Extensions algébriques : cas général et cas des radicaux

Najid-Zejli Hakima

THESE

présentée à

l' Université Scientifique et Médicale de Grenoble
et à
l' Institut National Polytechnique de Grenoble

pour obtenir le grade de
DOCTEUR DE 3ème CYCLE
«Algorithmique Mathématique»

par

NAJID-ZEJLI HAKIMA

EXTENSIONS ALGEBRIQUES:

CAS GENERAL ET CAS DES RADICAUX

Thèse soutenue le 24 juin 1985 devant la commission d'examen.

J.H. DAVENPORT	Président
J. DELLA-DORA	
M. DUC JACQUET	Examinateurs
D. DUVAL	

UNIVERSITE SCIENTIFIQUE ET MEDICALE DE GRENOBLE

Année universitaire 1982-1983

Président de l'Université : M. TANCHE

MEMBRES DU CORPS ENSEIGNANT DE L'U.S.M.G.

(RANG A)

SAUF ENSEIGNANTS EN MEDECINE ET PHARMACIE

PROFESSEURS DE 1ère CLASSE

ARNAUD Paul	Chimie organique
ARVIEU Robert	Physique nucléaire I.S.N.
AUBERT Guy	Physique C.N.R.S.
AYANT Yves	Physique approfondie
BARBIER Marie-Jeanne	Electrochimie
BARBIER Jean-Claude	Physique expérimentale C.N.R.S. (labo de magnétisme)
BARJON Robert	Physique nucléaire I.S.N.
BARNOUD Fernand	Biosynthèse de la cellulose-Biologie
BARRA Jean-René	Statistiques - Mathématiques appliquées
BELORISKY Elie	Physique
BENZAKEN Claude (M.)	Mathématiques pures
BERNARD Alain	Mathématiques pures
BERTRANDIAS Françoise	Mathématiques pures
BERTRANDIAS Jean-Paul	Mathématiques pures
BILLET Jean	Géographie
BONNIER Jean-Marie	Chimie générale
BOUCHEZ Robert	Physique nucléaire I.S.N.
BRAVARD Yves	Géographie
CARLIER Georges	Biologie végétale
CAUQUIS Georges	Chimie organique
CHIBON Pierre	Biologie animale
COLIN DE VERDIERE Yves	Mathématiques pures
CRABBE Pierre (détaché)	C.E.R.M.O.
CYROT Michel	Physique du solide
DAUMAS Max	Géographie
DEBELMAS Jacques	Géologie générale
DEGRANGE Charles	Zoologie
DELOBEL Claude (M.)	M.I.A.G. Mathématiques appliquées
DEPORTES Charles	Chimie minérale
DESRE Pierre	Electrochimie
DOLIQUE Jean-Michel	Physique des plasmas
DUCROS Pierre	Cristallographie
FONTAINE Jean-Marc	Mathématiques pures
GAGNAIRE Didier	Chimie physique

.../...

GASTINEL Noël	Analyse numérique - Mathématiques appliquées
GERBER Robert	Mathématiques pures
GERMAIN Jean-Pierre	Mécanique
GIRAUD Pierre	Géologie
IDELMAN Simon	Physiologie animale
JANIN Bernard	Géographie
JOLY Jean-René	Mathématiques pures
JULLIEN Pierre	Mathématiques appliquées
KAHANE André (détaché DAFCO)	Physique
KAHANE Josette	Physique
KOSZUL Jean-Louis	Mathématiques pures
KRAKOWIAK Sacha	Mathématiques appliquées
KUPTA Yvon	Mathématiques pures
LACAZE Albert	Thermodynamique
LAJZEROWICZ Jeannine	Physique
LAJZEROWICZ Joseph	Physique
LAURENT Pierre	Mathématiques appliquées
DE LEIRIS Joël	Biologie
LLIBOUTRY Louis	Géophysique
LOISEAUX Jean-Marie	Sciences nucléaires I.S.N.
LOUP Jean	Géographie
MACHE Régis	Physiologie végétale
MAYNARD Roger	Physique du solide
MICHEL Robert	Minéralogie et pétrographie (géologie)
MOZIERES Philippe	Spectrométrie - Physique
OMONT Alain	Astrophysique
OZENDA Paul	Botanique (biologie végétale)
PAYAN Jean-Jacques (détaché)	Mathématiques pures
PEBAY PEYROULA Jean-Claude	Physique
PERRIAUX Jacques	Géologie
PERRIER Guy	Géophysique
PIERRARD Jean-Marie	Mécanique
RASSAT André	Chimie systématique
RENARD Michel	Thermodynamique
RICHARD Lucien	Biologie végétale
RINAUDO Marguerite	Chimie CERMAV
SENGEL Philippe	Biologie animale
SERGERAERT Francis	Mathématiques pures
SOUTIF Michel	Physique
VAILLANT François	Zoologie
VALENTIN Jacques	Physique nucléaire I.S.N.
VAN CUTSEN Bernard	Mathématiques appliquées
VAUQUOIS Bernard	Mathématiques appliquées
VIALON Pierre	Géologie

