*** *(wreath product), noté $A \wr G$.*

Si A est un groupe abélien, il faut remarquer que le produit en couronne $A \wr G$ n'est autre que le produit semi-direct par G provenant du G-module $A^G \overset{G}{\simeq} \mathbb{Z}[G] \otimes_{\mathbb{Z}} A_0$.

Lemme IV.6.1 (voir [58], page 275) *Soit ρ une action quelconque d'un groupe* ***fini*** *G sur un groupe* ***abélien*** *M. Il existe un épimorphisme du produit régulier en couronne $M_0 \wr G$ sur le groupe $M_\rho \rtimes G$, à savoir*

$$\begin{array}{ccc} M_0 \wr G & \longrightarrow & M_\rho \rtimes G \\ (m, g) & \longmapsto & \left(\displaystyle\sum_{g\in G} g.m_g \ , \ g \right) \end{array}$$

Cet épimorphisme est la traduction du morphisme surjectif de G-modules de la propriété IV.6.1 : quand G est de cardinal fini, les éléments de $\mathbb{Z}[G] \otimes_{\mathbb{Z}} M_0$ sont de la forme $\sum_{g\in G} g \otimes m_g$.

IV.6.b G-modules co-induits

Définition IV.6.4 *Un G-module M' est dit* ***co-induit par*** *le groupe abélien M_0 s'il est isomorphe au G-module $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], M_0)$.*

Propriété IV.6.2 *Si M_ρ est un G-module alors il existe un isomorphisme canonique de G-modules entre $\mathrm{Hom}(\mathbb{Z}[G], M_0)$ et $\mathrm{Hom}(\mathbb{Z}[G], M_\rho)$, à savoir :*

$$\begin{array}{ccc} \mathrm{Hom}(\mathbb{Z}[G], M_0) & \overset{G}{\longleftrightarrow} & \mathrm{Hom}(\mathbb{Z}[G], M_\rho) \\ f & \longmapsto & \big(g \mapsto g.\ f(g)\big) \end{array}$$

Le G-module M_ρ s'injecte canoniquement dans le G-module co-induit par M_0.

$$\begin{array}{ccc} M_\rho & \overset{G}{\longrightarrow} & \mathrm{Hom}(\mathbb{Z}[G], M_0) \\ a & \longmapsto & \big(g \mapsto \rho(g^{-1}).a\big) \end{array} \qquad\qquad i \ : \ \begin{array}{ccc} M_\rho & \overset{G}{\longrightarrow} & \mathrm{Hom}(\mathbb{Z}[G], M_\rho) \\ a & \longmapsto & (g \mapsto a) \end{array}$$

Si nous posons $A = \mathbb{Z}[G]$ et $B' = \mathbb{Z}[G] \otimes B_0$, nous obtenons des isomorphismes canoniques de G-modules :

$$\begin{array}{ccccc} \mathrm{Hom}\big(\mathbb{Z}[G] \otimes B_0, C\big) & \simeq & \mathrm{Hom}\big(B_0, \mathrm{Hom}(\mathbb{Z}[G], C)\big) & \simeq & \mathrm{Hom}\big(B_0, \mathrm{Hom}(\mathbb{Z}[G], C_0)\big) \\ & \simeq & \mathrm{Hom}\big(\mathbb{Z}[G] \otimes B_0, C_0\big) & \simeq & \mathrm{Hom}\big(\mathbb{Z}[G], \mathrm{Hom}(B_0, C_0)\big) \end{array}$$

Ainsi on voit clairement que si B' est induit par B_0, alors $\mathrm{Hom}(B', C)$ est co-induit par $\mathrm{Hom}(B_0, C_0)$ et $\mathrm{Hom}_{\mathbb{Z}}(B', C) \simeq \mathrm{Hom}(B', C_0)$.

Après ces brefs rappels, voici à présent les propriétés essentielles (mais toujours élémentaires) qui nous serviront dans les prochaines sections. Il s'agit de résultats classiques de cohomologie (voir [52], ou [38] page 827). Il est bien connu que tout G-module M co-induit possède une cohomologie nulle : $H^q(G, M) = (0)$ pour tout $q \geq 1$. Or $H^2(G, M)$ est le groupe des classes d'extensions de G par M (i.e. les suites exactes $1 \to M \to \bullet \to G \to 1$) dont l'élément neutre est la classe de l'extension

$$1 \longrightarrow M \longrightarrow M \rtimes G \longrightarrow G \longrightarrow 1$$

Si $H^2(G, M)$ est réduit à son élément neutre, alors une extension quelconque de G par M est nécessairement isomorphe à $1 \to M \to M \rtimes G \to G \to 1$. En une petite page, nous désirons simplement prouver ce résultat de façon concrète et sans faire appel à la théorie cohomologique.

Lemme IV.6.2 *Si M_ρ est un G-module co-induit alors il existe une rétraction canonique de G-modules de* $\mathrm{Hom}(\mathbb{Z}[G], M_\rho)$ *sur M_ρ. En posant $M_\rho = \mathrm{Hom}(\mathbb{Z}[G], M_0')$, ce morphisme s'exprime par*

$$\begin{array}{rccl} m \ : & \mathrm{Hom}(\mathbb{Z}[G], M_\rho) & \xrightarrow{G} & \mathrm{Hom}(\mathbb{Z}[G], M_0') = M_\rho \\ & f & \longmapsto & \big(g \mapsto f(g)(g)\big) \end{array}$$

Si i est l'injection canonique de M_ρ dans $\mathrm{Hom}(\mathbb{Z}[G], M_\rho)$ *donnée par*

$$i(x) = \big(g \mapsto x\big)$$

on voit que $m \circ i = \mathrm{Id}_{M_\rho}$. Une telle application m vérifiant $m \circ i = \mathrm{Id}_{M_\rho}$ est appelée ***G-morphisme moyenne***.

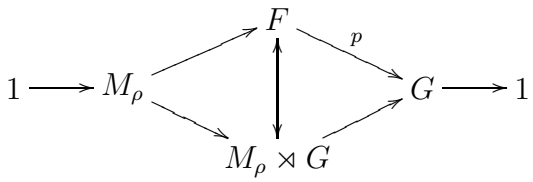
> Remarque. Si G est un groupe fini dont le cardinal est inversible dans un G-module M_ρ, alors il existe une application moyenne de $\mathrm{Hom}(\mathbb{Z}[G], M_\rho)$ sur M_ρ, sans que ce dernier soit supposé co-induit. Ce morphisme canonique est
>
> $$\begin{array}{rccl} m \ : & \mathrm{Hom}(\mathbb{Z}[G], M_\rho) & \xrightarrow{G} & M_\rho \\ & f & \longmapsto & \dfrac{1}{|G|} \displaystyle\sum_{g \in G} f(g) \end{array}$$
>
> Ici, le nom de "moyenne" prend tout son sens...

Propriété IV.6.3 (voir [12], page 190) *Soit une extension du groupe G par un groupe abélien M :*

$$1 \longrightarrow M \longrightarrow F \xrightarrow{p} G \longrightarrow 1$$

Alors G opère sur M par conjugaison intérieure à F. Notons ρ cette action. Si le G-module M_ρ provenant de cette extension possède une moyenne m, alors les deux extensions ci-dessous sont isomorphes.

Par suite, il existe une section pour p de G dans F.



Démonstration L'action de $g \in G$ sur M_ρ est donnée par

$$\begin{array}{rccc} g & : & M & \longrightarrow & M \\ & & y & \longmapsto & xyx^{-1} \end{array}$$

quel que soit l'antécédent x de g par la surjection p. L'élément xyx^{-1} appartient à M car M est distingué dans F, et le choix de l'antécédent x n'importe pas car M est abélien.

Soit $s : G \to F$ une section ensembliste : $s(g)$ est un antécédent de $g \in G$ par p. On a ainsi $p \circ s = \mathrm{Id}_M$ d'un point de vue ensembliste. Nous remarquons alors deux manières de calculer l'action de $p(x) \in G$ sur $y \in M$:

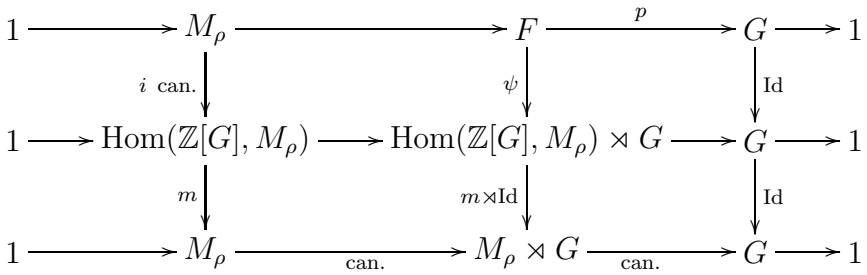
$$p(x).y = xyx^{-1} = \big(s \circ p(x)\big)\ y\ \big(s \circ p(x)\big)^{-1}$$

Pour $x \in F$, on considére l'application

$$\begin{array}{rccc} \phi_x & : & G & \longrightarrow & M_\rho \\ & & g & \longmapsto & x\ s\big(p(x^{-1})g\big)\ s(g)^{-1} \end{array}$$

Noter que $\phi_x(g)$ appartient bien à M_ρ car $p(\phi_x(g)) = p(x)p(x)^{-1}gg^{-1} = 1$. De plus, cette application ensembliste définit à son tour par $\mathbb{Z}$-linéarité un morphisme (que l'on notera encore $\phi_x \in \mathrm{Hom}(\mathbb{Z}[G], M_\rho)$) de $\mathbb{Z}[G]$ dans M, car G est une $\mathbb{Z}$-base de $\mathbb{Z}[G]$.

Considérons enfin ce diagramme de trois suites exactes de G-modules suivant :



où ψ est l'homomorphisme de groupes défini par $F \ni x \mapsto (\phi_x, p(x))$. Cette application est bien un morphisme de groupes car $\phi_{xy} = {}^{p(x)}\phi_y\ \phi_x = \phi_x\ {}^{p(x)}\phi_y$ pour tout $(x, y) \in F^2$.

Ce diagramme commutatif relie les première et troisième extensions. Or tout morphisme d'extensions est nécessairement bijectif. □

Corollaire IV.6.1 *Considérons l'extension de G par un groupe abélien M_0 :*

$$1 \longrightarrow M_0 \longrightarrow F \xrightarrow{p} G \longrightarrow 1$$

Si l'opération ρ de G sur M_0 déduite de cette suite exacte fait de M_ρ un G-module coinduit, alors p possède une section $s : G \to F$. En particulier, F est isomorphe à $M_\rho \rtimes G$.

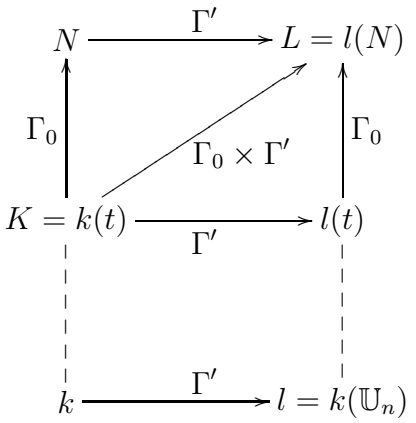
IV.7 Réalisation théorique des produits semi-directs à noyau abélien

La donnée du problème est un groupe fini Γ_0 et une extension galoisienne N de $k(t)$ régulière sur k dont le groupe de Galois est précisément Γ_0. De plus, une action quelconque ρ de Γ_0 sur un groupe abélien fini A est fixée une fois pour toutes. Nous allons voir comment réaliser le produit semi-direct $A_\rho \rtimes \Gamma_0$ sur $k(t)$ régulièrement sur le corps k. Plus précisément, nous voulons construire une extension E/N, galoisienne sur $k(t)$ de groupe de Galois $A_\rho \rtimes \Gamma_0$, avec la compatibilité suivante (*embedding problem*) :

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{Gal}_N E & \longrightarrow & \mathrm{Gal}_{k(t)} E & \longrightarrow & \mathrm{Gal}_{k(t)} N & \longrightarrow & 1 \\ & & \wr| & & \wr| & & \wr| & & \\ 1 & \longrightarrow & A & \longrightarrow & A_\rho \rtimes \Gamma & \longrightarrow & \Gamma & \longrightarrow & 1 \end{array}$$

Comme d'habitude, quitte à ajouter au corps de base certaines racines de l'unité, nous userons et abuserons de la théorie de Kummer pour assurer plus ou moins facilement quelques résultats, puis nous les "rétracterons" sur les scalaires de base pour obtenir ce que nous cherchons. A la différence des sections précédentes (réalisation régulière des groupes abéliens et diédraux), nous n'utiliserons pas le corps des séries formelles $k((t))$ car a priori Γ_0 n'est pas réalisé dans $k((t))$. Cela compliquera malheureusement la tâche quand il faudra prouver la régularité de nos extensions...

Introduisons le cadre de travail et les notations qui nous serviront tout au long de cette section. Soit k un corps dont la caractéristique est étrangère au cardinal de A, n l'exposant du groupe abélien A, le groupe $\mathbb{U}_n$ des n racines n-ièmes de l'unité, l'extension galoisienne $l = k(\mathbb{U}_n)$ de k dont le groupe des k-automorphismes est noté Γ', et enfin les corps $K = k(t)$ et $l(t)$ (où t est une indéterminée sur k), l'extension galoisienne donnée N réalisant régulièrement Γ_0 sur k, et l'extension $L = N(\mathbb{U}_n) = l(N)$.



Étant donné que N est régulière sur k, il en est de même de $l(N)$ sur l et le groupe de Galois de $N/k(t)$ est égal à celui de $l(N)/l(t)$. Les automorphismes du groupe $\Gamma' = \mathrm{Gal}_k l$ se prolongent également canoniquement sur les extensions $l(t)/k(t)$, puis L/N car $l(t)$ et N sont linéairement disjointes sur K. Alors L est une extension galoisienne de K et son groupe de Galois est

$$\Gamma = \Gamma_0 \times \Gamma'$$

Soit B/L^{*n} un sous-groupe fini (multiplicatif) de L^*/L^{*n}, stable sous l'action galoisienne de Γ, en fait $\gamma(B) = B$ pour tout $\gamma \in \Gamma$. Ceci équivaut à dire que $B \subset L^*$ est globalement invariant par Γ. Considérons l'extension M de L engendrée (dans une clôture algébrique $\overline{L}$ de L) par les racines n-ièmes des éléments de B.

$$M = L(B^{\frac{1}{n}}) = L\big(\{y \in \overline{L} \mid y^n \in B\}\big)$$

Cette extension M est une extension de Kummer sur L : elle est n-abélienne et son groupe de Galois est canoniquement isomorphe au dual de B/L^{*n}.

De plus, le corps $M = L(B^{\frac{1}{n}})$ est une extension galoisienne sur K : en effet, si σ appartient à $\mathrm{Hom}_K(M, \overline{L})$ alors $\sigma_{|L}$ appartient à $\Gamma = \mathrm{Gal}_K L$. Ainsi

$$\sigma(L) = L, \quad \sigma(L^{*n}) = L^{*n}, \quad \sigma(B/L^{*n}) = B/L^{*n}$$

car B/L^{*n} est stable par l'action galoisienne de Γ. Comme $\sigma_{|L}$ appartient à $\Gamma = \mathrm{Gal}_K L$ et que B est stable par Γ, il est facile de constater que $B^{\frac{1}{n}}$ est également stable sous l'action de σ :

$$\forall\ y \in B^{\frac{1}{n}} \qquad \sigma(y)^n = \sigma(y^n) \in \sigma(B) = B$$

Ainsi le corps $M = L(B^{\frac{1}{n}})$ est stabilisé par chaque $\sigma \in \mathrm{Hom}_K(M, \overline{L})$. C'est donc une extension normale (galoisienne) de K.

Dès lors, nous possédons la suite exacte suivante :

$$1 \longrightarrow \mathrm{Gal}_L M \simeq \mathrm{Hom}(B/L^{*n}, \mathbb{U}_n) \longrightarrow \mathrm{Gal}_K M \longrightarrow \mathrm{Gal}_K L = \Gamma \longrightarrow 1$$

Cette suite exacte fait naître une action de Γ sur le groupe abélien $\mathrm{Hom}(B/L^{*n}, \mathbb{U}_n)$. Constatons qu'il s'agit bien de la "Hom-action". Nous savons que Γ opère sur $\mathrm{Gal}_L M$ par conjugaison intérieure, grâce à un relevé "ensembliste" quelconque de Γ dans $\mathrm{Gal}_K M$ (voir la démonstration de la propriété IV.6.3). Nous rappelons l'isomorphisme canonique

$$\begin{array}{ccc} \mathrm{Gal}_L M & \xrightarrow{\sim} & \mathrm{Hom}_{\mathbb{Z}}(B/L^{*n}, \mathbb{U}_n) \\ \sigma & \longmapsto & \chi_\sigma \ : \ \left[\overline{b} \mapsto \frac{\sigma(b^{\frac{1}{n}})}{b^{\frac{1}{n}}}\right] \end{array}$$

Remarque. Lorsque $\mathbb{U}_n$ apparaît dans la notation des Γ-modules, le groupe $\mathbb{U}_n \subset L^*$ est muni de l'action galoisienne de $\Gamma = \mathrm{Gal}_K L$.

Pour tout $\gamma \in \Gamma$ et $b \in B$, si β désigne une racine n-ième de b, alors $\gamma(\beta)$ est une racine n-ième de $\gamma(b)$ et

$$\chi_{\gamma\sigma\gamma^{-1}}(\overline{b}) = \frac{\gamma\sigma\gamma^{-1}(\beta)}{\beta} = \gamma\frac{\sigma\gamma^{-1}(\beta)}{\gamma^{-1}(\beta)} = \gamma\frac{\sigma(\gamma^{-1}.\beta)}{(\gamma^{-1}.\beta)} = \gamma \circ \chi_\sigma(\gamma^{-1}.\overline{b})$$

L'action de Γ sur $\mathrm{Hom}_{\mathbb{Z}}(B/L^{*n}, \mathbb{U}_n)$ est bien l'action résultante des actions de Γ sur B/L^{*n} et sur $\mathbb{U}_n$.

Supposons à présent que le Γ-module B/L^{*n} soit co-induit par A

$$B/L^{*n} \simeq \quad \mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}} A_0$$

Comme B/L^{*n} est un Γ-module induit, son dual $\mathrm{Hom}_{\mathbb{Z}}(B/L^{*n}, \mathbb{U}_n)$ est un Γ-module co-induit. Grâce au corollaire IV.6.1, nous pouvons conclure immédiatement que $\mathrm{Gal}_K M$ est isomorphe canoniquement au produit semi-direct $\mathrm{Hom}_{\mathbb{Z}}(B/L^{*n}, \mathbb{U}_n) \rtimes \Gamma$: l'action

de Γ sur $\mathrm{Hom}_{\mathbb{Z}}(B/L^{*n}, \mathbb{U}_n)$ est la conjugaison intérieure dans $\mathrm{Gal}_K M$, c'est-à-dire la "Hom-action" sur le Γ-module $\mathrm{Hom}_{\mathbb{Z}}(B/L^{*n}, \mathbb{U}_n)$.

$$\mathrm{Gal}_K M \simeq \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}} A_0, \mathbb{U}_n) \rtimes \Gamma$$

L'action de Γ sur $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}} A_0, \mathbb{U}_n) \simeq \mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}} \mathrm{Hom}_{\mathbb{Z}}(A_0, \mathbb{U}_n)$ (car Γ est un groupe fini) est l'action "tordue" résultante de l'action régulière sur $\mathbb{Z}[\Gamma]$ et de l'action galoisienne de Γ sur $\mathbb{U}_n$:

$$(\gamma.\chi).(\tau \otimes a) = \gamma \circ \chi(\gamma^{-1}\tau \otimes a) \qquad a \in A,\ \gamma, \tau \in \Gamma,\ \chi \in (B/L^{*n})^{\bullet}$$

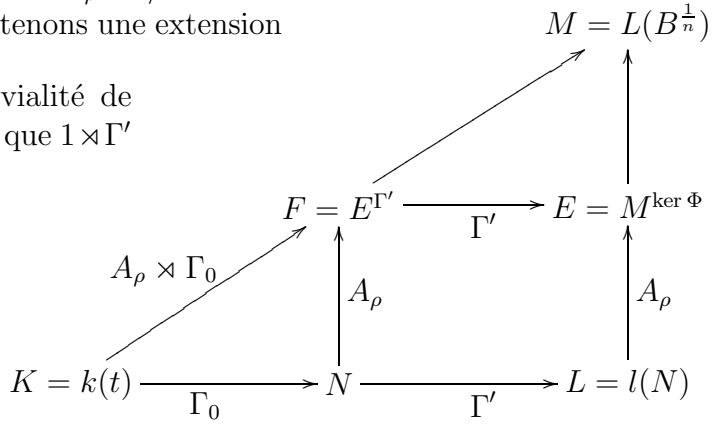
Nous savons de plus, grâce à la propriété IV.6.1, que l'action "tordue" de Γ sur le groupe $\mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}} \mathrm{Hom}_{\mathbb{Z}}(A_0, \mathbb{U}_n)$ est isomorphe à l'action régulière de Γ sur le groupe $\mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}} \mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{U}_n)_0$. Enfin, comme le dual de A est isomorphe à A, le groupe de Galois $\mathrm{Gal}_L M$ est isomophe (isomophisme de Γ-modules) à $\mathbb{Z}[\Gamma] \otimes A_0$.

Au vu de la définition de $\Gamma = \Gamma_0 \times \Gamma'$, nous pouvons prolonger l'action ρ de Γ_0 sur A en une action, toujours notée ρ pour ne pas alourdir les notations, de Γ sur A où seule la première composante opère : si $\gamma = (\gamma_0, \gamma') \in \Gamma_0 \times \Gamma'$ alors $\rho(\gamma) = \rho(\gamma_0)$. Le groupe Γ' opère trivialement sur A. Autrement dit, le produit semi-direct $A_\rho \rtimes \Gamma$ est isomorphe au groupe $(A_\rho \rtimes \Gamma_0) \times \Gamma'$.

La propriété IV.6.1 indique que tout Γ-module $\mathfrak{M}$ est un quotient canonique du Γ-module induit par $\mathfrak{M}_0$. Si nous appliquons ce résultat au groupe induit $\mathrm{Gal}_L M$ en considérant l'action ρ de Γ sur A, nous prouvons l'existence d'un épimorphisme de Γ-modules

$$\Phi \ :\ \mathrm{Gal}_L M \simeq \mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}} A_0 \longrightarrow A_\rho$$

Par suite, la sous-extension $E = M^{\ker \Phi}$ est galoisienne à la fois sur L et sur K. Les groupes de Galois respectifs sont A_ρ et $A_\rho \rtimes \Gamma \simeq (A_\rho \rtimes \Gamma_0) \times \Gamma'$.
Il est facile de constater que le quotient $A_\rho \rtimes \Gamma / 1 \rtimes \Gamma'$ est exactement $A_\rho \rtimes \Gamma_0$. Ainsi nous obtenons une extension de $K = k(t)$ de groupe $A_\rho \rtimes \Gamma_0$.
Remarquer l'importance de la trivialité de l'action de Γ' sur A_ρ : cela entraîne que $1 \rtimes \Gamma'$ est distingué dans $A_\rho \rtimes \Gamma$ et $E^{\Gamma'}$ est bien une extension galoisienne de K.



Propriété IV.7.1 *On suppose que Γ_0 est réalisé sur $K = k(t)$ par une extension N régulière sur k et que la caractéristique de k est étrangère à l'exposant n d'un groupe abélien fini A. Soit $L = N(\mathbb{U}_n)$ et $\Gamma = \mathrm{Gal}_K L$. Tout sous-groupe fini B/L^{*n} de L^*/L^{*n} induit par A permet de construire une extension F de N contenue dans $L(B^{\frac{1}{n}})$, galoisienne sur $K = k(t)$ dont le groupe de Galois est le produit semi-direct $A_\rho \rtimes \Gamma_0$ où ρ est une action quelconque de Γ_0 sur A.*

IV.8 Réalisation régulière effective de $A_\rho \rtimes \Gamma_0$

La section précédente nous montre une voie possible pour réaliser tout produit semi-direct $A_\rho \rtimes \Gamma_0$ sur $k(t)$. Il reste cependant plusieurs étapes à franchir si l'on veut réaliser concrètement le groupe $A_\rho \rtimes \Gamma_0$. Reprenons les notations de la section précédente : k est un corps de caractéristique étrangère à l'exposant n du groupe abélien A, $l = k(\mathbb{U}_n)$, $K = k(t)$, l'extension galoisienne N/K réalise le groupe Γ_0 régulièrement sur k, et l'extension $L = l(N) = N(\mathbb{U}_n)$. Enfin ρ est une action quelconque de Γ_0 sur A que l'on prolonge à $\Gamma = \mathrm{Gal}_K L = \Gamma_0 \times \mathrm{Gal}_k l$ en ne considérant que la première coordonnée.

La première étape de la méthode consiste à construire un sous-groupe de L^*/L^{*n} Γ-induit par le groupe abélien fini A donné :

$$B/L^{*n} \simeq \mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}} A_0$$

Ce groupe $B \subset L^*$ engendre l'extension kummerienne $M = L(B^{\frac{1}{n}})$. Nous avons vu que cette extension est galoisienne sur K et que son groupe de Galois est isomorphe canoniquement au produit semi-direct $(\mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}} A_0)^\bullet \rtimes \Gamma$.

Puis il faut connaître explicitement la sous-extension $E = M^{\ker \Phi}$ (voir le diagramme ci-dessus). On rappelle que E est une extension galoisienne de L et de K, de groupes de Galois respectifs A_ρ et $A_\rho \rtimes \Gamma$.

Pour trouver un système de générateurs de E/L, ou même une base de E/L, nous utiliserons la théorie de Kummer : cette théorie fournit une base de l'extension E/L à partir d'un système représentatif des classes d'un certain sous-groupe de B/L^{*n}. Elle donne également un système de générateurs de l'extension E/L en fonction d'un système générateur du même sous-groupe de B/L^{*n} (voir le théorème IV.2.1, page 105).

En dernier lieu, nous devrons assurer que l'extension galoisienne $F = E^{\mathrm{Gal}_k l}$ de K (dont le groupe de Galois est $A_\rho \rtimes \Gamma_0$) est régulière sur k. Le lecteur pourra vérifier que le critère que nous donnerons est excessivement simple. Il s'agit d'un critère de séparabilité portant sur des polynômes irréductibles (critère toujours vérifié en caractéristique 0).

IV.8.a Construction d'un sous-groupe induit de L^*/L^{*n}

Ce passage s'inspire du dernier paragraphe du chapitre 2 de Serre ([54], page 18).

Lemme IV.8.1 *Soit $\mathcal{O}$ un anneau de Dedekind de corps des fractions K et L/K une extension galoisienne de groupe de Galois Γ. Pour tout idéal premier $\mathfrak{p}$ de $\mathcal{O}$ totalement décomposé dans L, il existe $a \in L^*$ vérifiant*

$$v_{\gamma.\mathcal{P}}(\tau(a)) = \delta_{\tau,\gamma} \qquad \tau, \gamma \in \Gamma$$

où $\mathcal{P}$ désigne un idéal premier quelconque de L au-dessus de $\mathfrak{p}$ et $v_{\tau.\mathcal{P}}$ la valuation en $\tau.\mathcal{P}$ (δ est le symbole de Kronecker).

Par suite, l'élément a est un élément primitif de l'extension L/K, et quels que soient $n \in \mathbb{N}^*$ et $\gamma \in \Gamma$, $\gamma(a)$ est d'ordre n dans le quotient L^*/L^{*n}. De plus, toujours dans L^*/L^{*n}, le produit de sous-groupes $\prod_{\gamma\in\Gamma} \left\langle \overline{\gamma(a)} \right\rangle$ est direct. Il s'agit donc d'un sous-groupe de L^*/L^{*n} Γ-induit par $\mathbb{Z}/n\mathbb{Z}$.

Démonstration Comme $\mathfrak{p}$ est totalement ramifié dans L (extension galoisienne de K de groupe Γ), cet idéal se factorise en

$$\mathfrak{p} = \prod_{\gamma\in\Gamma} \gamma.\mathcal{P}$$

Le théorème chinois certifie l'existence d'un élément $a \in \mathcal{P}$ n'appartenant ni à $\mathcal{P}^2$, ni à $\gamma.\mathcal{P}$ pour $\gamma \in \Gamma$, $\gamma \neq \mathrm{Id}$:

$$a \in \mathcal{P} \setminus \{0\} \mod \mathcal{P}^2 \qquad \text{et} \qquad a \notin \gamma.\mathcal{P} \qquad \forall\, \gamma \neq \mathrm{Id}$$

Ainsi, nous avons la relation

$$v_{\gamma.\mathcal{P}}(a) = \delta_{\mathrm{Id},\gamma}$$

Cette relation peut être Γ-conjuguée pour prouver le premier résultat du lemme.

Par suite, a est un élément primitif de L/K puisqu'il possède un nombre maximum de conjugués sous l'action de Γ : $\gamma(a) \in \gamma.\mathcal{P} \setminus \mathcal{P}$ pour $\gamma \neq \mathrm{Id}$.

Pour montrer que $\overline{a}$ est d'ordre n dans L^*/L^{*n}, considérons une égalité $a^j = x^n$ avec $x \in L^*$. Prenons la valuation en $\mathcal{P}$ de chaque terme de cette égalité :

$$j = j v_{\mathcal{P}}(a) = n v_{\mathcal{P}}(x) \in \mathbb{Z}$$

Il est clair que j est multiple de n, donc $\overline{a}$ est bien d'ordre n. Par conjugaison, $\overline{\gamma(a)}$ est également d'ordre n.

Enfin, prenons simultanément tous les Γ-conjugués de a. Ils engendrent dans L^*/L^{*n} un produit direct : un élément de $\left\langle \overline{\gamma(a)} \mid \gamma \in \Gamma \right\rangle$ s'écrit comme la classe de

$$\prod_{\gamma} \gamma(a)^{\alpha_\gamma} \qquad \alpha_\gamma \in \mathbb{Z}/n\mathbb{Z}$$

L'élément unité de L^*/L^{*n} ne peut s'écrire qu'avec $\alpha_\gamma = 0$ pour tout $\gamma \in \Gamma$ (utiliser les valuations en $\gamma.\mathcal{P}$). Finalement, nous concluons que le sous-groupe $\prod_{\gamma\in\Gamma} \left\langle \overline{\gamma(a)} \right\rangle$ est Γ-induit par $\mathbb{Z}/n\mathbb{Z}$. □

D'après ce qui vient d'être démontré, la construction d'un Γ-module induit par $\mathbb{Z}/n\mathbb{Z}$ passe par la connaissance d'un idéal premier totalement décomposé. Voici comment trouver un tel idéal. Ce lemme établit une certaine réciproque effective au lemme précédent.

Lemme IV.8.2 *Soit $\mathcal{O}$ un anneau de Dedekind de corps des fractions K et L/K une extension galoisienne de groupe de Galois Γ. Soit a un élément de L entier sur $\mathcal{O}$. On note N la norme de l'extension L/K. Tout idéal premier $\mathfrak{p}$ de $\mathcal{O}$ vérifiant*

$$v_{\mathfrak{p}}(N(a)) = 1 \qquad \text{et} \qquad \mathfrak{p} \text{ non ramifié dans } L$$

est totalement décomposé dans L. De plus, il existe un idéal premier $\mathcal{P}$ de L au-dessus de $\mathfrak{p}$ tel que

$$v_{\gamma.\mathcal{P}}(\tau(a)) = \delta_{\tau,\gamma} \qquad \tau, \gamma \in \Gamma$$

où $v_{\tau.\mathcal{P}}$ la valuation en $\tau.\mathcal{P}$.

Démonstration Comme $\mathfrak{p}$ contient $N(a) = \prod_{\gamma\in\Gamma} \gamma(a)$, il existe un idéal premier $\mathcal{P}$ de L au-dessus de $\mathfrak{p}$ et contenant a.

Considérons à présent $v_{\mathfrak{p}}$ et $v_{\mathcal{P}}$ les valuations respectives liées aux premiers $\mathfrak{p}$ et $\mathcal{P}$ dans K et L. Comme $\mathfrak{p}$ n'est pas ramifié dans L, la valuation $v_{\mathcal{P}}$ est un prolongement de $v_{\mathfrak{p}}$. Ainsi on obtient

$$\sum_{\gamma\in\Gamma} v_{\mathcal{P}}(\gamma(a)) = v_{\mathcal{P}}\left(\prod_{\gamma\in\Gamma} \gamma(a)\right) = v_{\mathfrak{p}}\big(N(a)\big) = 1$$

Or $v_{\mathcal{P}}(a) \geq 1$ et $v_{\mathcal{P}}(\gamma(a)) \geq 0$ car a est entier sur $\mathcal{O}$, donc l'égalité ci-dessus force la suivante :

$$v_{\mathcal{P}}(\gamma(a)) = \delta_{\gamma,\mathrm{Id}} \qquad \forall\ \gamma \in \Gamma$$

Cette relation peut être Γ-conjuguée pour prouver le résultat du lemme. Enfin, le stabilisateur dans Γ de l'idéal $\mathcal{P}$ est réduit à $\{\mathrm{Id}\}$ car $\tau.\mathcal{P} = \mathcal{P}$ implique $\tau(a) \in \mathcal{P}$, donc $\tau = \mathrm{Id}$: l'idéal $\mathfrak{p}$ est par conséquent totalement décomposé dans L. □

Finalement, pour obtenir un groupe Γ-induit par un groupe abélien fini quelconque, il suffit simplement de généraliser les lemmes précédents :

Propriété IV.8.1 *Soit $\mathcal{O}$ un anneau de Dedekind de corps des fractions K et L/K une extension galoisienne de groupe de Galois Γ. Soit $(a_j)_{j\in J}$ une famille d'éléments de L entiers sur $\mathcal{O}$. On note N la norme de l'extension L/K. Soit $(\mathfrak{p}_j)_{j\in J}$ des* ***idéaux premiers distincts*** *de $\mathcal{O}$ tels que*

$$v_{\mathfrak{p}_i}(N(a_j)) = \delta_{i,j} \qquad \text{et} \qquad \mathfrak{p}_i \text{ non ramifié dans } L$$

Alors les $(a_j)_{j\in J}$ sont des éléments primitifs de L/K, et quel que soit le groupe abélien fini $A = \bigoplus_{j\in J} \mathbb{Z}/n_j\mathbb{Z}$ d'exposant n, le sous-groupe de L^*/L^{*n} engendré par $\overline{a_j}^{\frac{n}{n_j}}$ est un groupe Γ-induit par A.

Démonstration Grâce aux lemmes précédents, nous savons que les éléments a_j sont des éléments primitifs de l'extension L/K et nous avons la relation

$$v_{\gamma.\mathcal{P}_i}(\tau(a_j)) = \delta_{\tau,\gamma}\delta_{i,j} \qquad \tau, \gamma \in \Gamma,\ i, j \in J$$

où $\mathcal{P}_j$ est un idéal premier de L au-dessus de $\mathfrak{p}_j$ et contenant a_j. Ce genre d'égalité montre à la fois que les idéaux $\mathfrak{p}_j$ sont totalement décomposés dans L et que les groupes $\left\langle \overline{\gamma(a_j)} \right\rangle_{\substack{j\in J \\ \gamma\in\Gamma}}$ sont d'ordre n et en produit direct dans L^*/L^{*n} (utiliser les valuations en les $\gamma.\mathcal{P}_j$). Ainsi, $\prod_{\substack{j\in J \\ \gamma\in\Gamma}} \left\langle \overline{\gamma(a_j)} \right\rangle$ est Γ-induit par $\bigoplus_{j\in J} \mathbb{Z}/n\mathbb{Z}$. Il suffit alors d'élever les classes $\overline{\gamma(a_j)}$ à la puissance $\frac{n}{n_j}$ pour trouver le groupe induit par A désiré. □

Revenons au diagramme de la section IV.7 (page 137). Il nous est maintenant possible de construire un sous-groupe de L^*/L^{*n} qui soit Γ-induit par un groupe abélien fini donné. La méthode est la suivante : soit $(a_j)_{j\in J}$ des éléments primitifs distincts de $L/k(t)$ et entiers sur $k[t]$, $(p_j)_{j\in J}$ de polynômes irréductibles de $k[t]$, étrangers 2 à 2, non ramifiés dans L, divisant une seule fois la norme de leur a_j respectif et ne divisant pas la norme des autres a_i. (Ces conditions sont tout-à-fait raisonnables et faciles à contrôler.) Alors nous avons

$$\forall\ j \in J, \quad a'_j = a_j^{\frac{n}{n_j}} \qquad\qquad A = \bigoplus_{j\in J} \mathbb{Z}/n_j\mathbb{Z} \quad \widetilde{\longleftrightarrow} \quad \left\langle (a'_j)_{j\in J},\ L^{*n} \right\rangle \ /\ L^{*n} = A'$$

De plus, les Γ-conjugués $\gamma.A$ de A sont en produit direct dans L^*/L^{*n}, si bien que le sous-groupe de L^*/L^{*n}

$$B/L^{*n} = \prod_{\gamma\in\Gamma} \gamma.A' \simeq \mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}} A_0$$

est Γ-induit par A.

IV.8.b Réalisation du groupe $A_\rho \rtimes \Gamma_0$

Il faut à présent rendre *effective* l'extension $E = M^{\ker \Phi}$ construite *abstraitement* dans la section IV.7. Pour cela, nous allons expliciter complètement les morphismes canoniques que nous avons considérés dans la section IV.7.

Soit B/L^{*n} un sous-groupe fini de L^*/L^{*n}. Grâce à la théorie de Kummer, nous savons que le groupe de Galois de l'extension $M = L(B^{\frac{1}{n}})$ est isomorphe canoniquement au dual de B/L^{*n}

$$\begin{array}{ccc} \mathrm{Gal}_L M & \widetilde{\longrightarrow} & \mathrm{Hom}_{\mathbb{Z}}(B/L^{*n}, \mathbb{U}_n) \\ \sigma & \longmapsto & \left[\overline{b} \mapsto \frac{\sigma(b^{\frac{1}{n}})}{b^{\frac{1}{n}}} \right] \end{array}$$

> Remarque. Lorsque $\mathbb{U}_n$ apparaît dans la notation des Γ-modules, le groupe $\mathbb{U}_n \subset L^*$ est muni de l'action galoisienne de $\Gamma = \mathrm{Gal}_K L$.

Supposons que B/L^{*n} soit Γ-induit par le groupe abélien fini A fixé à l'avance :

$$B/L^{*n} \simeq \mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}} A_0$$

Le groupe $\mathrm{Hom}_{\mathbb{Z}}(B/L^{*n}, \mathbb{U}_n)$ est alors Γ-induit par $A_0^\bullet$ (car Γ est fini) :

$$\begin{array}{rcl} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}} A_0, \mathbb{U}_n) & \xrightarrow{\sim} & \mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}} \mathrm{Hom}_{\mathbb{Z}}(A_0, \mathbb{U}_n) \\ \chi & \longmapsto & \displaystyle\sum_{\gamma \in \Gamma} \gamma \otimes \chi(\gamma \otimes \bullet) \end{array}$$

$$\begin{array}{rcl} \mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}} \mathrm{Hom}_{\mathbb{Z}}(A_0, \mathbb{U}_n) & \xrightarrow{\sim} & \mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}} A_0^\bullet \\ \gamma \otimes \chi & \longmapsto & \gamma \otimes (\gamma^{-1} \circ \chi) \end{array}$$

Rappel. A tout morphisme de groupes abéliens finis $h : G_1 \to G_2$ on peut associer un morphisme "dual" $h^\bullet$ défini par $G_2^\bullet \to G_1^\bullet : \chi \mapsto \chi \circ h$.

Réciproquement, tout morphisme $g : G_2^\bullet \to G_1^\bullet$ est le "dual" d'un morphisme de G_1 dans G_2. En effet, si $g : G_2^\bullet \to G_1^\bullet$ est donné, nous pouvons considérer son morphisme "dual" $g^\bullet : G_1^{\bullet\bullet} \to G_2^{\bullet\bullet}$ qui envoie $\mathrm{eval}_x \in G_1^{\bullet\bullet}$ sur $\mathrm{eval}_x \circ g = \mathrm{eval}_{h(x)} \in G_2^{\bullet\bullet}$ pour tout $x \in G_1$ (tout caractère du bi-dual d'un groupe G est un morphisme d'évalution en un point de G). L'application $h : G_1 \to G_2$ ainsi obtenue est un morphisme de groupes, et son morphisme "dual" est g.

Si $G_1 = G_2 = G$, alors nous pouvons définir le morphisme canonique suivant entre le groupe d'automorphismes de G et celui de $G^\bullet$:

$$\begin{array}{rcl} \Psi \ : \ \mathrm{Aut}(G) & \xrightarrow{\sim} & \mathrm{Aut}\left(G^\bullet\right) \\ f & \longmapsto & \left(f^{-1}\right)^\bullet \ : \ \left[\chi \mapsto \chi \circ f^{-1}\right] \end{array}$$

D'après ce qui précède, cette application est surjective. Les cardinaux des deux groupes $\mathrm{Aut}(G)$ et $\mathrm{Aut}(G^\bullet)$ étant égaux, le morphisme Ψ est bijectif.

Si $\rho : \Gamma \to \mathrm{Aut}(G)$ est une représentation, on définit sa **représentation duale** ou **contragrédiente** $\rho^\bullet$ (voir [38], pages 664-665) par

$$\rho^\bullet(\gamma).\chi = \chi \circ \rho(\gamma^{-1}) \qquad\qquad \gamma \in \Gamma, \ \chi \in G^\bullet$$

Toute action sur $G^\bullet$ la contragrédiente d'une action sur G.

Soit ρ une action quelconque de Γ sur le groupe A. En choisissant un isomorphisme de groupes entre A et $A^\bullet$, nous transportons l'action $\rho : \Gamma \to \mathrm{Aut}(A)$ en une action isomorphe $\Gamma \to \mathrm{Aut}(A^\bullet)$. Cette action de Γ sur $A^\bullet$ est l'action contragrédiente d'une certaine action $\rho' : \Gamma \to \mathrm{Aut}(A)$, de sorte que les Γ-modules A_ρ et $A^\bullet_{\rho'^\bullet}$ sont isomorphes.

Remarque. Nous introduisons ici l'action contragrédiente d'une action isomorphe à ρ, ce qui peut paraître curieux. En fait, tout s'expliquera par la suite : il est presque obligatoire d'avoir une action sur $A^\bullet$ pour expliciter les morphismes canoniques qui suivent, et il sera plus commode de l'écrire sous la forme d'une action contragrédiente pour trouver un certain sous-groupe de $\mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}} A_0$.

Grâce à la théorie des Γ-modules (induits), nous disposons du morphisme surjectif suivant :

$$\begin{array}{rcl} \mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}} A_0^\bullet & \longrightarrow & A^\bullet_{\rho'^\bullet} \\ \gamma \otimes \chi & \longmapsto & \rho'^\bullet(\gamma).\chi \end{array}$$

Enfin, le groupe $\Gamma = \mathrm{Gal}_K L$ opère sur les racines n-ièmes de l'unité car $\mathbb{U}_n$ est inclus dans L. Comme pour tout groupe cyclique d'ordre n, les automorphismes de $\mathbb{U}_n$ sont des élévations à des puissances premières avec n : nous définissons donc un morphisme de groupes $i : \Gamma \to \mathrm{U}(\mathbb{Z}/n\mathbb{Z})$ par l'égalité

$$\gamma.w = w^{i(\gamma)} \qquad\qquad \gamma \in \Gamma, w \in \mathbb{U}_n$$

En composant tous les morphismes de Γ-modules ci-dessus, nous obtenons finalement

$$\begin{array}{rcccl} \Phi & : & (\mathrm{Gal}_L M)_\Gamma & \longrightarrow & (\mathrm{Gal}_L E)_\Gamma \longrightarrow 1 \\ & & \wr| & & \wr| \\ & & \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}} A_0, \mathbb{U}_n) & \longrightarrow & A_{\rho'}^{\bullet}{}_{\bullet} \simeq A_\rho \\ & & \chi & \longmapsto & \displaystyle\prod_{\gamma\in\Gamma} \chi(\gamma \otimes \rho'(\gamma^{-1})_\bullet)^{i(\gamma^{-1})} \end{array}$$

La théorie de Kummer relie les extensions abéliennes de L, telles M et E, et les sous-groupes finis de L^*/L^{*n}. L'extension M est engendrée par les racines n-ièmes des éléments de B/L^{*n}. Comme E est une sous-extension de M, elle est engendrée par les racines n-ièmes des éléments d'un certain sous-groupe de B/L^{*n}. Il nous faut trouver ce sous-groupe pour connaître l'extension E. Pour cela, il est bon de penser que nous cherchons un sous-Γ-module de $B/L^{*n} \simeq \mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}} A_0$ isomorphe au Γ-module A_ρ : ce sera l'image de A par l'injection suivante

$$\begin{array}{rcl} 1 \longrightarrow A & \longrightarrow & \mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}} A_0 \\ a & \longmapsto & \sum_\gamma \gamma \otimes f_\gamma(a) \end{array}$$

dont l'application duale est donnée par l'épimorphisme Φ. Dire que Φ est l'application duale de l'injection $A \hookrightarrow \mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}} A_0$ revient à poser

$$\forall\ \chi \in (\mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}} A_0)^\bullet, \qquad \chi\big(\sum_{\gamma\in\Gamma} \gamma \otimes f_\gamma(a)\big) = \prod_{\gamma\in\Gamma} \chi\big(\gamma \otimes \rho'(\gamma^{-1}).a^{i(\gamma^{-1})}\big)$$

Nous avons alors nécessairement $f_\gamma(a) = \rho'(\gamma^{-1}).a^{i(\gamma^{-1})}$, et finalement le sous-$\Gamma$-module cherché dans $\mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}} A_0$ est

$$\left\{ \sum_{\gamma\in\Gamma} \gamma \otimes \rho'(\gamma^{-1}).a^{i(\gamma^{-1})} \ \mid\ a \in A \right\}$$

Si B/L^{*n} est réalisé dans L^*/L^{*n} explicitement par un sous-groupe $A' \subset L^*/L^{*n}$ isomorphe à A tel que $B/L^{*n} = \prod_{\gamma\in\Gamma} \gamma.A'$ (conclusion de la section IV.8.a)

$$\begin{array}{rcccl} \pi & : & A & \longleftrightarrow & A' \\ & & a & \longmapsto & \pi(a) \end{array} \qquad\qquad \begin{array}{rcl} \mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}} A & \longleftrightarrow & A' \\ \gamma \otimes a & \longmapsto & \gamma \circ \pi(a) \end{array}$$

alors le sous-groupe de B (contenant L^{*n}) définissant la sous-extension de Kummer E/L est engendré par des éléments $(d_a)_{a\in A}$:

$$d_a \equiv \prod_{\gamma\in\Gamma} \gamma \circ \pi \circ \rho'(\gamma^{-1}).a^{i(\gamma^{-1})} \qquad \mod\ L^{*n}$$

Leurs racines n-ièmes $e_a = d_a^{\frac{1}{n}}$ engendrent E/L.

$$E = L\big((e_a)_{a\in A}\big)$$

Par cette égalité, nous venons d'expliciter l'extension $E \subset M$ dont le groupe de Galois sur L est isomorphe à A_ρ, et son groupe de Galois sur K est $A_\rho \rtimes \Gamma$. De plus, la théorie de Kummer nous affirme que les $(e_a)_{a\in A}$ forment une base de l'extension E/L.