PROFESSEURS DE 2ème CLASSE

ADIBA Michel	Mathématiques pures
ARMAND Gilbert	Géographie

.../...

AURIAULT Jean-Louis	Mécanique
BEGUIN Claude (M.)	Chimie organique
BOEHLER Jean-Paul	Mécanique
BOITET Christian	Mathématiques appliquées
BORNAREL Jean	Physique
BRUN Gilbert	Biologie
CASTAING Bernard	Physique
CHARDON Michel	Géographie
COHENADDAD Jean-Pierre	Physique
DENEUVILLE Alain	Physique
DEPASSEL Roger	Mécanique des fluides
DOUCE Roland	Physiologie végétale
DUFRESNOY Alain	Mathématiques pures
GASPARD François	Physique
GAUTRON René	Chimie
GIDON Maurice	Géologie
GIGNOUX Claude (M.)	Sciences nucléaires I.S.N.
GUITTON Jacques	Chimie
HACQUES Gérard	Mathématiques appliquées
HERBIN Jacky	Géographie
HICTER Pierre	Chimie
JOSELEAU Jean-Paul	Biochimie
KERCKOVE Claude (M.)	Géologie
LE BRETON Alain	Mathématiques appliquées
LONGEQUEUE Nicole	Sciences nucléaires I.S.N.
LUCAS Robert	Physiques
LUNA Domingo	Mathématiques pures
MASCLE Georges	Géologie
NEMOZ Alain	Thermodynamique (CNRS - CRTBT)
OUDET Bruno	Mathématiques appliquées
PELMONT Jean	Biochimie
PERRIN Claude (M.)	Sciences nucléaires I.S.N.
PFISTER Jean-Claude (détaché)	Physique du solide
PIBOULE Michel	Géologie
PIERRE Jean-Louis	Chimie organique
RAYNAUD Hervé	Mathématiques appliquées
ROBERT Gilles	Mathématiques pures
ROBERT Jean-Bernard	Chimie physique
ROSSI André	Physiologie végétale
SAKAROVITCH Michel	Mathématiques appliquées
SARROT REYNAUD Jean	Géologie
SAXOD Raymond	Biologie animale
SOUTIF Jeanne	Physique
SCHOOL Pierre-Claude	Mathématiques appliquées
STUTZ Pierre	Mécanique
SUBRA Robert	Chimie
VIDAL Michel	Chimie organique
VIVIAN Robert	Géographie

INSTITUT NATIONAL POLYTECHNIQUE DE GRENOBLE

Année universitaire 1982-1983

Président de l'Université : D. BLOCH

Vice-Président : René CARRE
Hervé CHERADAME
Marcel IVANES

PROFESSEURS DES UNIVERSITES :