Finalement, Γ' étant un sous-groupe distingué de $A_\rho \rtimes \Gamma$, l'extension $E^{\Gamma'}/K$ est galoisienne de groupe $A_\rho \rtimes \Gamma/\Gamma' \simeq A_\rho \rtimes \Gamma_0$.

Promesse d'explication...

Dans les sections IV.3 et IV.5, nous avions promis au lecteur de donner une explication quant au choix des éléments d et d_j. Ce sera maintenant chose faite !

Si A est cyclique d'ordre n, alors l'opération ρ' de Γ sur A est une exponentation :

$$\rho'(\gamma).a = a^{h(\gamma)} \qquad h(\gamma) \in \mathrm{U}(\mathbb{Z}/n\mathbb{Z})$$

si bien que l'élément d_a prend la forme

$$d_a \equiv \prod_{\gamma\in\Gamma} \gamma(a)^{h(\gamma^{-1})i(\gamma^{-1})} \qquad \mod\ L^{*n}$$

Dans le cas où $\Gamma_0 = \{\mathrm{Id}\}$, choisissons $a = 1 + xt$ où x est un élément primitif de l'extension $l = k(\mathbb{U}_n)$ de k : nous obtenons

$$d \equiv \prod_{\gamma\in\mathrm{Gal}_k\, l} \big(1+\gamma(x)t\big)^{i(\gamma^{-1})} \qquad \mod\ L^{*n}$$

Nous retrouvons l'expression de l'élément d donné page 108 pour réaliser les groupes cycliques.

De même si $\Gamma_0 = \{\tau, \mathrm{Id}\}$ et $h(\tau) \equiv -1 \mod n$, choisissons $a = 1 + xt^{\frac{1}{2}}$ où x est toujours primitif de l/k : nous obtenons

$$d \equiv \prod_{\gamma\in\mathrm{Gal}_k\, l} \big(1+\gamma(x)t^{\frac{1}{2}}\big)^{i(\gamma^{-1})}\big(1-\gamma(x)t^{\frac{1}{2}}\big)^{-i(\gamma^{-1})} \qquad \mod\ L^{*n}$$

Nous expliquons ainsi le choix de l'élément d_j donné page 122 pour réaliser les groupes diédraux.

IV.8.c Condition de régularité

Propriété IV.8.2 *Soit $\mathcal{O}$ un anneau de Dedekind, L son corps des fractions, et L'/L une extension finie. Considérons un sous-groupe fini $B/L^{*n} = \langle (a_i \mod L^{*n})_{i\in I}\rangle$ de L^*/L^{*n} fabriqué à partir d'éléments $a_i \in L$ et des idéaux premiers $(\mathcal{P}_i)_{i\in I}$ distincts 2 à 2 de L tels que*

$$v_{\mathcal{P}_i}(a_j) = \delta_{i,j} \qquad \forall\ i,j \in I$$

Si les $(\mathcal{P}_i)_{i\in I}$ ne sont pas ramifiés dans L', alors le morphisme

$$\begin{array}{ccc} L^*/L^{*n} & \longrightarrow & L'^*/L'^{*n} \\ x \mod L^{*n} & \longmapsto & x \mod L'^{*n} \end{array}$$

est injectif lorsque on le restreint à un sous-groupe de B/L^{*n}. Autrement dit, c'est un isomorphisme de B/L^{*n} sur $BL'/L'^{*n} = \langle (a_i \mod L'^{*n})_{i\in I}\rangle$.

Démonstration En premier lieu, remarquons que les groupes $\langle\overline{a_j}\rangle$ sont en produit direct dans L^*/L^{*n} et que l'ordre de $\overline{a_i}$ est égal à n : en effet, écrire l'élément unité de L^*/L^{*n} sous la forme

$$\prod_{i\in I} \overline{a_i}^{\alpha_i} \qquad\qquad \alpha_i \in \mathbb{Z}/n\mathbb{Z}$$

revient à poser $\alpha_i = 0 \in \mathbb{Z}/n\mathbb{Z}$ (utiliser la valuation $v_{\mathcal{P}_i}$).

Soit V_i une valuation de L' prolongeant la valuation $v_{\mathcal{P}_i}$. Comme $\mathcal{P}_i$ n'est pas ramifié dans L', la valuation V_i est à valeur dans $\mathbb{Z}$.

Dans L', nous avons évidemment $V_i(a_j) = \delta_{i,j}$. Ceci prouve, à l'instar des lignes précédentes, que les sous-groupes $\langle a_j \mod L'^{*n}\rangle$ sont en produit direct dans L'^*/L'^{*n}, et que l'ordre de $\overline{a_i} \in L'^*/L'^{*n}$ est égal à n. □

Lemme IV.8.3 *Considérons une extension finie L de $K = k(t)$, h une extension finie de k et le compositum $L' = h(L)$. Soit $p \in k[t]$ un irréductible séparable non ramifié dans L, et $\mathcal{P}$ un idéal de L au-dessus de p. Alors $\mathcal{P}$ n'est pas ramifié dans L'.*

Démonstration Comme p est séparable, p est non ramifié dans $h(t)$: p se factorise en produit d'irréductibles étrangers 2 à 2. En théorie des corps locaux, il est connu que le compositum de deux extensions finies non ramifiées est non ramifié (voir [46], pages 229-230). Ceci veut dire que p est non ramifié dans L'. En particulier, l'idéal $\mathcal{P}$ (au-dessus de p dans L) n'est pas ramifié dans L'. □

Reprenons à présent la situation de la section IV.7 : soit L une extension galoisienne de $K = k(t)$ de groupe de Galois Γ, et considérons l'anneau de Dedekind (principal) $k[t]$. En utilisant simultanément les lemmes et propriétés des sections IV.8.a et IV.8.c, nous voyons comment construire un sous-groupe $B/L^{*n} = \left\langle \overline{\gamma(a)} \mid \gamma \in \Gamma \right\rangle$ de L^*/L^{*n} Γ-induit tel que, pour toute extension finie h de k, le groupe $B.h(L)/h(L)^{*n}$ soit isomorphe à B/L^{*n}. Autrement dit, le groupe de Galois de l'extension $M = L(B^{\frac{1}{n}})$ ne changera pas si l'on ajoute des éléments algébriques au corps de base.

$$\mathrm{Gal}_{h(L)}\, h(M) \simeq (Bh(L)^*/h(L)^{*n})^\bullet \simeq (B/L^{*n})^\bullet \simeq \mathrm{Gal}_L\, M$$

Dans ces conditions, l'extension M est régulière sur $l = k(\mathbb{U}_n) = M \cap \overline{k}$.

Théorème IV.8.1 *Soit k un corps de caractéristique étrangère à n, $f_0 \in k[t, X]$ un polynôme régulier sur k réalisant le groupe Γ_0. Autrement dit si N est le corps de décomposition de f_0 sur $K = k(t)$, alors le groupe de Galois de N/K est isomorphe au groupe Γ_0*

et l'extension N/k est régulière. On se donne une action quelconque ρ de Γ sur le groupe abélien fini $A = \bigoplus_{j\in J} \mathbb{Z}/n_j\mathbb{Z}$ d'exposant $n = \mathrm{ppcm}(n_j \mid j \in J)$.

Soit $(a_j)_{j\in J}$ des éléments primitifs distincts de l'extension $N(\mathbb{U}_n)/K$, entiers sur $k[t]$ et $(p_j)_{j\in J}$ des polynômes irréductibles de $k[t]$ étrangers 2 à 2. Si

$$v_{p_j}(N(a_i)) = \delta_{i,j} \qquad \text{et} \qquad v_{p_j}(\mathrm{dis}(f_0)) = 0$$

alors on peut construire explicitement par la méthode ci-dessus une extension galoisienne de $k(t)$ contenant N de groupe de Galois isomorphe à $A_\rho \rtimes \Gamma_0$.

Si de plus les polynômes p_j sont séparables, alors l'extension construite est régulière sur k.

Démonstration Premièrement, les polynômes irréductibles p_j ne sont pas ramifiés dans l'extension $L = N(\mathbb{U}_n)$ de K. En effet, ces premiers ne sont ni ramifiés dans N, ni dans $l(t) = k(\mathbb{U}_n, t)$ car il ne divisent ni le discriminant de f_0 ni celui de Φ_n (Φ_n est le n-ième polynôme cyclotomique sur k : son discriminant appartient à k et ne peut être divisible par p_j).

En utilisant les méthodes effectives vues dans les sections IV.8.a et IV.8.b, nous pouvons construire une extension E/L galoisienne sur K de groupe de Galois $A_\rho \rtimes \Gamma$ où $\Gamma = \mathrm{Gal}_K L = \Gamma_0 \times \mathrm{Gal}_k l$. Cette construction passe par la réalisation d'une extension de Kummer M/L (galoisienne sur K), dont le groupe de Galois sur L est isomorphe au dual d'un groupe Γ-induit par A.

Pour obtenir une extension galoisienne de K de groupe $A_\rho \rtimes \Gamma_0$, il suffit de considérer les points de E invariants sous l'action de $\Gamma' = \mathrm{Gal}_k l$ en vertu de la propriété IV.7.1 (page 137).

$$\mathrm{Gal}_K E^{\Gamma'} \simeq A_\rho \rtimes \Gamma_0$$

Enfin, il faut assurer le caractère régulier de l'extension E/k. En fait, comme les premiers p_j sont séparables, l'extension M/l est régulière (voir la section IV.8.c). Par suite l'extension $M^{\Gamma'}$ est régulière sur $l^{\Gamma'} = k$. Or $E^{\Gamma'}$ est incluse dans $M^{\Gamma'}$, ce qui l'oblige à être régulière sur k elle aussi. □

IV.9 Réalisation régulière des sous-groupes $\mathbb{Z}/n\mathbb{Z} \rtimes \Gamma_0$ de $\mathrm{AGL}_1(\mathbb{Z}/n\mathbb{Z})$ sur $\mathbb{Q}$

IV.9.a La méthode

Notre objectif est de construire un polynôme régulier de degré n, dont le groupe de Galois sur $\mathbb{Q}(t)$ est $\mathbb{Z}/n\mathbb{Z} \rtimes \Gamma_0$, où $\Gamma_0 \subset \mathrm{U}(\mathbb{Z}/n\mathbb{Z})$ agit sur $\mathbb{Z}/n\mathbb{Z}$ par simple multiplication.

Réalisation d'une extension de $\mathbb{Q}(t)$, régulière sur $\mathbb{Q}$, de groupe $\mathbb{Z}/n\mathbb{Z} \rtimes \Gamma_0$

En premier lieu, il faut réaliser régulièrement le groupe abélien Γ_0. Ceci ne pose pas de problème : par exemple en utilisant la section IV.4, nous trouvons un polynôme f_0

régulier de groupe Γ_0.

$$K = \mathbb{Q}(t) \xrightarrow{\Gamma_0} N = K[X]/(f_0) \xrightarrow{\Gamma'} L = N(\mathbb{U}_n)$$

Par adjonction des racines n-ièmes, nous construisons l'extension $L = N(\mathbb{U}_n)$. Nous connaissons fort bien le groupe de Galois de L/N car l'extension $N/\mathbb{Q}$ est régulière. Il s'agit de

$$\Gamma' = \mathrm{Gal}_{\mathbb{Q}}\, \mathbb{Q}(\mathbb{U}_n) = \mathrm{U}(\mathbb{Z}/n\mathbb{Z})$$

De plus, nous savons que l'extension L/K est galoisienne, de groupe de Galois

$$\Gamma = \Gamma_0 \times \Gamma' \ \subset \ \mathrm{U}(\mathbb{Z}/n\mathbb{Z}) \times \mathrm{U}(\mathbb{Z}/n\mathbb{Z})$$

Remarquer que Γ est un groupe commutatif (L/K est donc abélienne). L'action de Γ_0 sur $\mathbb{Z}/n\mathbb{Z}$ est étendue à Γ où seule la première coordonnée opère : si $\gamma = (\gamma_0, \gamma') \in \Gamma$ et $x \in \mathbb{Z}/n\mathbb{Z}$, alors $\gamma.x = \gamma_0 x \in \mathbb{Z}/n\mathbb{Z}$.

Pour trouver un sous-groupe A' de L^*/L^{*n} isomorphe à $\mathbb{Z}/n\mathbb{Z}$, il suffit de choisir un élément primitif de L/K, entier sur $\mathbb{Z}[t]$, et dont la norme est divisible une seule fois par un polynôme irréductible $p \in \mathbb{Z}[t]$ non ramifié dans L. Sous ces conditions, le premier p est totalement décomposé dans L, et cet élément primitif est d'ordre n dans le quotient L^*/L^{*n} (voir la section IV.8).

> Remarque 1. Pour que p ne soit pas ramifié dans L, il suffit qu'il ne le soit ni dans N, ni dans $K(\mathbb{U}_n)$, car L est le compositum de N et $K(\mathbb{U}_n)$.
>
> Pour que $p \in \mathbb{Z}[t]$ ne soit pas ramifié dans $N = \mathbb{Q}(t)[X]/(f_0)$, il suffit que p ne divise pas $\mathrm{dis}(f_0)$.
>
> Pour que p ne soit pas ramifié dans $K(\mathbb{U}_n)$, il suffit qu'il soit non constant. En effet, le discriminant du n-ième polynôme cyclotomique Φ_n est une constante de $\mathbb{Z}$, et un polynôme non constant ne peut pas en être diviseur...
>
> Remarque 2. Si x est un élément primitif de l'extension galoisienne N/K régulière sur $\mathbb{Q}$ (par exemple, une racine de f_0) et ϵ un élément primitif de l'extension galoisienne $\mathbb{Q}(\mathbb{U}_n)/\mathbb{Q}$ (par exemple une racine primitive n-ième de l'unité), alors $x+\epsilon$ est un élément primitif de $L = N(\mathbb{U}_n)$ sur $K = \mathbb{Q}(t)$ (voir le lemme IV.4.1, page 118).

Une fois $A' \subset L^*/L^{*n}$ construit, il faut réaliser l'extension cyclique E (notation du diagramme page 137, repris ci-dessous). Pour cela, il est nécessaire de transporter l'action (de multiplication) de Γ sur $\mathbb{Z}/n\mathbb{Z}$ en une action isomorphe de Γ sur $\mathbb{U}_n = (\mathbb{Z}/n\mathbb{Z})^\bullet$, puis déterminer l'action ρ' (l'action contragrédiente...) de Γ sur $\mathbb{Z}/n\mathbb{Z}$ telle que $(\mathbb{Z}/n\mathbb{Z})_\rho$ et $(\mathbb{U}_n)_{\rho'\bullet}$ soient des Γ-modules isomorphes (voir la section IV.8.b).

$$\Gamma \ \subset \ \mathrm{U}(\mathbb{Z}/n\mathbb{Z}) \times \mathrm{U}(\mathbb{Z}/n\mathbb{Z})$$

$$\begin{array}{rccc} \rho \ : & \Gamma & \longrightarrow & \mathrm{Aut}\ \mathbb{Z}/n\mathbb{Z} \\ & (\gamma_0, \gamma') & \longmapsto & [x \mapsto \gamma_0 x] \end{array}$$

$$\begin{array}{rcl} \Gamma & \longrightarrow & \mathrm{Aut}(\mathbb{U}_n) = \mathrm{Aut}\ (\mathbb{Z}/n\mathbb{Z})^\bullet \\ (\gamma_0, \gamma') & \longmapsto & [w \mapsto w^{\gamma_0}] \end{array}$$

$$\begin{array}{rccl} \rho' : & \Gamma & \longrightarrow & \mathrm{Aut}\ \mathbb{Z}/n\mathbb{Z} \\ & (\gamma_0, \gamma') & \longmapsto & [x \mapsto -\gamma_0 x] \end{array}$$

L'action ρ' est donc très simple, et il est facile de déterminer l'extension E/L :

$$E = L\big(\{d_a^{\frac{1}{n}} \mid a \in A'\}\big) \qquad \text{avec} \qquad d_a = \prod_{(\gamma_0,\gamma') \in \Gamma_0 \times \Gamma'} \gamma_0\gamma'.a^{\langle \gamma_0 \gamma'^{-1} \rangle}$$

où $\langle \lambda \rangle$ désigne un représentant dans $\{0, \ldots, n-1\}$ de la classe de λ modulo n. Nous noterons e_a une racine n-ième quelconque de d_a :

$$e_a = d_a^{\frac{1}{n}}$$

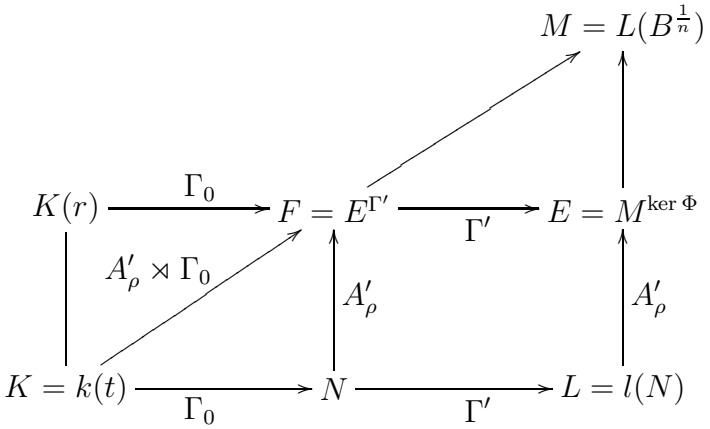
La théorie de Kummer nous rappelle plusieurs faits : les éléments $(e_a)_{a \in A'}$ forment une base de l'espace vectoriel E/L. De plus, a est un générateur du groupe $A' \subset L^*/L^{*n}$ si et seulement si e_a est un élément primitif de l'extension E/L.

La section IV.7 nous permet d'affirmer que E est une extension galoisienne du corps $K = \mathbb{Q}(t)$, de groupe de Galois $\mathbb{Z}/n\mathbb{Z} \rtimes \Gamma$. Nous savons que $F = E^{\Gamma'}$ est une extension galoisienne de $K = \mathbb{Q}(t)$ de groupe $\mathbb{Z}/n\mathbb{Z} \rtimes \Gamma_0$ (voir le diagramme ci-dessous).

De plus, la section IV.8.c nous prouve que l'extension $F/\mathbb{Q}$ est régulière si le polynôme irréductible $p \in \mathbb{Z}[t]$ est séparable... ce qui est évidemment vrai puisque $\mathbb{Z}$ est de caractéristique 0 !

Construction d'un polynôme régulier sur $\mathbb{Q}$, de degré n, réalisant $\mathbb{Z}/n\mathbb{Z} \rtimes \Gamma_0$

Maintenant, il faut exhiber un élément $r \in F = E^{\Gamma'}$, de degré n sur $K = \mathbb{Q}(t)$, entier sur $\mathbb{Z}[t]$ de préférence, tel que la clôture galoisienne de l'extension $K(r)/K$ soit exactement $F = E^{\Gamma'}$.



Considérons un élément primitif $e_a \in E$ sur L (a est donc un générateur du groupe cyclique $A' \subset L^*/L^{*n}$), ainsi que sa trace sur F :

$$r_a = \mathrm{tr}_{E/F}(e_a) = \sum_{\tau \in \Gamma'} \tau.e_a$$

Bien sûr, r_a appartient à $E^{\Gamma'}$ par définition. Mais en réalité, il est invariant par $\Gamma = \Gamma_0 \times \Gamma'$ tout entier : soit $\sigma \in \Gamma_0 \subset \mathrm{U}(\mathbb{Z}/n\mathbb{Z})$ et $\tau \in \Gamma' = \mathrm{U}(\mathbb{Z}/n\mathbb{Z})$, le lecteur pourra facilement démontrer par un calcul élémentaire cette égalité :

$$\sigma.\tau.e_a = \tau'.e_a \qquad \text{avec} \qquad \tau' = \sigma^{-1}\tau \in \mathrm{U}(\mathbb{Z}/n\mathbb{Z}) = \Gamma'$$

En clair, l'orbite de e_a sous l'action de Γ' est stable sous l'action de Γ_0. Comme r_a est la somme des éléments de $\Gamma'.e_a$, finalement r_a est invariant par $\Gamma = \Gamma_0 \times \Gamma'$.

Ainsi, r_a appartient à E^{Γ}. Son degré sur K est donc n au maximum. Montrons qu'il est exactement égal à n. Nous allons même montrer que r_a est un élément primitif de l'extension E/L. Soit $\tau \in \Gamma'$, alors visiblement on a

$$\tau.e_a = e_{\tau.a}$$

> Remarque. L'orbite de e_a sous l'action Γ' forme une famille libre dans l'espace vectoriel E/L (théorie de Kummer).

Comme a est un générateur de A' construit à partir de la méthode de la section IV.8.a, cet élément engendre l'extension L/K. Les Γ-conjugués de a sont par conséquent tous distincts. Ainsi, $\tau.a = a$ implique $\tau = \mathrm{Id} \in \Gamma'$.

Soit $g \in \mathrm{Gal}_L E$, alors

$$g(r_a) = \sum_{\tau \in \Gamma'} g(e_{\tau.a}) = \sum_{\tau \in \Gamma'} w_\tau e_{\tau.a}$$

où w_τ est un élément de $\mathbb{U}_n$. L'égalité $g(r_a) = r_a$ implique toutes les égalités $w_\tau = 1$ à la fois, car les $(e_{\tau.a})_{\tau \in \Gamma'}$ forment une famille libre sur E/L et $\mathbb{U}_n \subset L$. En particulier, $g \in \mathrm{Gal}_L L(e_a)$ est le morphisme identité puisqu'il envoie e_a sur lui-même. Ainsi le stabilisateur de r_a dans $\mathrm{Gal}_L E$ est $\{\mathrm{Id}\}$, donc

$$E = L(r_a)$$

Finalement r_a est de degré n sur L, donc de degré n sur $K = \mathbb{Q}(t)$. Autrement dit,

$$K(r_a) = E^{\Gamma} = F^{\Gamma_0}$$

Montrons enfin que la clôture galoisienne de $K(r)/K$ est bien F. Pour cela, nous utilisons le lemme suivant :

Lemme IV.9.1 *Supposons qu'un groupe G opère sur un autre groupe A (ces groupes ne sont pas nécessairement commutatifs). Alors l'intersection des conjugués de G dans le produit semi-direct $A \rtimes G$ est réduite au noyau du morphisme $\rho : G \to \mathrm{Aut}(A)$.*

Démonstration Il suffit de prouver $\bigcap_{a\in A} aGa^{-1} = \ker(\rho)$. Or, l'égalité

$$G \ni aga^{-1} = a\ \rho(g).a^{-1}\ g \qquad\qquad \forall\ a \in A$$

implique en premier lieu $a\ \rho(g).a^{-1} \in A \cap G = \{1\} \quad \forall\ a \in A$, d'où $a = \rho(g).a \quad \forall\ a \in A$, et finalement $g \in \ker(\rho)$.

L'inclusion réciproque est évidente puisque les éléments de $\ker(\rho)$ commutent avec ceux de A et $\ker(\rho)$ est un sous-groupe distingué de G. □

Comme l'action de Γ_0 sur $\mathbb{Z}/n\mathbb{Z} \simeq \mathrm{Gal}_N F$ est fidèle, l'intersection des conjugués de Γ_0 dans $\mathrm{Gal}_K F = \mathbb{Z}/n\mathbb{Z} \rtimes \Gamma_0$ est réduit à $\{\mathrm{Id}\}$. Nous pourrions également dire que le plus gros sous-groupe de Γ_0, normal dans $\mathrm{Gal}_K F$ est $\{\mathrm{Id}\}$. Ainsi la clôture galoisienne de $K(r_a) = F^{\Gamma_0}$ est exactement F.

Le polynôme minimal de r_a sur K est donc un polynôme de degré n, réalisant régulièrement le produit semi-direct $\mathbb{Z}/n\mathbb{Z} \rtimes \Gamma_0$.

IV.9.b Résultats numériques

Pour réaliser $\mathrm{AGL}_1(\mathbb{F}_5) = \mathbb{F}_5 \rtimes \mathbb{F}_5^*$, nous avons choisi le polynôme

$$f_0 = X^4 - 4(t^2+1)X^2 + 4(t^2+1)$$

afin de construire régulièrement $\mathbb{F}_5^* \simeq \mathbb{Z}/4\mathbb{Z}$ sur $\mathbb{Q}(t)$ (voir [64]). Si x est un zéro de ce polynôme, alors

$$x \quad , \quad -x \quad , \quad x^3/2t - (2t^2+1)x/t \quad , \quad -x^3/2t + (2t^2+1)x/t$$

en sont les quatre racines (valeurs obtenues grâce à un petit calcul dans l'algèbre de décomposition universelle de f_0 sur $\mathbb{Q}(t)$).

On choisit alors $a = x + \epsilon$ comme élément primitif de L/K. Les conjugués de d_a, e_a et r_a peuvent être calculés plus ou moins facilement... et le polynôme minimal sur $\mathbb{Q}(t)$ de ce dernier est

$$\begin{aligned}\mathrm{AGL}_1(\mathbb{Z}/5\mathbb{Z})\ : & X^5 - 10pX^3 + 20(20t^2+19)pX^2 \\ & +5p(6400t^8 + 17600t^6 + 1280t^5 + 15680t^4 + 2240t^3 \\ & \quad +4080t^2 + 960t - 403)X \\ & -4p(25600t^{10} + 51200t^9 + 115200t^8 + 185600t^7 + 203200t^6 \\ & \quad +251520t^5 + 173120t^4 + 150960t^3 + 69780t^2 + 33840t + 10261)\end{aligned}$$

$$\text{avec } p = 1280t^8 + 4800t^6 + 6720t^4 + 4160t^2 + 961$$

Pour réaliser $\mathrm{AGL}_1(\mathbb{Z}/10\mathbb{Z}) \simeq \mathbb{Z}/10\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$, nous avons choisi le polynôme

$$f_0 = X^4 + tX^3 - 6X^2 - tX + 1$$

Celui-ci réalise régulièrement également le groupe cyclique d'ordre 4 (voir [56]). Si x est en un zéro alors les 4 racines de ce polynôme sont

$$x \quad , \quad -x^3/2 - (t+1)x^2/2 + (5-t)x/2 + 3/2 \quad ,$$

$$x^3 + tx^2 - 6x - t \quad , \quad -x^3/2 + (1-t)x^2/2 + (5+t)x/2 - 3/2$$

Le polynôme minimal de r_a est donné par :

$$\begin{aligned}
\mathrm{AGL}_1(\mathbb{Z}/10\mathbb{Z}) \ : & X^{10} - 20pX^8 + 10p(60t^4 + 40t^3 + 2195t^2 + 640t + 19767)X^6 \\
& -25p(225t^8 + 1000t^7 + 15600t^6 + 49200t^5 + 404220t^4 \\
& \quad +806720t^3 + 4639880t^2 + 4408320t + 19909764)X^4 \\
& +5p(2250t^{12} + 24000t^{11} + 334500t^{10} + 2112000t^9 + 16896075t^8 \\
& \quad +73734800t^7 + 407987775t^6 + 1278232800t^5 + 5120377780t^4 \\
& \quad +11013808400t^3 + 31889578615t^2 + 37764870400t + 76233237373)X^2 \\
& -p(25t^8 - 500t^7 - 1400t^6 - 23200t^5 - 96715t^4 - 358220t^3 - 1608970t^2 \\
& \quad -1840320t - 8357276)^2 \\
& \\
& \text{avec } p = 5t^4 + 185t^2 + 1681
\end{aligned}$$

IV.9.c Encore des polynômes d'Eisenstein...

Visiblement, les polynômes obtenus sont des polynômes d'Eisenstein pour le premier $p \in \mathbb{Z}[t] \subset \mathbb{Q}[t]$ qui est précisé à chaque fois. On peut effectivement montrer qu'il en est toujours ainsi.

Par construction de p, nous savons qu'il est totalement décomposé dans l'anneau des entiers sur $\mathbb{Q}[t]$ de L (voir le lemme IV.8.2) : il existe un idéal premier $\mathcal{P}$ de L tel que

$$(p) = \prod_{\gamma \in \Gamma} \gamma.\mathcal{P}$$

Par conséquent la valuation en $\mathcal{P}$ dans l'extension L est un prolongement de celle en p dans $K = \mathbb{Q}(t)$. De plus, l'élément $a \in L$ (entier sur $\mathbb{Q}[t]$) possède la propriété suivante (voir le lemme IV.8.2) :

$$v_{\tau.\mathcal{P}}(\gamma(a)) = \delta_{\tau,\gamma} \qquad \forall\ \tau, \gamma \in \Gamma$$

où $v_{\tau.\mathcal{P}}$ désigne la valuation en le premier $\tau.\mathcal{P}$.

L'extension E est définie par $E = L(e_a)$, où le polynôme minimal de e_a est $X^n - d_a$ avec

$$d_a = \prod_{(\gamma_0,\gamma') \in \Gamma_0 \times \Gamma'} \gamma_0\gamma'.a^{\langle(\gamma_0\gamma')^{-1}\rangle}$$

Ce polynôme $X^n - d_a$ est un polynôme d'Eisenstein pour l'idéal premier $\mathcal{P}$. En effet, parmi ses conjugués $\gamma_0\gamma'.a$, seul a appartient à $\mathcal{P}$. De plus, l'exposant de a dans l'écriture

de d_a est 1, donc la valuation en $\mathcal{P}$ de d_a est exactement 1 : $X^n - d_a$ vérifie bien le critère d'Eisenstein avec l'idéal premier $\mathcal{P}$.

L'idéal premier $\mathcal{P}$ est alors totalement ramifié dans l'extension $E = L(e_a)$ (voir [52], page 30). Soit $\mathfrak{M}$ l'unique idéal premier de E au-dessus de $\mathcal{P}$: $\mathcal{P} = \mathfrak{M}^n$. La valuation $v_{\mathcal{P}}$ en $\mathcal{P}$ de L se prolonge donc en $\frac{1}{n}v_{\mathfrak{M}}$ sur E. Ainsi, nous avons

$$\begin{array}{l} v_{\mathcal{P}}(\tau.d_a) = \langle\tau\rangle \in \{0,\ldots,n-1\} \\ v_{\mathfrak{M}}(\tau.e_a) = \langle\tau\rangle \end{array} \qquad \forall\ \tau \in \Gamma' = \mathrm{U}(\mathbb{Z}/n\mathbb{Z})$$

Comme les valeurs $\langle\tau\rangle$ sont toutes différentes quand τ parcourt $\Gamma' = \mathrm{U}(\mathbb{Z}/n\mathbb{Z})$, nous avons

$$v_{\mathfrak{M}}(r_a) = v_{\mathfrak{M}}\left(\sum_{\tau\in\Gamma'} \tau.e_a\right) = \min_{\tau\in\Gamma'} \langle\tau\rangle = 1$$

Le polynôme minimal de r_a sur L est nécessairement un polynôme d'Eisenstein pour le premier $\mathcal{P}$ (voir [52], pages 30-31) : r_a est une uniformisante dans le localisé en $\mathfrak{M}$ de l'anneau des entiers de E sur $\mathbb{Q}[t]$.

Enfin, nous rapellons que le polynôme minimal de r_a sur L est à coefficients dans le corps $K = \mathbb{Q}(t)$, plus précisément dans l'anneau intégralement clos $\mathbb{Z}[t]$ car r_a est entier sur $\mathbb{Z}[t]$. De plus, nous avons vu que la valuation en $\mathcal{P}$ prolonge celle de p. Nous concluons :

Propriété IV.9.1 *Le polynôme minimal de r_a sur $K = \mathbb{Q}(t)$ est donc un polynôme à coefficients dans $\mathbb{Z}[t]$, d'Eisenstein pour le premier $p \in \mathbb{Z}[t]$.*

Chapitre A

Algorithme de Bareiss

L'étude des algorithmes de Bareiss et des sous-résultants amène à penser à l'existence d'un lien entre ces méthodes, bien qu'assez différentes par les objets qu'elles manipulent. Dans un premier temps, on étudiera la méthode de Bareiss "pas à pas" afin de donner naissance de façon naturelle à quelques formules simples d'algèbre multilinéaire.

En fait, aborder l'algorithme de Bareiss est un prétexte pour développer un certain formalisme non traditionnel. Celui-ci permet de traiter avec un certain systématisme les relations que l'on rencontre dans ce chapitre (relations de Sylvester) et surtout celles données dans le chapitre B sur les sous-résultants.

A.1 L'élimination de Gauss et l'application $\natural$

Soit R un anneau commutatif intègre et M un R-module libre muni d'une base fixée. On note π_i la projection sur la $i^{ème}$ coordonnée et $\Omega^n(M)$ le R-module des n-linéaires alternées de M dans R (que l'on nommera n-formes).

Étant donnés w, x, y, z quatre vecteurs de M, si l'on veut annuler la première coordonnée des vecteurs x, y, z par une élimination "à la Gauss" en se servant de w, la combinaison la plus simple est :

$$x' = \pi_1(w)x - \pi_1(x)w \qquad y' = \pi_1(w)y - \pi_1(y)w \qquad z' = \pi_1(w)z - \pi_1(z)w$$

Ces combinaisons font apparaître une 2-application (application 2-linéaire alternée)

$$\pi_1^{\natural} \ : \ (a,b) \in M^2 \mapsto \pi_1(a)b - \pi_1(b)a \in M$$

> Rappel. Si $g \in \Omega^n(M)$ et $f \in \Omega^m(M)$ sont deux formes multilinéaires alternées, on définit le produit extérieur de g et f (noté $g \wedge f$) par :
>
> $$(v_1, \dots, v_{n+m}) \in M^{n+m} \mapsto \sum_{\sigma} \operatorname{sgn}(\sigma) g(v_{\sigma_1}, \dots, v_{\sigma_n}) f(v_{\sigma_{n+1}}, \dots, v_{\sigma_{n+m}})$$
>
> où la somme porte sur les permutations σ de $\mathcal{S}_{n+m}$ telles que
>
> $$\sigma_1 < \sigma_2 < \cdots < \sigma_n \qquad \text{et} \qquad \sigma_{n+1} < \cdots < \sigma_{n+m}$$
>
> On voit bien que l'on peut prendre pour $f : M^m \to N$ une *application* multilinéaire alternée tout en laissant la formule ci-dessus bien définie.

Définition A.1.1 *Soit $g \in \Omega^n(M)$ et $f : M^m \to N$ une application multilinéaire alternée, on définit le* ***produit extérieur*** *$g \wedge f$ par :*

$$M^{n+m} \to N \ : \quad (v_1, \ldots, v_{n+m}) \mapsto \sum_{\sigma} \mathrm{sgn}(\sigma) g(v_{\sigma_1}, \ldots, v_{\sigma_n}) f(v_{\sigma_{n+1}}, \ldots, v_{\sigma_{n+m}})$$

Par cette extension du produit extérieur, on a :

$$\pi_1^\natural = \pi_1 \wedge \mathrm{Id}_M$$

Si l'on réalise une étape supplémentaire pour éliminer la seconde coordonnée de y', z', on combine :

$$y'' = \pi_2(x')y' - \pi_2(y')x' = \pi_2^\natural(x', y') \qquad z'' = \pi_2(x')z' - \pi_2(z')x' = \pi_2^\natural(x', z')$$

et on s'aperçoit (la démonstration sera faite dans le paragraphe A.2.a page 156, relation A.1) que $y'' = \pi_1(w)\mu(w, x, y)$ et $z'' = \pi_1(w)\mu(w, x, z)$ où μ est la 3-application suivante :

$$(a, b, c) \in M^3 \mapsto \begin{vmatrix} \pi_1(a) & \pi_1(b) \\ \pi_2(a) & \pi_2(b) \end{vmatrix} c - \begin{vmatrix} \pi_1(a) & \pi_1(c) \\ \pi_2(a) & \pi_2(c) \end{vmatrix} b + \begin{vmatrix} \pi_1(b) & \pi_1(c) \\ \pi_2(b) & \pi_2(c) \end{vmatrix} a$$

Si l'on pose $\det_{\left[\begin{smallmatrix}1\\2\end{smallmatrix}\right]} = \pi_1 \wedge \pi_2 \ : \ (a, b) \in M^2 \mapsto \begin{vmatrix} \pi_1(a) & \pi_1(b) \\ \pi_2(a) & \pi_2(b) \end{vmatrix}$, et si l'on se permet l'extension du produit extérieur, on obtient alors :

$$\mu = \det_{\left[\begin{smallmatrix}1\\2\end{smallmatrix}\right]} \wedge \mathrm{Id}_M = \det^\natural_{\left[\begin{smallmatrix}1\\2\end{smallmatrix}\right]}, \qquad \frac{y''}{\pi_1(w)} = \det^\natural_{\left[\begin{smallmatrix}1\\2\end{smallmatrix}\right]}(w, x, y), \qquad \frac{z''}{\pi_1(w)} = \det^\natural_{\left[\begin{smallmatrix}1\\2\end{smallmatrix}\right]}(w, x, z)$$

C'est en utilisant ce genre de propriétés de divisibilité que E.H. Bareiss démontre dans [7] comment calculer le déterminant d'une matrice, à condition de pouvoir diviser par certaines valeurs ($\pi_1(w)$ par exemple). Le lecteur pourra aussi consulter [20] (pages 389 à 405) pour plus de détails sur la méthode de Bareiss et des améliorations possibles.

On voit maintenant la nécessité de définir une transformation $g \mapsto g^\natural$. On en ébauchera quelques propriétés avant de continuer l'étude de la méthode de Gauss.

Notation : Si $x \in M^n$ alors $x_i \in M$ désigne sa $i^{ème}$ composante.

Définition A.1.2 *Si $g \in \Omega^{n-1}(M)$ est une $(n-1)$-**forme** de M alors on note $g^\natural$ la n-**application***

$$\begin{array}{rccl} g \wedge \mathrm{Id}_M \ : & M^n & \longrightarrow & M \\ & v & \longmapsto & \displaystyle\sum_{i=1}^{n} (-1)^{n-i} g(v_1, \ldots, \not{v}_i, \ldots, v_n) v_i \end{array}$$

Propriété A.1.1 *Si $f \in \Omega^m(M)$ et $g \in \Omega^n(M)$, on a*

$$(f \wedge g)^\natural = f \wedge g^\natural \qquad g \wedge f^\natural = (-1)^{mn} f \wedge g^\natural$$

Si $f \ : \ M \mapsto N$ est un morphisme de R-modules alors $f \circ g^\natural = g \wedge f$.

Remarquer que $g^\natural$ est la seule application vérifiant la dernière relation pour toute f (g étant fixée).

A.2 L'algorithme...

A.2.a Un (tout petit) peu d'algèbre extérieure

Définition A.2.1 *Si g est une application multilinéaire alternée de M^n sur un R-module (en particulier si g est une n-forme multilinéaire alternée de M), on nomme* $\ker g$ *le sous-module formé des éléments de M qui annulent g dès qu'ils font partie de ses arguments.*

Exemple et contre-exemple : Le vecteur $(0,0,1)$ fait partie de $\ker(\pi_1 \wedge \pi_2)$, mais n'est pas élément de $\ker(\pi_2 \wedge \pi_3)$.

Propriété A.2.1 *Soit f une m-application et g une n-forme sur M. Alors*

$$\ker g \cap \ker f \subset \ker(g \wedge f)$$

Le théorème suivant est inspiré de ce qu'expose C. Quitté dans [49].

Théorème A.2.1 *Soit M et N deux R-modules, $f : M^{n+1} \to N$ une $(n+1)$-application et $g \in \Omega^{m-1}(M)$. On considère $x \in M^m$, $z \in M^n$ tels que $\forall\ j \in \{1,\dots,n\}$, $z_j \in \ker g$. Alors on a :*

$$f(g^\natural(x), z) = (g \wedge f)(x, z).$$

Démonstration

$$\begin{aligned}
(g \wedge f)(x,z) &= \sum_{i=1}^{m} (-1)^{m-i} g(x_1, \dots, \not{x}_i, \dots, x_m) f(x_i, z) \qquad \text{car } \forall\ j,\ z_j \in \ker g, \\
&= f\left(\sum_{i=1}^{m} (-1)^{m-i}\ g(x_1, \dots, \not{x}_i, \dots, x_m).x_i, z \right) \quad \text{par linéarité de } f, \\
&= f(g^\natural(x), z).
\end{aligned}$$

□

Définition A.2.2 *On dit que g est une n-**forme pure** si g est le produit extérieur de n 1-formes.*

Théorème A.2.2 *Si g est une n-forme pure alors* $\operatorname{im} g^\natural \subset \ker g$.

Démonstration On a $g = g_1 \wedge g_2 \wedge \cdots \wedge g_n$ où g_i est une forme linéaire de M sur R, donc $\forall\ i,\ g_i \circ g^\natural = g \wedge g_i = 0$ et comme $g = g_1 \wedge g_2 \wedge \cdots \wedge g_n$, on a bien le résultat annoncé car :

$$\operatorname{im} g^\natural \subset \bigcap \ker g_i \subset \ker\left(\bigwedge g_i\right) = \ker g$$

□

Par exemple, en prenant f une 2-application de M dans N et g une n-forme pure de M, $w \in M^n$ et $x, y \in M$, grâce au théorème A.2.2 on a $g^\natural(w,y) \in \ker g$ et grâce au théorème A.2.1 on obtient :

$$f\left(g^\natural(w,x), g^\natural(w,y)\right) = (g \wedge f)(w, x, g^\natural(w,y))$$

Comme $g \wedge f$ est alternée, seul le terme $g(w).y$ de $g^\natural(w,y)$ n'est pas éliminé par les composantes de w :

$$(g \wedge f)(w, x, g^\natural(w,y)) = (g \wedge f)(w, x, g(w)y - g(y)w) = (g \wedge f)(w, x, g(w)y)$$

On a maintenant :

$$f\left(g^\natural(w,x), g^\natural(w,y)\right) = g(w)(g \wedge f)(w,x,y) \tag{A.1}$$

Si l'on pose $f = \pi_2^\natural$ et $g = \pi_1$ et que l'on reprend la deuxième élimination "à la Gauss" de la page 154, cette relation devient :

$$y'' = \pi_2^\natural\left(\pi_1^\natural(w,x), \pi_1^\natural(w,y)\right) = \pi_1(w)(\pi_1 \wedge \pi_2^\natural)(w,x,y) = \pi_1(w)\det{}^\natural_{\left[\begin{smallmatrix}1\\2\end{smallmatrix}\right]}(w,x,y)$$

(et de même avec z'', w, x, z) ce qui prouve (comme il était annoncé) que $\mu = \det^\natural_{\left[\begin{smallmatrix}1\\2\end{smallmatrix}\right]}$.

On divise y'' et z'' par $\pi_1(w)$ (le pivot de la première étape) et on appelle de nouveau ces quotients exacts y'' et z'' pour simplifier. En réitérant une dernière fois l'élimination "à la Gauss" avec y'' et z'', grâce aux théorèmes A.2.1 et A.2.2, on a :

$$\begin{aligned}\pi_3^\natural(y'', z'') &= \pi_3^\natural\big(\det^\natural_{\left[\begin{smallmatrix}1\\2\end{smallmatrix}\right]}(w,x,y), \det^\natural_{\left[\begin{smallmatrix}1\\2\end{smallmatrix}\right]}(w,x,z)\big)\\ &= \det^\natural_{\left[\begin{smallmatrix}1\\3\end{smallmatrix}\right]}\big(w,x,y,\det^\natural_{\left[\begin{smallmatrix}1\\2\end{smallmatrix}\right]}(w,x,z)\big) = \det_{\left[\begin{smallmatrix}1\\2\end{smallmatrix}\right]}(w,x)\det^\natural_{\left[\begin{smallmatrix}1\\3\end{smallmatrix}\right]}(w,x,y,z)\end{aligned}$$

où $\det^\natural_{\left[\begin{smallmatrix}1\\3\end{smallmatrix}\right]} = \det_{\left[\begin{smallmatrix}1\\2\end{smallmatrix}\right]} \wedge \pi_3^\natural = \pi_1 \wedge \pi_2 \wedge \pi_3 \wedge \mathrm{Id}$.

On voit que $\pi_3^\natural(y'', z'')$ est divisible par $\det_{\left[\begin{smallmatrix}1\\2\end{smallmatrix}\right]}(w,x) = \pi_2(\pi_1^\natural(w,x))$ (le pivot de la deuxième étape) et le résultat d'une telle division est $\det^\natural_{\left[\begin{smallmatrix}1\\3\end{smallmatrix}\right]}(w,x,y,z)$. On comprend alors comment le processus se poursuit avec un nombre de vecteurs plus importants.