ANCEAU François	E.N.S.I.M.A.G.
BARRAUD Alain	E.N.S.I.E.G.
BAUDELET Bernard	E.N.S.I.E.G.
BESSON Jean	E.N.S.E.E.G.
BLIMAN Samuel	E.N.S.E.R.G.
BLOCH Daniel	E.N.S.I.E.G.
BOIS Philippe	E.N.S.H.G.
BONNETAIN Lucien	E.N.S.E.E.G.
BONNIER Etienne	E.N.S.E.E.G.
BOUVARD Maurice	E.N.S.H.G.
BRISSONNEAU Pierre	E.N.S.I.E.G.
BUYLE BODIN Maurice	E.N.S.E.R.G.
CAVAIGNAC Jean-François	E.N.S.I.E.G.
CHARTIER Germain	E.N.S.I.E.G.
CHENEVIER Pierre	E.N.S.E.R.G.
CHERADAME Hervé	U.E.R.M.C.P.P.
CHERUY Arlette	E.N.S.I.E.G.
CHIAVERINA Jean	U.E.R.M.C.P.P.
COHEN Joseph	E.N.S.E.R.G.
COUMES André	E.N.S.E.R.G.
DURAND Francis	E.N.S.E.E.G.
DURAND Jean-Louis	E.N.S.I.E.G.
FELICI Noël	E.N.S.I.E.G.
FOULARD Claude	E.N.S.I.E.G.
GENTIL Pierre	E.N.S.E.R.G.
GUERIN Bernard	E.N.S.E.R.G.
GUYOT Pierre	E.N.S.E.E.G.
IVANES Marcel	E.N.S.I.E.G.
JAUSSAUD Pierre	E.N.S.I.E.G.
JOUBERT Jean-Claude	E.N.S.I.E.G.
JOURDAIN Geneviève	E.N.S.I.E.G.
LACOUME Jean-Louis	E.N.S.I.E.G.
LATOMBE Jean-Claude	E.N.S.I.M.A.G.

.../...

LESSIEUR Marcel	E.N.S.H.G.
LESPINARD Georges	E.N.S.H.G.
LONGEQUEUE Jean-Pierre	E.N.S.I.E.G.
MAZARE Guy	E.N.S.I.M.A.G.
MOREAU René	E.N.S.H.G.
MORET Roger	E.N.S.I.E.G.
MOSSIERE Jacques	E.N.S.I.M.A.G.
PARIAUD Jean-Charles	E.N.S.E.E.G.
PAUTHENET René	E.N.S.I.E.G.
PERRET René	E.N.S.I.E.G.
PERRET Robert	E.N.S.I.E.G.
PIAU Jean-Michel	E.N.S.H.G.
POLOUJADOFF Michel	E.N.S.I.E.G.
POUPOT Christian	E.N.S.E.R.G.
RAMEAU Jean-Jacques	E.N.S.E.E.G.
RENAUD Maurice	U.E.R.M.C.P.P.
ROBERT André	U.E.R.M.C.P.P.
ROBERT François	E.N.S.I.M.A.G.
SABONNADIERE Jean-Claude	E.N.S.I.E.G.
SAUCIER Gabrielle	E.N.S.I.M.A.G.
SCHLENKER Claire	E.N.S.I.E.G.
SCHLENKER Michel	E.N.S.I.E.G.
SERMET Pierre	E.N.S.E.R.G.
SILVY Jacques	U.E.R.M.C.P.P.
SOHM Jean-Claude	E.N.S.E.E.G.
SOUQUET Jean-Louis	E.N.S.E.E.G.
VEILLON Gérard	E.N.S.I.M.A.G.
ZADWORNY François	E.N.S.E.R.G.

PROFESSEURS ASSOCIES

BASTIN Georges	E.N.S.H.G.
BERRIL John	E.N.S.H.G.
CARREAU Pierre	E.N.S.H.G.
GANDINI Alessandro	U.E.R.M.C.P.P.
HAYASHI Hirashi	E.N.S.I.E.G.

PROFESSEURS UNIVERSITE DES SCIENCES SOCIALES (Grenoble II)

BOLLIET Louis
Chatelin Françoise

PROFESSEURS E.N.S. Mines de Saint-Etienne

RIEU Jean
SOUSTELLE Michel

CHERCHEURS DU C.N.R.S.

FRUCHART Robert	Directeur de Recherche
VACHAUD Georges	Directeur de Recherche

.../...

ALLIBERT Michel	Maître de Recherche
ANSARA Ibrahim	Maître de Recherche
ARMAND Michel	Maître de Recherche
BINDER Gilbert	
CARRE René	Maître de Recherche
DAVID René	Maître de Recherche
DEPORTES Jacques	
DRIOLE Jean	Maître de Recherche
GIGNOUX Damien	
GIVORD Dominique	
GUELIN Pierre	
HOPFINGER Emil	Maître de Recherche
JOUD Jean-Charles	Maître de Recherche
KAMARINOS Georges	Maître de Recherche
KLEITZ Michel	Maître de Recherche
LANDAU Ioan-Dore	Maître de Recherche
LASJAUNIAS J.C.	
MERMET Jean	Maître de Recherche
MUNIER Jacques	Maître de Recherche
PIAU Monique	
PORTESEIL Jean-Louis	
THOLENCE Jean-Louis	
VERDILLON André	