Principe de l'algorithme de Bareiss A l'aide des seules applications $\pi_i^\natural$, on peut calculer le déterminant d'une matrice. Pour ce faire, après chaque combinaison

$$\pi_i^\natural \ : \ (x,y) \mapsto x_i y - y_i x$$

de deux vecteurs colonnes de l'étape i, on divise par le pivot de l'étape précédente afin de réduire au plus tôt la taille des coefficients des vecteurs tout en restant dans le module M.

A.2.b La preuve de l'algorithme

Le lecteur trouvera dans [7] ou [20] des démonstrations de l'algorithme ébauché ci-dessus. La démonstration exposée ici est différente et donne une vision vectorielle sur l'algorithme : ce ne sont plus les coefficients de la matrice qui sont étudiés, mais les vecteurs colonnes qui la composent.

Notations : On note $\left[\begin{smallmatrix}i\\j\end{smallmatrix}\right]$ la liste ordonnée $\{i, i-1, \dots, j+1, j\}$ si $i \geq j$, ou l'ensemble vide si $i < j$. Si K est une liste ordonnée $\{a, b, c, \dots, z\}$, on pose :

$$\det{}_K = \pi_a \wedge \pi_b \wedge \pi_c \wedge \cdots \wedge \pi_z$$

et par exemple, si $i \geq j$:

$$\det{}_{\left[\begin{smallmatrix}i\\j\end{smallmatrix}\right]} = \pi_i \wedge \cdots \wedge \pi_j \qquad \det^\natural_\emptyset = \mathrm{Id}_M$$

Remarquer que la typographie n'est pas innocente : $\det_{\left[\begin{smallmatrix} i \\ j \end{smallmatrix}\right]}$ est un déterminant dont la première ligne correspond à la projection π_i,... la dernière à π_j.
Encore un petit exemple... $\pi_1 \circ \det^\natural_{\left[\begin{smallmatrix} n \\ 2 \end{smallmatrix}\right]} = \det_{\left[\begin{smallmatrix} n \\ 2 \end{smallmatrix}\right]} \wedge \pi_1 = \det_{\left[\begin{smallmatrix} n \\ 1 \end{smallmatrix}\right]}$

Soit $(f_i)_{i\geq 1}$ une suite de 1-formes. On pose $g_i = f_1 \wedge f_2 \wedge \cdots \wedge f_i$ (g_i est donc pure). Par convention $g_0^\natural = \mathrm{Id}_M$. On choisit $X \in M^i$ ainsi que $y, z \in M$. On a alors pour $i \geq 1$:

$$\begin{aligned} f_{i+1}^\natural \left(g_i^\natural(X,y), g_i^\natural(X,z) \right) &= g_i(X)\ (g_i \wedge f_{i+1}^\natural)(X,y,z) \qquad \text{relation A.1} \\ &= (g_{i-1} \wedge f_i)(X)\ g_{i+1}^\natural(X,y,z) \\ &= f_i(g_{i-1}^\natural(X))\ g_{i+1}^\natural(X,y,z). \end{aligned}$$

Pour obtenir une preuve *complète* de l'algorithme de Bareiss (appliqué à une matrice A de dimension $d \times d$), il faudra poser : pour tout $i \in \{1, \ldots, d\}$, A_i est la sous-matrice de A formée par ses i premiers vecteurs colonnes, $f_i = \pi_{\alpha_i}$ (et donc $g_i = \pi_{\alpha_1} \wedge \cdots \wedge \pi_{\alpha_i}$) en choisissant $\alpha_i \in \{1, \ldots, d\} - E_{i-1}$ (où $E_{i-1} = \{\alpha_1, \ldots, \alpha_{i-1}\}$) tel que $\pi_{\alpha_i}(g_{i-1}^\natural(A_i))$ (le pivot de l'étape i) soit non nul. Dans le cas où un tel α_i n'existe pas, on conclut : $\det(A) = 0$ car les vecteurs de A_i sont liés. Si un tel α_i existe, en posant $X = A_i$, la dernière formule donne alors pour $i \geq 1$:

$$\frac{\pi_{\alpha_{i+1}}^\natural \left(\det_{E_i}^\natural(A_i, y), \det_{E_i}^\natural(A_i, z) \right)}{\pi_{\alpha_i}(\det_{E_{i-1}}^\natural(A_i))} = \det_{E_{i+1}}^\natural(A_i, y, z) = \det_{E_{i+1}}^\natural(A_{i+1}, z)$$

où y est le $(i+1)^{ième}$ vecteur colonne de A, (colonne du pivot de l'étape $i+1$) et z un autre vecteur colonne de A.

A l'étape $d-1$, on voit que l'on calcule $\det_{E_{d-1}}^\natural(A)$. On peut connaître alors le déterminant de A car :

$$\pi_{\alpha_d}(\det_{E_{d-1}}^\natural(A)) = \det_{E_{d-1}} \wedge \pi_{\alpha_d}(A) = \mathrm{sgn}(i \mapsto E_i) \det(A).$$

Voici l'algorithme calculant le déterminant d'une matrice par la méthode de Bareiss décrite ci-dessus.

Algorithme de Bareiss.
Donnée : $A = (x_1, x_2, \ldots, x_d) \in \mathcal{M}_d(R)$
Résultat : $\det(A)$

$E \leftarrow [\,]$; $oldpivot \leftarrow 1$
for i in $1 \ldots d-1$ loop
  if $x_i = 0$ then return 0
  $(k, pivot) :=$ `aComponentOf`(x_i) — ici, $pivot = \pi_k(x_i) \neq 0$ —
  $E := E \cup [k]$
  for j in $i+1 \ldots d$ loop
    $$x_j \leftarrow \frac{pivot \times x_j - \pi_k(x_j) \times x_i}{oldpivot}$$
  end loop
  $oldpivot \leftarrow pivot$
end loop — ici, $\forall\ j > i,\ \forall\ e \in E,\ \pi_e(x_j) = 0$ —
— ici, $|E| = d-1$ —
for j in $1 \ldots d$ loop
  if $j \notin E$ then return `signature`$(E \cup [j]) \times \pi_j(x_d)$
end loop

Dans l'algorithme ci-dessus, on utilise deux fonctions qui sont `aComponentOf` et `signature` : `aComponentOf` prend en argument un vecteur x non nul et renvoie le couple formé respectivement par le numéro et la valeur d'une coordonnée non nulle de x ; la fonction `signature` calcule la signature de la permutation $i \mapsto E_i$.

A.3 La meilleure élimination

A.3.a Dans un module

Annuler $m-1$ composantes en combinant m vecteurs est l'élimination maximale à laquelle on peut s'attendre dans le cas général : on ne peut pas annuler m composantes dans tous les cas, car alors m vecteurs de dimension m seraient toujours liés. De plus si K est une liste d'entiers de cardinal $m-1$, alors $\det_K^\natural$ combine m vecteurs quelconques de manière à annuler les coordonnées indexées par K. La propriété A.1.1 nous le prouve si l'on prend $f = \pi_k,\ k \in K$ et $g = \det_K$. En effet $\pi_k \circ \det_K^\natural = \det_K \wedge \pi_k = 0$ car $k \in K$.

La propriété suivante montre que $\det_K^\natural$ est une application de référence à laquelle on peut comparer toute autre élimination "maximale" ponctuelle.

Propriété A.3.1 *Soit* $x \in M^m,\ y = \sum_{i=1}^{m} \lambda_i x_i \in M$ *et* $K \subset \mathbb{N}$ *tel que* $\forall\ k \in K,\ \pi_k(y) = 0$ *et* $|K| = m-1$. *Alors*

$$\lambda_i \det_K^\natural(x) = \alpha_i y \qquad \forall\ i \in \{1, \ldots, m\}$$

où $\alpha_i = (-1)^{m-1} \det_K(x_1, \ldots, \not{x}_i, \ldots, x_m)$ *est le coefficient de* x_i *dans* $\det_K^\natural(x)$.

Démonstration On a

$$\begin{aligned}\lambda_i \det_K^\natural(x) &= \det_K^\natural(x_1,\dots,\lambda_i x_i,\dots,x_m) \qquad \text{par linéarité,}\\ &= \det_K^\natural(x_1,\dots,y,\dots,x_m) \qquad \text{car } \det_K^\natural \text{ est alternée,}\\ &= (-1)^{m-i}\det_K(x_1,\dots,\not{x}_i,\dots,x_m)y \quad \text{car } \forall\ k\in K,\ \pi_k(y)=0,\\ &= \alpha_i y.\end{aligned}$$

□

A.3.b Les sous-résultants

Soit P et Q deux polynômes dans $R[X]$ de degrés respectifs p et q. Étant donné un entier $d \le \min(p,q)$, on cherche une élimination portant sur les m polynômes

$$X^{q-d}P,\dots,XP,P,X^{p-d}Q,\dots,XQ,Q$$

qui permettrait d'annuler les $m-1$ coefficients des monômes de plus hauts degrés. Tous ces polynômes appartiennent au R-module $\sum_{i=0}^{p+q-d} R.X^i$. D'après le paragraphe A.3.a (si on pose $\pi_i : T \in R[X] \mapsto$ coefficient en X^i de T), il y en a une "plus belle" que les autres :

$$\det^\natural_{\left[\substack{p+q-d\\ d}\right]}(X^{q-d}P,\dots,XP,P,X^{p-d}Q,\dots,XQ,Q)$$

On l'appelle **le sous-résultant de P et Q d'indice** $d-1$ et on le note $S_{d-1}(P,Q)$. Par l'expression "S_{d-1} est la plus belle des éliminations", nous entendons la propriété suivante :

Propriété A.3.2 *Si U,V sont deux polynômes de degré inférieur ou égal à $q-d$ et $p-d$ respectivement, tels que $(U,V)\neq(0,0)$, alors le degré de $UP+VQ$ est supérieur ou égal à celui de S_{d-1}. Si les degrés de $UP+VQ$ et S_{d-1} sont égaux alors $UP+VQ$ et S_{d-1} sont proportionnels. (Note :* $\deg(0)=-\infty$*)*

Démonstration C'est une conséquence directe de la propriété A.3.1 où les vecteurs $(x_i)_i$ sont les polynômes $X^{q-d}P,\dots,P,X^{p-d}Q,\dots,Q$. □

Par exemple si l'on choisit $p \le q$ et $d=p$, le sous-résultant considéré est

$$\det^\natural_{\left[\substack{q\\ p}\right]}(X^{q-p}P,\dots,XP,P,Q)$$

Si l'on calcule ce déterminant en éliminant petit à petit les coefficients de Q, on s'aperçoit que l'on effectue les opérations élémentaires correspondant au calcul du pseudo-reste (abrégé par prem) de Q par P. On obtient finalement l'égalité :

$$S_{p-1}(P,Q)=\det^\natural_{\left[\substack{q\\ p}\right]}(X^{q-p}P,\dots,XP,P,Q)=\mathrm{prem}(Q,P)$$

Chapitre B

Calcul optimisé des sous-résultants

B.1 Sous-résultants

Le lecteur trouvera dans les ouvrages suivants des démonstrations des principales propriétés des polynômes sous-résultants, ainsi que diverses méthodes pour prouver l'algorithme des sous-résultants.

Un des premiers articles sur le sujet, [15], donne une démonstration "polynomiale" de l'algorithme : les auteurs amènent progressivement les algorithmes de Collins et des sous-résultants. Le même style d'exposé est repris dans [20] (pages 285-299).

Dans [17] (pages 116-123), H. Cohen redémontre avec une méthode très concise l'algorithme des sous-résultants : il considère les formules de l'algorithme et montre qu'elles conduisent effectivement au calcul du résultant (en admettant que les divisions dans l'anneau de base sont exactes).

Dans [34], les auteurs s'attachent à définir les sous-résultants et démontrer des relations "susceptibles de passer à travers" les morphismes d'anneaux (spécialisation par exemple). On y voit les propriétés fondamentales des polynômes sous-résultants.

Dans tous ces documents, la pseudo-division entre deux polynômes est considérée comme une opération élémentaire d'élimination. Le but premier de ce chapitre est de faire la preuve que l'élimination élémentaire entre deux polynômes est l'opération $\pi_i^\natural = \pi_i \wedge \mathrm{Id}$ (en considérant ces polynômes comme des vecteurs sur l'anneau de base). Nous montrerons également certains bénéfices que l'on peut tirer de cette opération élémentaire : nous trouverons de nouvelles relations de divisibilité liées aux sous-résultants et à leurs coefficients. Enfin, nous donnerons une version optimisée de l'algorithme des sous-résultants. Cette optimisation porte sur la taille des scalaires générés par l'algorithme : celle-ci ne dépasse pas le double de la taille du résultat, contrairement à ce que produit l'algorithme des sous-résultants.

B.1.a Rappels

Dans cette section, les résultats les plus simples sur les sous-résultants seront montrés ou rappelés pour le lecteur non spécialiste. Nous reviendrons sur les relations de similarité et de divisibilité entre les sous-résultants (elles sont déjà bien connues, voir les

ouvrages précités ci-dessus). Grâce à de nouvelles relations, nous justifierons non seulement l'algorithme des sous-résultants, mais aussi (et surtout) l'optimisation proposée.

Notations : Si $P \in R[X]$ alors on note $X^{[i,j]}P$ $(i \geq j)$ la liste constituée de

$$X^iP, X^{i-1}P, \ldots, X^{j+1}P, X^jP$$

Par convention, si $i < j$ alors la liste est vide. $\pi_k(P)$ désignera le coefficient de P en X^k. On note $\binom{i}{j}$ la liste ordonnée $\{i, i-1, \ldots, j+1, j\}$ si $i \geq j$, ou l'ensemble vide si $i < j$. Si K est une liste ordonnée $\{a, b, c, \ldots, z\}$, on pose :

$$\det_K = \pi_a \wedge \pi_b \wedge \pi_c \wedge \cdots \wedge \pi_z$$
$$\det\nolimits_K^\natural = \pi_a \wedge \pi_b \wedge \cdots \wedge \pi_z \wedge \mathrm{Id}$$

et par exemple, si $i \geq j$:

$$\det\nolimits_{\binom{i}{j}} = \pi_i \wedge \cdots \wedge \pi_j \qquad \det\nolimits_\emptyset^\natural = \mathrm{Id}_M$$

Dans [42], par définition, le d-ième sous-résultant de deux polynômes P et Q (de degrés p et q respectivement) est le déterminant polynomial de la matrice formée par les $X^{[q-d-1,0]}P$ et les $X^{[p-d-1,0]}Q$. On a donc

$$S_d(P,Q) = \det\nolimits^\natural_{\binom{p+q-d-1}{d+1}}(X^{[q-d-1,0]}P, X^{[p-d-1,0]}Q)$$

On voit facilement avec cette écriture que :

- $S_d(P,Q) = (-1)^{(p-d)(q-d)}S_d(Q,P)$;

- $S_d(P,Q)$ est de degré inférieur à d (toutes les coordonnées de $S_d(P,Q)$ entre $X^{p+q-d-1}$ et X^{d+1} sont nulles) ;

- Les coefficients de $S_d(P,Q)$ sont des polynômes en les coefficients de P et Q. Cette propriété est intéressante pour la spécialisation des polynômes sous-résultants ;

- **Notation :** $\begin{cases} s_d = \pi_d(S_d(P,Q)) & \text{si } d < \min(p,q), \\ s_d = \mathrm{lc}(P)^{q-p} & \text{si } d = p = \min(p,q), \\ s_d = \mathrm{lc}(Q)^{p-q} & \text{si } d = q = \min(p,q). \end{cases}$

Remarquer que, de façon générale, s_d est le coefficient en X^d de $S_d(P,Q)$.
Remarquer également que $s_{\min(p,q)} \in R \setminus \{0\}$ et si $p = q = d$ alors $s_d = 1$.

Propriété B.1.1 *Le polynôme $S_d(P,Q)$ appartient à l'idéal de $R[X]$ engendré par P et Q car combinaison linéaire des $X^{[p-d-1,0]}P$ et des $X^{[q-d-1,0]}Q$;*
Dans cette combinaison linéaire, les coefficients de $X^{q-d-1}P$ et de $X^{p-d-1}Q$ sont respectivement :

$$(-1)^{p-d}\det\nolimits_{\binom{p+q-d-1}{d+1}}(X^{[q-d-2,0]}P, X^{[p-d-1,0]}Q) = (-1)^{p-d}\,\mathrm{lc}(Q)s_{d+1} \text{ et}$$
$$(-1)^{p-d-1}\det\nolimits_{\binom{p+q-d-1}{d+1}}(X^{[q-d-1,0]}P, X^{[p-d-2,0]}Q) = (-1)^{p-d-1}\,\mathrm{lc}(P)s_{d+1}$$

Définition B.1.1 *On dit qu'un sous-résultant $S_d(P,Q)$ est **dégénéré** si son degré est strictement inférieur à son indice d. Dans le cas où ses indice et degré sont égaux, on dit qu'il est **régulier**.*

Rappel de quelques autres propriétés des sous-résultants

- $\mathrm{res}(P,Q) = S_0(P,Q)$;
- Dans $K[X]$ (où K est le corps des fractions de R), si $d = \deg(\gcd(P,Q))$ alors $S_d(P,Q)$ est de degré d ;
- Les sous-résultants représentent les meilleures éliminations des coefficients des monômes des plus hauts degrés de deux polynômes (voir la section A.3.b, page 159).

B.1.b Encore un peu d'algèbre extérieure...

Le prochain théorème (théorème B.1.1) permettra à lui seul de démontrer l'algorithme des sous-résultants : en effet, les résultats sur les similarité (section B.2.a) et divisibilité (section B.2.b) entre sous-résultants n'en sont que des "applications numériques" où les x_i, y_j et z_l sont des polynômes bien choisis. De plus il représente une généralisation du théorème A.2.1 dont nous nous sommes servis pour démontrer l'algorithme de Bareiss. C'est donc ce théorème qui joue le rôle d'une passerelle entre les deux algorithmes.

Définition B.1.2 *Soit $x \in M^m,\ y,z \in M^n$. On dit que z est **échelonné sur** y **modulo** x si z_j est exprimable linéairement en fonction des x_i, de y_j et des y_l qui ont déjà servi pour les z_l précédents.*

Afin d'illustrer cette définition, voici deux exemples où z est échelonné sur y modulo x :

- pour $j = 1,2...n,\ z_j \in R.y_j + \sum_{l<j} R.y_l + \sum_{i=1}^{m} R.x_i$;
- pour $j = n...1,\ z_j \in R.y_j + \sum_{l>j} R.y_l + \sum_{i=1}^{m} R.x_i$.

Il faut souligner que le sens de parcours des valeurs $1...n$ par j est important.

Théorème B.1.1 *Soit M et N deux R-modules, $f : M^{n+1} \to N$ une (n+1)-application et $g \in \Omega^{m-1}(M)$. On considère $x \in M^m,\ y,z \in M^n,\ \lambda \in R^n$ tel que z soit* **échelonné sur** *y* **modulo** *x et λ_j soit le coefficient de y_j dans l'écriture de z_j. On suppose de plus que $\forall\ j \in \{1,\ldots,n\},\ z_j \in \ker g$. Alors on a :*

$$f(g^\natural(x),z) = \left(\prod_{l=1}^{n} \lambda_l\right)\ (g \wedge f)(x,y).$$

Démonstration

$$\begin{aligned}\prod_{l=1}^{n}\lambda_l\ (g\wedge f)(x,y) = &\quad (g\wedge f)(x,\lambda_1.y_1,\ldots,\lambda_n.y_n) \quad \text{par linéarité de } g\wedge f,\\ = &\quad (g\wedge f)(x,z_1,\ldots,z_n)\\ &\quad \text{car } g\wedge f \text{ est alternée et } z \text{ échelonné sur } y \text{ modulo } x,\\ = &\quad f(g^{\natural}(x),z) \quad \text{grâce au théorème A.2.1.}\end{aligned}$$ □

Avant de poursuivre dans le vif du sujet, voici quelques identités (de Sylvester) qui montrent l'efficacité du théorème B.1.1 malgré sa simplicité...
Si l'on pose : $g=\pi_1,\ f=\det_{\{2,3,4\}},\ a_i,b_i,c_i,d_i\in R$,

$$x=(a,b),\ y=(c,d),\ z=(g^{\natural}(a,c),g^{\natural}(b,d)),\ \lambda=(g(a),g(b)),$$

on obtient alors :

$$\begin{Vmatrix} \begin{vmatrix} a_1 & b_1\\ a_2 & b_2\end{vmatrix} & \begin{vmatrix} a_1 & c_1\\ a_2 & c_2\end{vmatrix} & \begin{vmatrix} b_1 & d_1\\ b_2 & d_2\end{vmatrix}\\ \begin{vmatrix} a_1 & b_1\\ a_3 & b_3\end{vmatrix} & \begin{vmatrix} a_1 & c_1\\ a_3 & c_3\end{vmatrix} & \begin{vmatrix} b_1 & d_1\\ b_3 & d_3\end{vmatrix}\\ \begin{vmatrix} a_1 & b_1\\ a_4 & b_4\end{vmatrix} & \begin{vmatrix} a_1 & c_1\\ a_4 & c_4\end{vmatrix} & \begin{vmatrix} b_1 & d_1\\ b_4 & d_4\end{vmatrix}\end{Vmatrix} = a_1.b_1.\begin{vmatrix} a_1 & b_1 & c_1 & d_1\\ a_2 & b_2 & c_2 & d_2\\ a_3 & b_3 & c_3 & d_3\\ a_4 & b_4 & c_4 & d_4\end{vmatrix}$$

Si l'on pose :

$$g=\det_{\{1,2\}},\ f=\pi_3^{\natural},\ x=(a,b,c),\ y=d,\ z=g^{\natural}(a,b,d),\ \lambda=g(a,b),$$

on obtient alors :

$$\begin{Vmatrix} \begin{vmatrix} a_1 & b_1 & c_1\\ a_2 & b_2 & c_2\\ a_3 & b_3 & c_3\end{vmatrix} & \begin{vmatrix} a_1 & b_1 & d_1\\ a_2 & b_2 & d_2\\ a_3 & b_3 & d_3\end{vmatrix}\\ \begin{vmatrix} a_1 & b_1 & c_1\\ a_2 & b_2 & c_2\\ a & b & c\end{vmatrix} & \begin{vmatrix} a_1 & b_1 & d_1\\ a_2 & b_2 & d_2\\ a & b & d\end{vmatrix}\end{Vmatrix} = \begin{vmatrix} a_1 & b_1\\ a_2 & b_2\end{vmatrix}\begin{vmatrix} a_1 & b_1 & c_1 & d_1\\ a_2 & b_2 & c_2 & d_2\\ a_3 & b_3 & c_3 & d_3\\ a & b & c & d\end{vmatrix}$$

B.2 Relations liées aux polynômes sous-résultants

B.2.a Relations de similarité entre sous-résultants

Le but du théorème suivant est de trouver des relations entre les sous-résultants de P et Q afin de mieux comprendre leur structure. On utilisera aussi ces résultats pour donner une variante de l'algorithme des sous-résultants.

Lemme B.2.1 *Soit $0<d\le\min(p,q)$ et $S=S_{d-1}(P,Q)$ dont le degré e est strictement inférieur à $d-1$ ($\deg(0)<0$). On considère $i<d-1$ et $\delta\in\{1,\ldots,d-e-1\}$. On pose $I=\binom{p+q+\delta-d}{d}$ et $J=\binom{i+\delta}{i+1}$. Alors on a :*

$$\det_J^{\natural}(X^{[\delta,0]}S)=s_d^{\delta}\det_{I\cup J}^{\natural}(X^{[q+\delta-d,0]}P,\ X^{[p+\delta-d,0]}Q)$$

Démonstration La démonstration suivante est inspirée de celle que donne D. Lazard dans [39]. On pose :

$$f = \det^{\natural}_{\left[\substack{i+\delta \\ i+1}\right]} \qquad g = \det_{\left[\substack{p+q+\delta-d \\ d}\right]} \qquad x' = X^{[q-d,0]}P \cup X^{[p-d,0]}Q$$

$$x = X^{[\delta,1]}X^{q-d}P \ \cup \ x' \qquad y = X^{[\delta,1]}X^{p-d}Q \qquad z = X^{[\delta,1]}S$$

Comme $\deg(S) + \delta = e + \delta < d$, chaque z_k est de degré strictement inférieur à d, donc dans le noyau de g. De plus, si $\alpha = (-1)^{p-d}\operatorname{lc}(P)s_d$, on a

$$S \in \alpha X^{p-d}Q + \sum_{j<p-d} R.X^jQ + \sum_{j\leq p-d} R.X^jP$$

et en multipliant cette appartenance par X^k ($k \in \{1,\ldots,\delta\}$), on voit que z remplit la condition d'échelonnement du théorème B.1.1 et que λ_k est égal à α. Ainsi, en posant $A = \det^{\natural}_I(x)$ et $B = \det^{\natural}_{I\cup J}(x,y)$, le théorème fournit :

$$\det^{\natural}_J(A, X^{[\delta,1]}S) = \alpha^\delta B = s_d^\delta(-1)^{\delta(p-d)}\operatorname{lc}(P)^\delta B$$

Mais $A = \operatorname{lc}(P)^\delta \det^{\natural}_{\left[\substack{p+q-d \\ d}\right]}(x') = \operatorname{lc}(P)^\delta S$, si bien que le membre de gauche de l'égalité devient :

$$\det^{\natural}_J(\operatorname{lc}(P)^\delta S, X^{[\delta,1]}S) = \operatorname{lc}(P)^\delta(-1)^\delta \det^{\natural}_J(X^{[\delta,0]}S)$$

Le membre de droite devient à son tour après permutation des arguments de B :

$$s_d^\delta(-1)^\delta \operatorname{lc}(P)^\delta \det^{\natural}_{I\cup J}(X^{[q+\delta-d,0]}P,\ X^{[p+\delta-d,0]}Q)$$

On conclut en simplifiant de chaque côté par $(-1)^\delta \operatorname{lc}(P)^\delta$. □

Théorème B.2.1 *On désigne par S_i le $i^{ème}$ sous-résultant de P et Q. On suppose que S_{d-1} est de degré $e < d-1$. Alors :*

1. *S_{d-1} non nul implique*
   - *(a)* $\deg(S_d) = d$ *(où $d < \min(p,q)$) ;*
   - *(b)* $S_{d-1} \sim S_e$ *;*
   - *(c)* $\operatorname{lc}(S_{d-1})^{d-e} = s_d^{d-e-1}\operatorname{lc}(S_e)$ *;*
   - *(d)* $\forall\ \delta \in \{0,\ldots,d-e-1\},\ \operatorname{lc}(S_{d-1})^\delta S_{d-1} \in s_d^\delta.R[X]$ *;*
2. *Si $s_d \neq 0$ alors $\forall\ i \in \{e+1,\ldots,d-2\},\ S_i = 0$;*
3. *Si $s_d \neq 0$ et $S_{d-1} = 0$ alors $S_d = \gcd(P,Q)$ dans $K[X]$ où K est le corps des fractions de R, (ou $\gcd(P,Q) \in \{P,Q\}$ si $d = \min(p,q)$) ;*

   Remarque. Les assertions *1.(b)* et *1.(c)*, si $p = q = d$ alors S_e est un multiple de S_{d-1} car $s_d = 1$;

   L'assertion 1.(d) est due à D. Lazard dans [39]. Cette formule sera utilisée pour obtenir la variante proposée de l'algorithme des sous-résultants ;

   Par 3., si $\deg(S_d) = d$ et S_d n'est pas le pgcd de P et Q dans $K[X]$, alors S_{d-1} est non nul ;

Démonstration D'une part, si l'on pose $i = e$ alors le lemme précédent nous donne :

$$\forall\ \delta \in \{1, \ldots, d-e-1\}, \quad \mathrm{lc}(S_{d-1})^{\delta} S_{d-1} = s_d^{\delta} \det_K^{\natural}(X^{[q+\delta-d,0]}P,\ X^{[p+\delta-d,0]}Q).$$

Alors S_{d-1} non nul implique globalement :

- s_d non nul i.e. $\deg S_d = d$ si $d < \min(P, Q)$ d'où 1.(a) ;
- 1.(b) et 1.(c) en posant $\delta = d - e - 1$;
- 1.(d) en faisant varier δ.

D'autre part, si l'on pose $\delta = d - i - 1$ alors le lemme précédent nous donne :

$$\forall\ i \in \{e, \ldots, d-1\}, \quad 0 = s_d^{\delta} \det_{\left[\substack{p+q-i-1 \\ i+1}\right]}^{\natural}(X^{[q+\delta-d,0]}P,\ X^{[p+\delta-d,0]}Q) = s_d^{\delta} S_i.$$

Alors $s_d \neq 0$ implique 2.. L'assertion 3. n'est qu'une conséquence de 2. lorsque $S_{d-1} = 0$, ou encore $e < 0$ (voir les rappels sur les sous-résultants). □

Remarquer qu'un sous-résultant en milieu de chaîne (i.e. d'indice $d-1 < d \leq \min(p, q)$ appartient à deux paires de polynômes : le couple (S_d, S_{d-1}) est un couple de polynômes qui est réglé par l'équivalence "S_d non dégénéré $\Leftrightarrow$ S_{d-1} non nul" ; le couple (S_{d-1}, S_e) regroupe les sous-résultants associés où $e = \deg(S_{d-1}) < d-1$. Grâce au théorème B.2.1, on peut représenter toute la structure de l'ensemble des sous-résultants de P et Q, depuis $S_{\min(p,q)}$ jusqu'à $S_0 = \mathrm{res}(P, Q)$.

Ci-contre une figure représentant ces correspondances entre sous-résultants. On a choisi de prendre P de degré supérieur à celui de Q pour amorcer plus facilement le haut de la chaîne des sous-résultants.

La chaîne représentée est *étendue* dans le sens où les polynômes S_{d-1}, S_{e-1}, ... sont ici dégénérés, alors que dans la réalité, ils peuvent très bien ne pas l'être (on a alors $S_{d-1} = S_e$). Cette chaîne se poursuit ainsi jusqu'à

$$i = \deg(\gcd(P, Q))$$

(on a alors $S_i \neq 0$), puis tous les sous-résultants d'indice inférieur sont nuls. Bien sûr i peut lui-même être nul...

S_i	$\deg(S_i)$	commentaires
P	p	
$\vdots$	$\vdots$	
Q	q	$s_q \neq 0$
S_{q-1}	d	$S_{q-1} \neq 0$
0		
$\vdots$	$\vdots$	$\forall\ i \in]d, q-1[,\ S_i = 0$
0		
S_d	d	$S_{q-1} \sim S_d$
S_{d-1}	e	$S_{d-1} \neq 0$
0		
$\vdots$	$\vdots$	$\forall\ i \in]e, d-1[,\ S_i = 0$
0		
S_e	e	$S_{d-1} \sim S_e$
S_{e-1}	f	$S_{e-1} \neq 0$
0		
$\vdots$	$\vdots$	

B.2.b Relations de divisibilité entre sous-résultants

Dans cette section, nous allons démontrer l'algorithme des sous-résultants. C'est un algorithme qui calcule le résultant de deux polynômes P et Q grâce à une suite de pseudo-divisions euclidiennes de certains sous-résultants de P et Q.

On choisit P et Q dans $R[X]$, avec $p = \deg(P) \geq \deg(Q) = q$. On abrégera encore le $i^{ème}$ sous-résultant de P et Q par S_i. Le but des relations qui suivent est de montrer le lien qu'il existe entre S_{e-1} et le couple (S_d, S_{d-1}) lorsque S_d est régulier et $S_{d-1} \neq 0$ de degré e.

Premier cas : le premier sous-résultant calculé. On a toujours :

$$\mathrm{prem}(P, -Q) = \det^{\natural}_{\left[\substack{p\\q}\right]}(-X^{[p-q,0]}Q, P) = \det^{\natural}_{\left[\substack{p\\q}\right]}(P, X^{[p-q,0]}Q) = S_{q-1}$$

Deuxième cas : le second sous-résultant calculé.

Théorème B.2.2 *Si S_{q-1} est non nul et de degré e, alors*

$$\mathrm{prem}(Q, -S_{q-1}) = \mathrm{lc}(Q)^{(p-q)(q-e)+1} S_{e-1}$$

Démonstration On pose $A = \det^{\natural}_{\left[\substack{p+q-e\\e}\right]}(X^{[p-e,0]}Q, X^{[q-e,0]}S_{q-1})$. Comme le coefficient de P dans S_{q-1} est $(-1)^{p-q+1}\,\mathrm{lc}(Q)^{p-q+1}$, et qu'il en est de même pour celui de $X^k P$ dans $X^k S_{q-1}$ pour $k \in \{0, \ldots, q-e\}$,

$$\begin{aligned}
\text{il vient } A &= ((-1)^{p-q+1}\,\mathrm{lc}(Q)^{p-q+1})^{q-e+1}\,\det^{\natural}_{\left[\substack{p+q-e\\e}\right]}(X^{[p-e,0]}Q, X^{[q-e,0]}P) \\
&= \mathrm{lc}(Q)^{(p-q+1)(q-e+1)}\,\det^{\natural}_{\left[\substack{p+q-e\\e}\right]}(X^{[q-e,0]}P, X^{[p-e,0]}Q) \\
&= \mathrm{lc}(Q)^{(p-q+1)(q-e+1)} S_{e-1}.
\end{aligned}$$

De plus $A = \mathrm{lc}(Q)^{p-e}\,\det^{\natural}_{\left[\substack{q\\e}\right]}(Q, X^{[q-e,0]}S_{q-1}) = \mathrm{lc}(Q)^{p-e}\,\mathrm{prem}(Q, -S_q)$. On obtient alors l'égalité annoncée en simplifiant par $\mathrm{lc}(Q)^{p-e}$. □

Troisième cas : les autres sous-résultants.

Théorème B.2.3 *Toujours avec les mêmes notations, en supposant S_d et S_{d-1} de degré d et e respectivement, nous avons*

$$\mathrm{prem}(S_d, -S_{d-1}) = \mathrm{lc}(S_d)^{d-e+1} S_{e-1}$$

Si S_{c-1} est le sous-résultant (éventuellement dégénéré) similaire à S_d alors

$$\mathrm{prem}(S_{c-1}, -S_{d-1}) = \mathrm{lc}(S_{c-1})\,\mathrm{lc}(S_d)^{d-e} S_{e-1}$$

Démonstration On pose :

$$f = \det^{\natural}_{\left[\substack{d\\e}\right]} \qquad g = \det_{\left[\substack{p+q-e\\d+1}\right]} \qquad x' = X^{[q-d-1,0]}P \cup X^{[p-d-1,0]}Q$$

$$x = X^{[d-e,0]}X^{q-d}P \ \cup \ x' \qquad y = X^{[d-e,0]}X^{p-d}Q \qquad z = X^{[d-e,0]}S_{d-1}$$

Chaque z_k est de degré strictement inférieur à $d+1$, donc dans le noyau de g. De plus, si $\alpha = (-1)^{p-d}\operatorname{lc}(P)s_d$, on a

$$S_{d-1} \in \alpha X^{p-d}Q + \sum_{j<p-d} R.X^jQ + \sum_{j\leq q-d} R.X^jP$$

et en multipliant cette appartenance par X^k ($k \in \{0,\dots,d-e\}$), on voit que z remplit la condition d'échelonnement du théorème B.1.1 et que λ_k est égal à α. Ainsi, en posant $A = \det^{\natural}_{\left[\substack{p+q-e\\ d+1}\right]}(x)$ et $B = \det^{\natural}_{\left[\substack{p+q-e\\ e}\right]}(x,y)$, le théorème fournit :

$$\det^{\natural}_{\left[\substack{d\\ e}\right]}(A, X^{[d-e,0]}S_{d-1}) = \alpha^{d-e+1}B = \operatorname{lc}(S_d)^{d-e+1}(-1)^{(d-e+1)(p-d)}\operatorname{lc}(P)^{d-e+1}B$$

Mais $A = \operatorname{lc}(P)^{d-e+1}\det^{\natural}_{\left[\substack{p+q-d-1\\ d+1}\right]}(x') = \operatorname{lc}(P)^{d-e+1}S_d$, si bien que le membre de gauche de l'égalité devient :

$$\operatorname{lc}(P)^{d-e+1}\det^{\natural}_{\left[\substack{d\\ e}\right]}(S_d, X^{[d-e,0]}S_{d-1}) = \operatorname{lc}(P)^{d-e+1}\operatorname{prem}(S_d, -S_{d-1})$$

Le membre de droite devient à son tour après permutation des arguments de B :

$$\operatorname{lc}(S_d)^{d-e+1}\operatorname{lc}(P)^{d-e+1}\det^{\natural}_{\left[\substack{p+d-e\\ e}\right]}(X^{[q-e,0]}P, X^{[p-e,0]}Q) = \operatorname{lc}(S_d)^{d-e+1}\operatorname{lc}(P)^{d-e+1}S_{e-1}$$

On obtient alors le premier résultat annoncé en simplifiant par $\operatorname{lc}(P)^{d-e+1}$.

La seconde formule est facile à prouver : comme S_{c-1} et S_d sont similaires, on a $\operatorname{lc}(S_d)\operatorname{prem}(S_{c-1},...) = \operatorname{lc}(S_{c-1})\operatorname{prem}(S_d,...)$. En utilisant le résultat précédent, on conclut aisément. □

B.2.c Relations de divisibilité plus générales

Propriété B.2.1 *Soit K une liste d'entiers positifs et E un sous-ensemble de $R[X]$ tel que $|E| = 1 + |K|$. Alors :*

$$\det^{\natural}_{K+1}(X.E) = X.\det^{\natural}_{K}(E)$$

Démonstration Si T est un polynôme de $R[X]$, on a d'une part $\pi_{i+1}(X.T) = \pi_i(T)$, et d'autre part $\operatorname{Id}_{R[X]}(X.T) = X.\operatorname{Id}_{R[X]}(T)$. Ainsi

$$\begin{aligned}\det^{\natural}_{K+1}(X.E) &= \left(\textstyle\bigwedge_{i\in K}\ \pi_{i+1}\right) \wedge \operatorname{Id}_{R[X]}(X.E)\\ &= \left(\textstyle\bigwedge_{i\in K}\ \pi_{i}\right) \wedge X.\operatorname{Id}_{R[X]}(E)\\ &= X.\det^{\natural}_{K}(E).\end{aligned}$$

□

Théorème B.2.4 *Soit S_{d-1} un sous-résultant non nul de degré e. On sait alors que les sous-résultants S_d et S_e sont de degré respectifs d et e. On pose $s_e = \operatorname{lc}(S_e)$, $s_d = \operatorname{lc}(S_d)$.*

Quel que soit $G \in R[X]$ de degré inférieur à $d-1$, on peut effectuer la division euclidienne de $s_d s_e G$ par S_{d-1} dans $R[X]$ et le reste de cette division est multiple de s_d. Autrement dit, si $\deg(G) \leq d-1$ alors

$$s_eG = \frac{LS_{d-1}}{s_d} + H \qquad\qquad L, H \in R[X], \quad \deg(H) < e$$

Démonstration Posons $c_{d-1} = \mathrm{lc}(S_{d-1})$, $\delta = d-e$ et considérons la pseudo-division de G (vu comme un polynôme de degré $d-1$) par S_{d-1}

$$c_{d-1}^{\delta} G = US_{d-1} + V \qquad\qquad U, V \in R[X]$$

Montrons que U est divisible par $s_d^{\delta-2}$ et V par $s_d^{\delta-1}$. Pour cela il suffira de travailler au signe près. On rappelle que

$$S_{d-1} = \det\nolimits^{\natural}_{\binom{p+q-d}{d}}(X^{[q-d,0]}P, X^{[p-d,0]}Q)$$

Commençons par V.

$$\begin{aligned}
V &= \pm \det\nolimits^{\natural}_{\binom{d-1}{e}}(G, X^{[\delta-1,0]}S_{d-1}) \\
&= \pm \det\nolimits^{\natural}_{\binom{d-1}{e}}(G, X^{[\delta-1,1]}S_{d-1}, \det\nolimits^{\natural}_{\binom{p+q-d}{d}}(X^{[q-d,0]}P, X^{[p-d,0]}Q)) \\
&= \pm \det\nolimits^{\natural}_{\binom{p+q-d}{e}}(G, X^{[\delta-1,1]}S_{d-1}, X^{[q-d,0]}P, X^{[p-d,0]}Q) \qquad \text{(théorème A.2.1)} \\
&= \pm \mathrm{lc}(P)^{1-\delta} \det\nolimits^{\natural}_{\binom{p+q-e-1}{e}}(G, X^{[\delta-1,1]}S_{d-1}, X^{[q-e-1,0]}P, X^{[p-d,0]}Q) \\
&= \pm s_d^{\delta-1} \det\nolimits^{\natural}_{\binom{p+q-e-1}{e}}(G, X^{[q-e-1,0]}P, X^{[p-e-1,0]}Q) \qquad \text{(propriétés B.1.1 et B.2.1)} \\
&= s_d^{\delta-1} H
\end{aligned}$$

En résumé, pour indiquer rapidement comment le facteur $s_d^{\delta-1}$ apparaît, on peut dire que $X^0 S_{d-1}$ est le terme initialisateur de la formule et que chaque $X^k S_{d-1}$ apporte un s_d pour k variant dans $\{1, \ldots, \delta-1\}$.

Passons maintenant à U. On peut calculer chaque coefficient de U en développant $\det^{\natural}_{\binom{d-1}{e}}$ en $\det_{\binom{d-1}{e}} \wedge \mathrm{Id}$. Pour $0 \leq j < \delta$, le coefficient α_j en X^j de U est

$$\det\nolimits_{\binom{d-1}{e}}(G, X^{[\delta-1,j+1]}S_{d-1}, X^{[j-1,0]}S_{d-1})$$

Or ce déterminant est successivement égal à $c_{d-1}^{j} \det_{\binom{d-1}{e+j}}(G, X^{[\delta-1,j+1]}S_{d-1})$, puis finalement à

$$\alpha_j = \det\nolimits_{\binom{d-1+j}{e+j}}(G, X^{[\delta-1+j,j+1]}S_{d-1})$$

On a simplement mis "bout-à-bout" les $X^k S_{d-1}$. Maintenant

$$\begin{aligned}
\alpha_j &= \pm \det\nolimits_{\binom{d-1}{e}}(G^*, X^{[\delta-1,1]}S_{d-1}) \qquad \text{où } G^* = G \text{ quo } X^j \qquad \text{(propriété B.2.1)} \\
&= \pm \det\nolimits_{\binom{d-1}{e}}(G^*, X^{[\delta-1,2]}S_{d-1}, \det\nolimits^{\natural}_{\binom{p+q-d+1}{d+1}}(X^{[q-d+1,1]}P, X^{[p-d+1,1]}Q)) \\
&= \pm \det\nolimits_{K}(G^*, X^{[\delta-1,2]}S_{d-1}, X^{[q-d+1,1]}P, X^{[p-d+1,1]}Q) \qquad \text{où } K = \tbinom{p+q-d+1}{d+1} \cup \tbinom{d-1}{e}
\end{aligned}$$

$$= \pm \operatorname{lc}(P)^{2-\delta} \det_{K'}(G^*, X^{[\delta-1,2]} S_{d-1}, X^{[q-e-1,1]} P, X^{[p-d+1,1]} Q)$$
$$\text{où } K' = \tbinom{p+q-e-1}{p+q-d+2} \cup K$$

$$= \pm s_d^{\delta-2} \det_{K'}(G^*, X^{[q-e-1,1]} P, X^{[p-e-1,1]} Q) \qquad \text{(propriétés B.2.1 et B.1.1)}$$

$$= s_d^{\delta-2} \operatorname{coeff}_{X^j}(L)$$

En résumé, on peut dire que $X^1 S_{d-1}$ est le terme initialisateur de la formule et que chaque $X^k S_{d-1}$ apporte un s_d pour k variant dans $\{2, \ldots, \delta - 1\}$.

Après ces deux preuves de divisibilité, nous obtenons

$$c_{d-1}^{\delta} G = s_d^{\delta-2} L S_{d-1} + s_d^{\delta-1} H \qquad\qquad L, H \in R[X]$$

Il ne reste plus qu'à diviser tout cela par $s_d^{\delta-1}$ et remarquer que $s_e = \dfrac{c_{d-1}^{\delta}}{s_d^{\delta-1}}$ afin de faire apparaître la relation $s_e G = \dfrac{L S_{d-1}}{s_d} + H$. □

Théorème B.2.5 *Avec les mêmes notations que le théorème B.2.4,*
— si l'on pose $G = \pi_d^{\natural}(X^{d-e} S_{d-1}, F)$ où F est un polynôme de degré inférieur à d, alors on obtient

$$s_e c_{d-1} F = L^* S_{d-1} + H \qquad\qquad L^*, H \in R[X], \quad \deg(H) < e$$

— si l'on pose $G = \pi_d^{\natural}(F, S_d)$ où F est un polynôme de degré inférieur à d, alors on obtient

$$s_e \pi_d^{\natural}(F, S_d) = \frac{L S_{d-1}}{s_d} + s_d H^* \qquad\qquad L, H^* \in R[X], \quad \deg(H^*) < e$$

— si l'on pose $G = \pi_d^{\natural}(X^{d-e} S_{d-1}, S_d)$, alors on obtient une formule due à T. Lickteig et M.-F. Roy (voir [40]) :

$$c_{d-1} s_e S_d = L^* S_{d-1} + (-1)^{d-e+1} s_d^2 S_{e-1} \qquad\qquad L^* \in R[X]$$

Ces trois premières formules ont pour conséquence les suivantes : soit S_{c-1} le sous-résultant (éventuellement dégénéré) similaire à S_d. Son coefficient dominant (en X^d) est noté c_{c-1}.
Si l'on pose $G = \pi_d^{\natural}(F, S_{c-1})$ où F est un polynôme de degré inférieur à d, alors on obtient

$$s_e \pi_d^{\natural}(F, S_{c-1}) \equiv c_{c-1} H^* \mod S_{d-1} \qquad\qquad H^* \in R[X], \quad \deg(H^*) < e$$

Si l'on pose $G = \pi_d^{\natural}(X^{d-e} S_{d-1}, S_{c-1})$, alors on obtient

$$c_{d-1} s_e S_{c-1} \equiv (-1)^{d-e+1} s_d c_{c-1} S_{e-1} \mod S_{d-1}$$

Démonstration Nous prouvons ces relations, chaque • suivant correspondant à l'une d'entre elles respectivement.

• Nous savons déjà que H appartient à $R[X]$ puisqu'il est égal au reste de la division de $s_e G = s_e \pi_d^\natural(X^{d-e} S_{d-1}, F)$ par S_{d-1} (théorème B.2.4). Il suffit donc de démontrer que le pseudo-quotient (de la pseudo-division de F par S_{d-1}) est bien divisible par $s_d^{\delta-1}$ pour assurer le fait que Q^* appartient à $R[X]$ (rappel : $\delta = d - e$). Pour cela, il faut refaire le même type de preuve que précédemment.

Posons $\delta = d - e$ et considérons la pseudo-division de F (vu comme un polynôme de degré d) par S_{d-1}

$$c_{d-1}^{\delta+1} F = U S_{d-1} + V \qquad\qquad U, V \in R[X]$$

On peut calculer chaque coefficient de U en développant $\det^\natural_{\left[\begin{smallmatrix} d \\ e \end{smallmatrix}\right]}$ en $\det_{\left[\begin{smallmatrix} d \\ e \end{smallmatrix}\right]} \wedge \mathrm{Id}$. Pour tout entier $j \in \{0, \ldots, \delta\}$, le coefficient α_j en X^j de U est

$$\det_{\left[\begin{smallmatrix} d \\ e \end{smallmatrix}\right]}(F, X^{[\delta, j+1]} S_{d-1}, X^{[j-1,0]} S_{d-1})$$

Or ce déterminant est successivement égal à $c_{d-1}^j \det_{\left[\begin{smallmatrix} d \\ e+j \end{smallmatrix}\right]}(F, X^{[\delta, j+1]} S_{d-1})$, puis finalement à

$$\alpha_j = \det_{\left[\begin{smallmatrix} d+j \\ e+j \end{smallmatrix}\right]}(F, X^{[\delta+j, j+1]} S_{d-1})$$

On a simplement mis "bout-à-bout" les $X^k S_{d-1}$. Maintenant

$$\begin{aligned}
\alpha_j &= \pm \det_{\left[\begin{smallmatrix} d \\ e \end{smallmatrix}\right]}(G^*, X^{[\delta,1]} S_{d-1}) \qquad \text{où } G^* = G \text{ quo } X^j \qquad \text{(propriété B.2.1)} \\
&= \pm \det_{\left[\begin{smallmatrix} d \\ e \end{smallmatrix}\right]}(G^*, X^{[\delta,2]} S_{d-1}, \det^\natural_{\left[\begin{smallmatrix} p+q-d+1 \\ d+1 \end{smallmatrix}\right]}(X^{[q-d+1,1]} P, X^{[p-d+1,1]} Q)) \\
&= \pm \det_{\left[\begin{smallmatrix} p+q-d+1 \\ e \end{smallmatrix}\right]}(G^*, X^{[\delta,2]} S_{d-1}, X^{[q-d+1,1]} P, X^{[p-d+1,1]} Q) \\
&= \pm \operatorname{lc}(P)^{1-\delta} \det_{\left[\begin{smallmatrix} p+q-e-1 \\ e \end{smallmatrix}\right]}(G^*, X^{[\delta,2]} S_{d-1}, X^{[q-e,1]} P, X^{[p-d+1,1]} Q) \\
&= \pm s_d^{\delta-1} \det_{\left[\begin{smallmatrix} p+q-e-1 \\ e \end{smallmatrix}\right]}(G^*, X^{[q-e,1]} P, X^{[p-e,1]} Q) \qquad \text{(propriétés B.2.1 et B.1.1)} \\
&= s_d^{\delta-1} \operatorname{coeff}_{X^j}(L^*)
\end{aligned}$$

En résumé, on peut dire que $X^1 S_{d-1}$ est le terme initialisateur de la formule et que chaque $X^k S_{d-1}$ apporte un s_d pour $k \in \{2, \ldots, \delta\}$.

• Il faut démontrer que le pseudo-reste (de la pseudo-division de $G = \pi_d^\natural(F, S_d)$ par S_{d-1}) est bien divisible par s_d^δ pour assurer le fait que H^* appartient à $R[X]$. Pour cela, il faut refaire le même type de preuve que précédemment...

Posons $\delta = d - e$ et considérons la pseudo-division de $G = \pi_d^\natural(F, S_d)$ (vu comme un polynôme de degré $d-1$) par S_{d-1}

$$c_{d-1}^{\delta+1} G = c_{d-1}^{\delta+1} \pi_d^\natural(F, S_d) = U S_{d-1} + V \qquad\qquad U, V \in R[X]$$

$$
\begin{aligned}
V &= \pm \det^{\natural}_{\left[\substack{d-1\\ e}\right]}(G, X^{[\delta-1,0]}S_{d-1}) \\
&= \pm \det^{\natural}_{\left[\substack{d-1\\ e}\right]}(\pi^{\natural}_d(F, S_d), X^{[\delta-1,0]}S_{d-1}) \\
&= \pm \det^{\natural}_{\left[\substack{d\\ e}\right]}(F, S_d, X^{[\delta-1,0]}S_{d-1}) \qquad \text{(théorème A.2.1)} \\
&= \pm \det^{\natural}_{\left[\substack{d\\ e}\right]}(F, \det^{\natural}_{\left[\substack{p+q-d-1\\ d+1}\right]}(X^{[q-d-1,0]}P, X^{[p-d-1,0]}Q), X^{[\delta-1,0]}S_{d-1}) \\
&= \pm \det^{\natural}_{\left[\substack{p+q-d-1\\ e}\right]}(F, X^{[q-d-1,0]}P, X^{[p-d-1,0]}Q, X^{[\delta-1,0]}S_{d-1}) \qquad \text{(théorème A.2.1)} \\
&= \pm \operatorname{lc}(P)^{-\delta} \det^{\natural}_{\left[\substack{p+q-e-1\\ e}\right]}(F, X^{[\delta-1,0]}S_{d-1}, X^{[q-e-1,0]}P, X^{[p-d,0]}Q) \\
&= \pm s_d^{\delta} \det^{\natural}_{\left[\substack{p+q-e-1\\ e}\right]}(F, X^{[q-e-1,0]}P, X^{[p-e-1,0]}Q) \qquad \text{(propriétés B.1.1 et B.2.1)} \\
&= s_d^{\delta} H^*
\end{aligned}
$$

En résumé, disons que S_d est le terme initialisateur de la formule et que chaque $X^k S_{d-1}$ apporte un s_d pour k variant dans $\{0, \ldots, \delta - 1\}$.

• On pourrait "s'amuser" à démontrer cette formule avec du calcul extérieur, mais cette fois-ci, pour aller plus vite, utilisons la relation classique de divisibilité entre sous-résultants $c_{d-1}^{\delta+1} S_d = L S_{d-1} + (-s_d)^{\delta+1} S_{e-1}$. Il suffit de la diviser par $s_d^{\delta-1}$ et de considérer la première relation de ce théorème B.2.5 pour justifier que le quotient $\frac{L}{s_d^{\delta-1}}$ est exact.

• Enfin, les deux dernières relations s'obtiennent avec les formules précédentes du théorème B.2.5 et par le lien de similarité entre S_{c-1} et S_d : $\frac{S_{c-1}}{c_{c-1}} = \frac{S_d}{s_d}$. □

B.3 Algorithmes

Ici encore, on choisit deux polynômes P et Q dans $R[X]$ et on note S_i leur $i^{ème}$ sous-résultant. Dans la section B.3.a, on traite rapidement l'algorithme des sous-résultants. La section B.3.b est consacrée exclusivement au développement de la variante optimisé de l'algorithme des sous-résultants.

B.3.a L'algorithme des sous-résultants

L'algorithme des sous-résultants est maintenant totalement démontré : à l'aide des sous-résultants éventuellement dégénérés notés S_{i-1}, on calcule le résultant de deux polynômes de $R[X]$.

1. On se donne deux polynômes P et Q, le degré de P étant supérieur à celui de Q (échanger P et Q si nécessaire).
2. Calcul direct de S_{q-1} (de degré d) par $\operatorname{prem}(P, -Q)$.
3. Calcul de S_{d-1} (de degré e) en fonction de Q, S_{q-1} et $\deg(P)$ (théorème B.2.2 2.).

4. Calcul de $\mathrm{lc}(S_d)$ en fonction de $Q,\ S_{q-1}$ et $\deg(P)$ (théorème B.2.1 1.(c)).
   Calcul de S_{e-1} (de degré f) en fonction de $S_{q-1},\ S_{d-1}$ et $\mathrm{lc}(S_d)$ (théorème B.2.3 3.).

5. Calcul de $\mathrm{lc}(S_e)$ en fonction de $\mathrm{lc}(S_d),\ S_{d-1}$ et $\deg(S_{q-1})$ (théorème B.2.1 1.(c)).
   Calcul de S_{f-1} en fonction de $S_{d-1},\ S_{e-1}$ et $\mathrm{lc}(S_e)$ (théorème B.2.3 3.).

6. Répéter le 5. jusqu'au calcul de $\mathrm{lc}(S_0)$...

7. $\mathrm{res}(P,Q) = \mathrm{lc}(S_0)$ (théorème B.2.1 1.(c) ou B.2.1 2.).

Algorithme des sous-résultants.
Données : $P, Q \in R[X]$ $\qquad \deg(P) \geq \deg(Q) \geq 1$
Résultat : $\mathrm{res}(P,Q)$

$\delta \leftarrow \deg(P) - \deg(Q)$; $s \leftarrow \mathrm{lc}(Q)^\delta$
$(P,Q) \leftarrow \big(Q, \mathrm{prem}(P,-Q)\big)$
loop $\qquad$ — ici, $P = S_{c-1},\ Q = S_{d-1},\ s = \mathrm{lc}(S_d)$ —
  if $Q = 0$ then return 0
  $\delta \leftarrow \deg(P) - \deg(Q)$
  if $\deg(Q) = 0$ then return $\dfrac{\mathrm{lc}(Q)^\delta}{s^{\delta-1}}$
  $(P,Q) \leftarrow \big(Q, \dfrac{\mathrm{prem}(P,-Q)}{\mathrm{lc}(P).s^\delta}\big)$
  $s \leftarrow \dfrac{\mathrm{lc}(P)^\delta}{s^{\delta-1}}$
end loop

B.3.b Optimisations de l'algorithme

Cherchons à optimiser l'algorithme des sous-résultants. En effet ce dernier n'est pas "parfait" car on constate une croissance inutile des différentes quantités calculées :

• (Remarque due à D. Lazard) Le calcul du coefficient dominant de S_e par la formule *1.(d)* du théorème B.2.1 1.(c) fait apparaître une fraction de deux éléments de R avec certains exposants. Il est coûteux de calculer d'abord deux puissances puis de les "éliminer" en les divisant. Un calcul plus efficace est donné par le point 1.(d) du même théorème (considérer le coefficient dominant de S_{d-1} et S_e) :

$$\mathrm{lc}(S_e) = \frac{\mathrm{lc}(S_{d-1})^{d-e}}{s_d^{d-e-1}} = \frac{\dfrac{\dfrac{\mathrm{lc}(S_{d-1})^2}{s_d} \times \mathrm{lc}(S_{d-1})}{s_d} \times \cdots \times \mathrm{lc}(S_{d-1})}{s_d}$$

où tous les quotients sont exacts. Dans le terme de droite, seuls des éléments de "hauteur" 1 ou 2 apparaissent : après chaque multiplication, on effectue une simplification.

Calcul optimisé de s_e.
Données : $d,\ e,\ s_d = \mathrm{lc}(S_d),\ c_{d-1} = \mathrm{lc}(S_{d-1})$
Résultat : s_e

$y \leftarrow c_{d-1}$
for j in $e+1 \ldots d-1$ loop $\qquad y \leftarrow \dfrac{y.c_{d-1}}{s_d} \qquad$ end loop
return y

Remarque. Il est possible d'améliorer encore la procédure de calcul de S_e ci-dessus en programmant un calcul dichotomique de $\dfrac{\mathrm{lc}(S_{d-1})^{d-e}}{s_d^{d-e-1}}$:

Calcul optimisé et dichotomique de s_e.
Données : $d,\ e,\ s_d = \mathrm{lc}(S_d),\ c_{d-1} = \mathrm{lc}(S_{d-1})$
Résultat : s_e

$n \leftarrow d-e$ $\qquad$ — ici, $n_0 = d-e$
if $n = 1$ then return c_{d-1}
$a \leftarrow 2^{\lfloor \log_2(n) \rfloor}$ $\qquad$ — ici, $a \le n < 2a$
$x \leftarrow s_d$
$n \leftarrow n-a$
loop $\qquad$ — ici, $x = c_{d-1}^j / s_d^{j-1},\ aj \le n_0 < a(j+1),\ a = 2^?$ —
  when $a = 1$ return x
  $a \leftarrow \dfrac{a}{2}\ ;\ x \leftarrow \dfrac{x^2}{s_d}$
  if $n \ge a$ then $x \leftarrow \dfrac{x.c_{d-1}}{s_d}\ ;\ n \leftarrow n-a$
end loop

• Le calcul de S_{e-1} par le théorème B.2.3 est aussi coûteux. Après avoir calculé le pseudo-reste de S_{c-1} par S_{d-1}, on le divise par un élément de R de "hauteur" $d-e+1$, qui peut être énorme... Pour rendre efficace le calcul de S_{e-1}, il faudrait commencer à diviser pendant que l'on effectue les éliminations élémentaires de la pseudo-division. Mais en fait, le principe de la pseudo-division n'est pas très adapté : en effet, les restes intermédiaires de la pseudo-division de S_{c-1} par S_{d-1} sont divisibles par s_d seulement à partir de la seconde élimination (c'est-à-dire à partir du second reste intermédiaire), si bien que des éléments de "hauteur" 3 apparaissent lors de cette division.

Par un principe de calcul différent, on peut effectuer ce calcul en "hauteur" 2... Posons $s_d = \mathrm{lc}(S_d)$, $c_{c-1} = \mathrm{lc}(S_{c-1})$, $c_{d-1} = \mathrm{lc}(S_{d-1})$. Nous pouvons alors calculer la constante $s_e = \mathrm{lc}(S_e)$ en utilisant l'algorithme précédent.

Ensuite, il est possible d'obtenir la classe de $s_e X^j$ modulo S_{d-1} par des calculs de "hauteur" 2 dans $R[X]$:

$$H_j = \frac{\mathrm{rem}(s_e s_d X^j, S_{d-1})}{s_d} \equiv s_e X^j \mod S_{d-1} \qquad \forall\ j < d$$

Les H_j appartiennent tous à $R[X]$ en vertu du théorème B.2.4 et sont de "hauteur" 1. En fait, pour $j < e$ on a $H_j = s_e X^j$, pour $j = e$ on a $H_j = s_e X^e - S_e$, et pour $j > e$ on a

$$H_j = XH_{j-1} - \frac{\pi_e(XH_{j-1})S_{d-1}}{c_{d-1}}$$

où le quotient est exact. Dans le cas où $e = d - 1$ (i.e. $S_{d-1} = S_e$ est régulier), tous les H_j (pour $j < d$) sont obtenus sans nouveau calcul. Grâce à ces polynômes H_j, nous sommes capables de donner le reste de la division euclidienne de $s_e G$ par S_{d-1} où G est un polynôme quelconque de degré strictement inférieur à d. En particulier le reste de $s_e \pi_d^\natural(X^d, S_{c-1})$ par S_{d-1} est :

$$B = \operatorname{rem}\left(s_e \pi_d^\natural(X^d, S_{c-1}), S_{d-1}\right) = \operatorname{rem}\left(s_e(S_{c-1} - c_{c-1}X^d), S_{d-1}\right) = \sum_{j<d} \pi_j(S_{c-1})H_j$$

Noter que B est de "hauteur" 2, et divisible par c_{c-1} en vertu du théorème B.2.5.
Il est également possible d'obtenir la classe de $s_e c_{d-1} X^d$ modulo S_{d-1}, simplement par

$$H_d = c_{d-1}XH_{d-1} - \pi_e(XH_{d-1})S_{d-1} \equiv s_e c_{d-1} X^d \mod S_{d-1}$$

Noter que H_d est de "hauteur" 2.

Considérons la relation du théorème B.2.5 :

$$c_{d-1} s_e S_{c-1} \equiv (-1)^{d-e+1} s_d c_{c-1} S_{e-1} \mod S_{d-1}$$

et écrivons $S_{c-1} = c_{c-1}X^d + (S_{c-1} - c_{c-1}X^d)$, alors nous voyons très bien les relations de congruence

$$\begin{aligned}(-1)^{d-e+1} s_d c_{c-1} S_{e-1} &\equiv c_{c-1}c_{d-1}s_e X^d + c_{d-1}s_e(S_{c-1} - c_{c-1}X^d) \mod S_{d-1} \\ &\equiv c_{c-1}H_d + c_{d-1}B \mod S_{d-1}\end{aligned}$$

Or les polynômes S_{e-1}, H_d et B ont des degrés inférieurs strictement à celui de S_{d-1}. La dernière relation de congruence est donc une réelle égalité :

$$S_{e-1} = (-1)^{d-e+1}\frac{H_d + c_{d-1}\frac{B}{c_{c-1}}}{s_d} = (-1)^{d-e+1}\frac{c_{d-1}\left(\frac{B}{c_{c-1}} + XH_{d-1}\right) - \pi_e(XH_{d-1})S_{d-1}}{s_d}$$

Nous obtenons une formule de "hauteur" 2 exprimant S_{e-1}, ayant lieu dans $R[X]$ car B est divisible pas c_{c-1}.

Calcul optimisé de S_{e-1}.
Données : S_{c-1}, S_{d-1}, $s_d = \mathrm{lc}(S_d)$, $s_e = \mathrm{lc}(S_e)$
Résultat : S_{e-1}

$(d, e) \leftarrow \big(\deg(S_{c-1}), \deg(S_{d-1})\big)$
$(c_{c-1}, c_{d-1}) \leftarrow \big(\mathrm{lc}(S_{c-1}), \mathrm{lc}(S_{d-1})\big)$
for j in $0 \ldots e-1$ loop
    $H_j \leftarrow s_e X^j$
end loop
$H_e \leftarrow s_e X^e - \dfrac{s_e S_{d-1}}{c_{d-1}}$
for j in $e+1 \ldots d-1$ loop
    $H_j \leftarrow XH_{j-1} - \dfrac{\pi_e(XH_{j-1})S_{d-1}}{c_{d-1}}$
end loop
$B \leftarrow \displaystyle\sum_{0 \le j < d} \pi_j(S_{c-1})H_j$ — ici, $H_j \equiv s_e X^j \mod S_{d-1}$ —
return $(-1)^{d-e+1} \dfrac{c_{d-1}\left(\dfrac{B}{c_{c-1}} + XH_{d-1}\right) - \pi_e(XH_{d-1})S_{d-1}}{s_d}$

Voici maintenant le corps du nouvel algorithme faisant appel aux petites procédures vues ci-dessus :

Algorithme optimisé.
Données : $P, Q \in R[X]$ $\deg(P) \ge \deg(Q) \ge 1$
Résultat : $\mathrm{res}(P, Q)$

$\delta \leftarrow \deg(P) - \deg(Q)$; $s \leftarrow \mathrm{lc}(Q)^\delta$
$(P, Q) \leftarrow (Q, \mathrm{prem}(P, -Q))$
loop — ici, $P = S_{c-1}$, $Q = S_{d-1}$, $s = \mathrm{lc}(S_d)$ —
    if $Q = 0$ then return 0
    $\delta \leftarrow \deg(P) - \deg(Q)$
    $s' \leftarrow$ *calcul optimisé de* s_e *en fonction de* $\deg(P), \deg(Q), s, \mathrm{lc}(Q)$
    if $\deg(Q) = 0$ then return s'
    $(P, Q) \leftarrow \big(Q,$ *calcul optimisé de* S_{e-1} *en fonction de* $P, Q, s, s'\big)$
    $s \leftarrow s'$
end loop

B.4 Mise en œuvre et expérimentation

Afin de rendre compte de l'efficacité de cette variante de l'algorithme des sous-résultants, nous donnons juste deux séries de tests.

Pour la première série, on reprend les tests fournis dans [1] (pages 268 à 279) :

test1 $P = X^8 + X^6 - 3X^4 - 3X^3 + 8X^2 + 2X - 5$
$Q = 3X^6 + 5X^4 - 4X^2 - 9X + 21$

test2 $P = 3X^4 + 5X^3 + 5X^2 - 2X + 1$
$Q = 3X^3 + 3X^2 + 3X - 4$

test3 $P = 2X^6 + X^5 + 4X^4 + 3X^3 + 5X^2 - 2X + 2$
$Q = X^6 - X^5 - X^4 + 4X^3 - 2X^2 + X + 1$

test4 $P = X^6 + X^5 - X^4 - X^3 + X^2 - X + 1$
$Q = 6X^5 + 5X^4 - 4X^3 - 3X^2 + 2X - 1$

test5 $P = 3X^9 + 5X^8 + 7X^7 - 3X^6 - 5X^5 - 7X^4 + 3X^3 + 5X^2 + 7X - 2$
$Q = X^8 - X^5 - X^2 - X - 1$

test6 $P = 3X^8 + 4X^7 - 7X^5 - 9X^3 + X^2 - X + 2$
$Q = 3X^5 + 12X^4 - 7X^2 + 1$

test7 $P = X^5 + 5X^4 + 10X^3 + 5X^2 + 5X + 2$
$Q = X^4 + 4X^3 + 6X^2 + 2X + 1$

test8 $P = 2X^4 + 3X^3 + 5X^2 - 2X - 1$
$Q = X^3 + X^2 + 2X - 1$

test9 $P = 6X^8 + 7X^7 - 3X^6 + 16X^5 + 20X^4 + 8X^3 + 17X^2 + 6X + 18$
$Q = 2X^7 + X^6 + 3X^5 + X^4 - 2X^3 + 9X^2 - 7X + 3$

test10 $P = 2X^4 - X^3 - 14X^2 + 17X - 5$
$Q = 6X^3 - 7X^2 + 4X - 1$

Le tableau suivant résume les performances des trois algorithmes étudiés en ce qui concerne les tailles (i.e. le nombre de chiffres) des plus grands entiers générés sur chaque test. Bien sûr, il n'est pas question avec ces premiers tests de comparer des temps de calculs car ceux-ci sont trop petits (en ce qui concerne les algorithmes des sous-résultants et sa variante) pour être significatifs.

	Algorithme des sous-résultants	Algorithme optimisé	Algorithme de Bareiss
test1	11	9	10
test2	6	6	7
test3	16	11	12
test4	11	8	10
test5	23	16	17
test6	28	20	21
test7	5	5	6
test8	1	1	2
test9	21	16	18
test10	11	9	10

Tailles maximales des entiers générés.

Nous donnons aussi un jeu de calculs de résultants avec des polynômes plus ou moins paramétrés et de degrés plus importants. Ici, nous comparons les temps de réponse de l'algorithme des sous-résultants et de sa variante.

test11 $P = X^7 + aX^6 + bX^5 + cX^4 + dX^3 + eX^2 + fX + g$
$Q = P'$

test12 $P = X^5 + aX^4 + bX^3 + cX^2 + dX + e$
$Q = X^5 + fX^4 + gX^3 + hX^2 + iX + j$

test13 $P = X^7 + aX^3 + bX^2 + cX + d$
$Q = X^7 + eX^3 + fX^2 + gX + h$

test14 $P = X^{20} + aX^{15} + b$
$Q = X^{20} + cX^5 + d$

test15 $P = (X + a)^{15}$
$Q = (X + z)^{15}$

test16 $P = X^{30} + aX^{20} + 2aX^{10} + 3a$
$Q = X^{25} + 4bX^{15} + 5bX^5$

test17 $P = \Phi_{198}(aX)$ (polynôme cyclotomique)
$Q = \Phi_{98}(bX)$

test18 $P = \sum_{j=0}^{75} a^{75-j} X^j$
$Q = \sum_{j=0}^{75} j a^j X^j$

test19 $P = \sum_{j=0}^{200} X^j$
$Q = 1 + \sum_{j=0}^{100} jX^j$

test20 $P = 1 + \sum_{j=1}^{900} jX^j$
$Q = 1 + \sum_{j=1}^{900} j^2 X^j$

Le tableau suivant résume les performances des deux algorithmes programmés en Axiom version 2.0. Les temps sont exprimés en secondes.

	Algorithme des sous-résultants	Algorithme optimisé		Algorithme des sous-résultants	Algorithme optimisé
test11 (0)	1142	69	test16 (1)	935	27
test12 (0)	2364	80	test17 (4)	134	71
test13 (3)	1162	77	test18 (2)	2342	7.6
test14 (1)	1091	59	test19 (2)	39	1.3
test15 (0)	499	245	test20 (2)	264	14

Temps de calculs (en secondes).

Commentaire sur les degrés des sous-résultants de ce test :

(0) aucun sous-résultant dégénéré,
(1) sous-résultants dans $R[X^5]$,
(2) un seul saut (quasiment maximal) au milieu la chaîne des sous-résultants,
(3) sous-résultants de plus grand indice seul dégénéré,
(4) deux petits sauts en fin de chaîne.

Références bibliographiques

[1] A.G. Akritas. *Elements of computer algebra with applications.* John Wiley and Sons, 1989.

[2] J.M. Arnaudiès. Sur la résolubilité explicite des équations de degré 5 quand elles sont résolubles par radicaux. Institut de Recherche Mathématique Avancée, Strasbourg, 1974.

[3] J.M. Arnaudiès. Sur la résolution explicite des équations de degré 5, quand elles sont résolubles par radicaux. *Bulletin des sciences mathématiques, deuxième serie*, 100:241–254, 1976.

[4] J.M. Arnaudiès and A. Valibouze. *Résolvantes de Lagrange.* Institut Blaise Pascal, Université Pierre et Marie Curie, décembre 1993. `http://medicis.polytechnique.fr/pub/publications/valibouze/lagrange.*`.

[5] E. Artin. *Galois Theory.* 2. Notre Dame Mathematical Lectures, 1959.

[6] M. Auslander and O. Goldman. The Brauer group of a commutative ring. *Trans. Amer. Math. Soc.*, 97:367–409, 1960.

[7] E.H. Bareiss. Sylvester's identity and multistep integer-preserving Gaussian elimination. *Math. Comp.*, 22:565–578, 1968.

[8] N. Bourbaki. *Algèbre commutative,* ch. 2, Localisation. Hermann, 1961.

[9] N. Bourbaki. *Algèbre commutative,* ch. 4, Idéaux premiers associés et décomposition primaire. Hermann, 1961.

[10] N. Bourbaki. *Algèbre commutative,* ch. 5, Entiers. Hermann, 1964.

[11] N. Bourbaki. *Algèbre,* ch. 1. Hermann, 1970.

[12] N. Bourbaki. *Algèbre,* ch. 10, Algèbre homologique. Masson, 1980.

[13] N. Bourbaki. *Algèbre,* ch. 4, Polynômes et fractions rationnelles. Masson, 1981.

[14] N. Bourbaki. *Algèbre,* ch. 5, Corps commutatifs. Masson, 1981.

[15] W.S. Brown and J.F. Traub. On Euclid's Algorithm and Theory of Subresultants. *Ass. Comp. Mach.*, 18(4):505–514, Octobre 1971.

[16] S.U. Chase, D.K. Harrison, and A. Rosenberg. Galois Theory and Galois Cohomology of Commutative Rings. *Memoirs of the American Mathematical Society*, 52:15–33, 1965.

[17] H. Cohen. *A course in computational algebraic number theory,* ch.3. Springer-Verlag, 1993.

[18] A. Colin. *Théorie des invariants effective. Applications à la théorie de Galois et à la résolution de systèmes algébriques. Implantation en Axiom.* École polytechnique, juin 1997. Thèse doctorale,
`http://medicis.polytechnique.fr/pub/publications/colin/these.*`.

[19] J.H. Conway, A. Hulpke, and J. McKay. On transitive Permutation Groups. preliminary version
`http://www-groups.dcs.st-and.ac.uk/~ahulpke/publ.html` .

[20] S.R. Czapor, K.O. Geddes, and G. Labahn. *Algorithms for computer algebra.* Kluwer Academic Publishers, 1992.

[21] A. Dahan-Dalmedico and J. Peiffer. *Une histoire des mathématiques (routes et dédales).* Editions du Seuil, mars 1986.

[22] P. Dèbes and B. Deschamp. The Regular Inverse Galois Problem over Large Fields. Preprint.

[23] F. DeMeyer and E. Ingraham. Separable algebras over commutative rings, ch. 3. *Lecture notes in Math., 181, Springer-Verlag, Berlin*, 1971.

[24] R. Dentzer. Polynomials with Cyclic Galois Group. *Communications in Algebra*, 23(4):1593–1603, 1995.

[25] B. Deschamps. Existence de points p-adiques pour tout p sur un espace de Hurwitz. *Contemporary Mathematics*, 186:239–247, 1995.

[26] J. Dieudonné. *Abrégé d'histoire des mathématiques.* Hermann, 1986.

[27] L. Ducos. Algorithme de Bareiss, algorithme des sous-résultants. Prépublication de l'Université de Poitiers, n.89, janvier 1995.

[28] L. Ducos. Algorithme de Bareiss, Algorithme des sous-résultants. *Theoretical Informatics And Applications*, 30(4):319–347, 1996.

[29] L. Ducos and C. Quitté. *Algèbre de décomposition universelle, Implémentation et applications à la théorie de Galois.* Prépublication de l'Université de Poitiers, n.98, juin 1996.
`http://medicis.polytechnique.fr/pub/publications/ducos/`.

[30] D.S. Dummit. Solving solvable quintics. *Mathematics of computation*, 57(195):387–401, july 1991.

[31] Y. Eichenlaub. *Problèmes effectifs de théorie de Galois en degré 8 à 11.* Université de Bordeaux, 1996. Thèse doctorale.

[32] E. Galois. *Présence d'Évariste Galois 1811-1832.* Publication de L'A.P.M.E.P., n.48, 1982.

[33] E. Galois and S. Lie. *Oeuvres mathématiques. Influence de Galois sur le développement des mathématiques.* Éditions Jacques Gabay, 1989.

[34] L. González-Vega, H. Lombardi, T. Recio, and M.-F. Roy. Spécialisation de la suite de Sturm et sous-résultants (I). *Informatique théorique et Applications*, 24(6):561–588, Décembre 1990.

[35] G. Kemper. Generic Polynomials and Nœther's Problem for Linear Groups. IWR-Preprint 95-19, 1995.

[36] J. Kuntzmann. *Méthodes numériques. Interpolation – Dérivées.* Dunos, Paris, 1959.

[37] S. Lang. *Algebraic number theory.* Addison-Wesley publishing company, Inc., 1970.

[38] S. Lang. *Algebra, third edition.* Addison-Wesley publishing compagny, Inc., 1993.

[39] D. Lazard. Sous-résultants. Manuscrit non publié.

[40] T. Lickteig and M.-F. Roy. Cauchy index computation. Manuscrit non publié (à paraître), Novembre 1996.

[41] Q. Liu. Tout groupe fini est un groupe de Galois sur $\mathbb{Q}_p(T)$, d'après Harbater. *Contemporary Mathematics*, 186:261–265, 1995.

[42] R. Loos. Generalized Polynomial Remainder Sequences. *Symbolic and algebraic computation*, Computing, Supplementum(4):115–137, 1982. Springer-Verlag.

[43] G. Malle and B.H. Matzat. Inverse Galois Theory. Universität Heidelberg, Preprint 92-21.

[44] M.P. Malliavin. *Algèbre commutative, applications en géométrie et théorie des nombres.* Masson, 1985.

[45] H. Matsumura. *Commutative Ring Theory.* Cambridge University Press, 1989. Cambridge studies in advanced mathematics 8.

[46] W. Narkiewicz. *Elementary and Analytic Theory of Algebraic Numbers.* Springer-Verlag, 1990. Second Edition.

[47] P. Naudin and C. Quitté. *Cours de DEA 1993-1994 : algorithmique en théorie des corps.* Prépublication de l'Université de Poitiers, janvier 1995.

[48] M. Pohst and H. Zassenhaus. *Algorithmic algebraic number theory,* ch. 2. Cambridge University press, 1989.

[49] C. Quitté. Une démonstration de l'algorithme de Bareiss par l'algèbre extérieure. Manuscrit non publié.

[50] D.J. Saltman. Generic Galois Extensions and Problems in Field Theory. *Advances in Mathematics*, 43:250–283, 1982.

[51] P. Samuel. *Théorie algébrique des nombres*. Hermann, 1967.

[52] J.P. Serre. *Corps locaux*. Hermann, 1968.

[53] J.P. Serre. *Groupes de Galois sur* $\mathbb{Q}$. 689. Séminaire Bourbaki, novembre 1987-88.

[54] J.P. Serre. *Topics in Galois Theory*. Jones and Bartlett Publishers, 1992. Research Notes in Mathematics, Volume 1.

[55] G.W. Smith. Generic Cyclic polynomial of Odd Degree. *Communications in Algebra*, 19(12):3367–3391, 1991.

[56] G.W. Smith. Some Polynomials over $\mathbb{Q}(t)$ and their Galois Groups. Preprint, University of Toledo, 1993.

[57] B.K. Spearman and K.S. Williams. Characterization of solvable quintics $x^5 + ax + b$. *Amer. Math. Month*, 101(10):986–992, december 1994.

[58] M. Suzuki. *Group Theory I*. Springer-Verlag Berlin Heidelberg New York, 1982.

[59] P. Tauvel. *Mathématiques générales pour l'agrégation*. Masson, 1993.

[60] J.G. Thomson. Some finite groups with appear as Gal L/K, where $K \subset \mathbb{Q}(\mu_n)$. *Lecture Notes in Mathematics*, 1195:210–220, 1984.

[61] A. Valibouze. *Mémoire d'Habilitation*. L.I.T.P. 93.61, 1993.

[62] B.L. Van Der Waerden. *Modern Algebra*, volume I. F. Ungar Publishing, 1953.

[63] G. Verriest. *Évariste Galois et la théorie des équations algébriques*. Gauthier-Villars, Paris, 1934.

[64] H. Volklein. *Groups as Galois Groups, An introduction*, volume 53. Cambridge University Press, 1996.

[65] E. Weber. *Lehrbuch der Algebra*. Chelsea Publishing Compagny, 1908.

Errata et addenda

· page 1 : l'Institut Blaise Pascal, l'Université Pierre et Marie Curie et l'Université Paris VI ne font qu'un !

· page 16, ligne 5 avant le bas de page : [...] $\mathfrak{p} = R \cap \mathfrak{p}'$ sa trace sur R [...]

· page 18, dernière ligne de la remarque : [...] extension séparable de k dans k'.

· page 29, ligne 4 en haut de page : Dans [9], l'anneau est supposé réduit et nœthérien. Mais la propriété reste vraie dans un anneau seulement réduit :
– $\bigcup_{\mathfrak{p}\ 1^{\text{er}}\ \text{min.}} \mathfrak{p} \subset \{\text{diviseurs de } 0\}$: si $\mathfrak{p}$ 1^{er} minimal de A alors, dans le localisé $A_{\mathfrak{p}}$, $\mathfrak{p}A_{\mathfrak{p}}$ est le seul idéal premier (car minimal et maximal). Ses éléments sont donc nilpotents : $\forall\ x \in \mathfrak{p},\ \exists\ s \in A \setminus \mathfrak{p},\ \exists\ k \in \mathbb{N}^*,\ sx^{k-1} \neq 0$ et $sx^k = 0$, donc x est diviseur de 0.
– $\{\text{diviseurs de } 0\} \subset \bigcup_{\mathfrak{p}\ 1^{\text{er}}\ \text{min.}} \mathfrak{p}$ par contraposée : si $x \notin \bigcup_{\mathfrak{p}\ 1^{\text{er}}\ \text{min.}} \mathfrak{p}$ et $xy = 0$ alors $xy \in \mathfrak{p}$ pour tout $\mathfrak{p}$ premier, donc $y \in \bigcap_{\mathfrak{p}\ 1^{\text{er}}\ \text{min.}} \mathfrak{p} = \{0\}$ car l'anneau est réduit, donc x n'est pas diviseur de 0.

· page 35, lemme I.7.1 : *Soit A une algèbre libre sur R de base $\mathcal{B}$, $G \in \mathrm{Aut}_R(A)$, et $n = |G| = |\mathcal{B}|$. Alors la matrice $P = \big(g(b)\big)_{\substack{g\in G\\ b\in\mathcal{B}}}$ est inversible (dans $M_n(A)$) si et seulement si A est galoisienne sur R de groupe G.*

· page 54, ligne 6 en bas de page : [...] la $R_{\mathfrak{m}}$-base canonique [...]

· pages 58-59 : tableaux concernant le degré 9

ordre	classe	r
9	$C(9) = 9$	
9	$E(9) = 3[x]3$	
54	$[3^2]S(3)$	$*$
72	$M(9) = E(9) : Q_8$	
72	$E(9) : 8$	
162	$[3^3]S(3) = 3 \wr S(3)$	$*$
432	$E(9) : 2S_4$	$*$
504	$L(9) = PSL(2,8)$	
181440	$A9$	
362880	$S9$	

classe de G	générateurs de G
$[3^2]\, S(3)$	$[(4,5,6)(7,8,9), (1,4,9)(2,5,8)(3,6,7), (4,9)(5,8)(6,7)]$
$[3^3]\, S(3) = 3 \wr S(3)$	$[(1,2,3), (1,4,7)(2,5,8)(3,6,9), (4,7)(5,8)(6,9)]$
$E(9) : 2S_4$	$[(1,2,3)(4,5,6)(7,9,8), (1,4,7)(2,5,9)(3,6,8),$ $(1,8,4,5,2,6,9,7), (4,5,6)(7,8,9)]$

Remarque. Les indices des sous-groupes de $\mathcal{S}_9$ ci-dessus sont trop importants pour que l'on puisse calculer des résolvantes associées.

· page 62, bas de page : il faut prendre $x' = x_1x_2^3 + x_2x_3^3 + x_3x_4^3 + x_4x_1^3$...

· pages 90, section III.4.d : le groupe du polynôme $T^5 - 5T + 12$ est le groupe diédral D_5. En fait, la phrase :

> "Comme $\sqrt{5} \notin \mathbb{Q}$, le groupe de Galois de $T^5 - 5T + 12$ ne peut pas être contenu dans le groupe diédral D_5."

est fausse. Il faut la remplacer par :

> "Comme $\dfrac{d}{\sqrt{5}} = 5 \in \mathbb{Q}$, le groupe de Galois de $T^5 - 5T + 12$ est contenu dans le groupe diédral D_5."

· pages 90-91, section III.4.e : le $\xi = \pm 1$ est inutile, car son changement de signe équivaut à ceux simultanés de e et c. La paramétrisation devient $T^5 + \frac{5e^4(3-4c)}{c^2+1}\, T - \frac{4e^5(11+2c)}{c^2+1}$ (en posant $e = -1$ et $c = 2$, on retrouve $T^5 - 5T + 12$).

De plus, ce polynôme est la composée de $T \mapsto \frac{c^2+1}{e} T$ par

$$T^5 + 5(3-4c)(c^2+1)^3\, T - 4(11+2c)(c^2+1)^4$$

multipliée par $\left(\frac{e}{c^2+1}\right)^5$: ces deux polynômes sont donc "Tschirnhaus-équivalents".

· page 111, autre corollaire du théorème IV.3.1 :

Le coefficient en X^{n-j} du polynôme minimal de r sur $k(t)$ est de degré inférieur à $\frac{j|\Gamma|}{2}$.

Démonstration. On considère $v_\infty = -\deg$ la valuation infinie sur $k(\mathbb{U}_n)[t]$. On considère un prolongement w à E de v_∞. Si e' désigne une racine n-ième quelconque de d, g un élément de $\mathrm{Gal}(E/K)$, on a alors

$$w(d) = -\deg(d) = -\sum_{\gamma \in \Gamma} \big\langle i(\gamma^{-1}) \big\rangle \geq -\frac{n|\Gamma|}{2},$$

$$w(e') = \frac{w(d)}{n} \geq -\frac{|\Gamma|}{2}, \qquad w\big(g(r)\big) = (g^{-1}.w)(r) \geq -\frac{|\Gamma|}{2},$$

Enfin, le coefficient c_{n-j} en X^{n-j} du polynôme minimal de r est une somme de produit de j conjugués de r, on obtient alors $w(c_{n-j}) \geq -\frac{j|\Gamma|}{2}$, i.e. $\deg(c_{n-j}) \leq \frac{j|\Gamma|}{2}$. □

· page 118, autre corollaire du théorème IV.4.1 :

En posant $k = \mathbb{Q}$, dans toute extension abélienne $F/\mathbb{Q}(t)$ construite à partir du théorème IV.4.1, la valuation en $t \in \mathbb{Q}[t]$ est totalement décomposée dans F.

Démonstration. Il est clair que t n'est pas ramifié dans $F = \mathbb{Q}(t, r)$ car il ne l'est dans aucune des extensions $\mathbb{Q}(t, r_j)$. De plus, F est incluse dans $\mathbb{Q}((t))$, donc tout premier au-dessus de t est de degré résiduel 1. Ainsi, il est totalement décomposé dans $F/\mathbb{Q}(t)$. □

· page 132, lemme IV.6.1 : l'application surjective est

$$\begin{array}{ccc} M_0 \wr G & \longrightarrow & M_\rho \rtimes G \\ (m, g) & \longmapsto & \left(\sum_{h \in G} h.m_h \ , \ g \right) \end{array}$$

· page 176, second algorithme : dans la boucle, $\delta \leftarrow \deg(P) - \deg(Q)$ ne sert à rien.

Abstract

The initial and central point of this thesis is the Universal Splitting Ring (U.S.R.) of a monic polynomial f. It is a commutative free algebra spanned by the roots coming from an "universal" decomposition of f. A study of this algebra is made in chapter II. If the discriminant of the polynomial f is invertible, then the U.S.R. is a Galois algebra with group S_n where n is the degree of f. Therefore, a preliminary and necessary study of Galois algebras is made in chapter I. The U.S.R. has been programmed over any commutative ring with unity. Some procedures allow to compute characteristic and minimal polynomials, resolvent polynomials, and relations of algebraic dependence between roots of f, etc. So, the U.S.R. is on one hand a mathematic "substance" and on other hand a formal calculus tool.

Moreover, we develop several applications at the end of chapter II: Computation of the Galois group and the splitting field of a polynomial, research of totally decomposed primes... In the same way, chapter III uses the U.S.R. in order to find explicit formulas which permit to solve the polynomial equation $f = 0$ with radicals when the degree of f is lower than 5.

Chapter IV is an important point of this work and concerns the reciprocal Galois problem: Using the Kummer theory and the ramification in algebraic function fields, we regularly build all semi-direct product groups $A \rtimes G$ where A is a finite Abelian group and G is already regularly built.

Finally, some independent chapters: Chapter A resumes the Bareiss algorithm (computation of the determinant of a matrix) developing a "efficient" formalism. It procures new Euclidean divisibility relations between the subresultant polynomials and any other polynomials having coefficients in an integral domain (chapter B). Using those formulas, we find an "optimal" algorithm which computes the chain of subresultant polynomials.

Key-words

Galois algebra — Universal splitting ring — Galois theory — Solvability by radicals — Explicit regularly realization of Galois groups — Kummer theory — Subresultant algorithm — Exterior algebra

Résumé

Le point initial et central de cette thèse est l'Algèbre de Décomposition Universelle (A.D.U.) d'un polynôme f unitaire. Il s'agit d'une algèbre commutative libre, engendrée par les racines de f provenant d'une factorisation "universelle". Une étude mathématique en est réalisée dans le chapitre II. Si le polynôme f possède un discriminant inversible, l'A.D.U. est une algèbre galoisienne de groupe S_n où n est le degré de f. Par conséquent, une étude préliminaire et nécessaire des algèbres galoisiennes est réalisée dans le chapitre I. La mise en œuvre (en machine) de cette algèbre fonctionne sur tout anneau commutatif unitaire. Quelques procédures permettront d'effectuer des calculs de polynômes caractéristiques, minimaux et résolvantes, de déterminer des relations de dépendance algébrique entre les racines du polynôme f, etc. Ainsi cette algèbre représente à la fois de la matière mathématique et un outil de calcul formel.

Plusieurs applications de l'A.D.U. sont données à la fin du chapitre II : calcul du groupe de Galois et du corps de décomposition d'un polynôme, recherche de premiers totalement décomposés... De même, le chapitre III utilise l'A.D.U. dans le but de donner des formules explicites pour calculer par radicaux les racines d'un polynôme résoluble de degré inférieur à 5.

Point important de ce travail, le chapitre IV concerne le problème de Galois inverse : grâce à la théorie de Kummer et à la ramification dans les corps de fonctions, nous réalisons régulièrement tous les groupes produits semi-directs $A \rtimes G$ où A est un groupe abélien fini et G (fini) est réalisé régulièrement.

Enfin, quelques pages indépendantes de la théorie de Galois : le chapitre A reprend l'algorithme de Bareiss (calcul du déterminant d'une matrice) en développant un formalisme "efficace", donnant naissance à de nouvelles relations de divisibilité euclidienne entre les polynômes sous-résultants et des polynômes quelconques à coefficients dans un anneau intègre (chapitre B). L'utilisation de ces relations nous conduit à un algorithme "optimisé" calculant la chaîne des sous-résultants.

Mots-clés

Algèbre galoisienne — Algèbre de décomposition universelle — Théorie de Galois — Équation résoluble par radicaux — Réalisation régulière explicite — Théorie de Kummer — Algorithme des sous-résultants — Algèbre extérieure