CHERCHEURS du MINISTERE de la RECHERCHE et de la TECHNOLOGIRE (Directeurs et Maîtres de Recherches, ENS Mines de St. Etienne)

LESBATS Pierre	Directeur de Recherche
BISCONDI Michel	Maître de Recherche
KOBYLANSKI André	Maître de Recherche
LE COZE Jean	Maître de Recherche
LALAUZE René	Maître de Recherche
LANCELOT Francis	Maître de Recherche
THEVENOT François	Maître de Recherche
TRAN MINH Canh	Maître de Recherche

PERSONNALITES HABILITEES à DIRIGER des TRAVAUX de RECHERCHE (Décision du Conseil Scientifique)

ALLIBERT Colette	E.N.S.E.E.G.
BERNARD Claude	E.N.S.E.E.G.
BONNET Rolland	E.N.S.E.E.G.
CAILLET Marcel	E.N.S.E.E.G.
CHATILLON Catherine	E.N.S.E.E.G.
CHATILLON Christian	E.N.S.E.E.G.
COULON Michel	E.N.S.E.E.G.
DIARD Jean-Paul	E.N.S.E.E.G.
EUSTAPOPOULOS Nicolas	E.N.S.E.E.G.
FOSTER Panayotis	E.N.S.E.E.G.

.../...

GALERIE Alain	E.N.S.E.E.G.
HAMMOU Abdelkader	E.N.S.E.E.G.
MALMEJAC Yves	E.N.S.E.E.G. (CENG)
MARTIN GARIN Régina	E.N.S.E.E.G.
NGUYEN TRUONG Bernadette	E.N.S.E.E.G.
RAVAINE Denis	E.N.S.E.E.G.
SAINFORT	E.N.S.E.E.G. (CENG)
SARRAZIN Pierre	E.N.S.E.E.G.
SIMON Jean-Paul	E.N.S.E.E.G.
TOUZAIN Philippe	E.N.S.E.E.G.
URBAIN Georges	E.N.S.E.E.G. (Laboratoire des ultra-réfractaires ODEILLON)
GUILHOT Bernard	E.N.S. Mines Saint Etienne
THOMAS Gérard	E.N.S. Mines Saint Etienne
DRIVER Julien	E.N.S. Mines Saint Etienne
BARIBAUD Michel	E.N.S.E.R.G.
BOREL Joseph	E.N.S.E.R.G.
CHOVET Alain	E.N.S.E.R.G.
CHEHIKIAN Alain	E.N.S.E.R.G.
DOLMAZON Jean-Marc	E.N.S.E.R.G.
HERAULT Jeanny	E.N.S.E.R.G.
MONLLOR Christian	E.N.S.E.R.G.
BORNARD Guy	E.N.S.I.E.G.
DESCHIZEAU Pierre	E.N.S.I.E.G.
GLANGEAUD François	E.N.S.I.E.G.
KOFMAN Walter	E.N.S.I.E.G.
LEJEUNE Gérard	E.N.S.I.E.G.
MAZUER Jean	E.N.S.I.E.G.
PERARD Jacques	E.N.S.I.E.G.
REINISCH Raymond	E.N.S.I.E.G.
ALEMANY Antoine	E.N.S.H.G.
BOIS Daniel	E.N.S.H.G.
DARVE Félix	E.N.S.H.G.
MICHEL Jean-Marie	E.N.S.H.G.
OBLED Charles	E.N.S.H.G.
ROWE Alain	E.N.S.H.G.
VAUCLIN Michel	E.N.S.H.G.
WACK Bernard	E.N.S.H.G.
BERT Didier	E.N.S.I.M.A.G.
CALMET Jacques	E.N.S.I.M.A.G.
COURTIN Jacques	E.N.S.I.M.A.G.
COURTOIS Bernard	E.N.S.I.M.A.G.
DELLA DORA Jean	E.N.S.I.M.A.G.
FONLUPT Jean	E.N.S.I.M.A.G.
SIFAKIS Joseph	E.N.S.I.M.A.G.
CHARUEL Robert	U.E.R.M.C.P.P.
CADET Jean	C.E.N.G.
COEURE Philippe	C.E.N.G. (LETI)

.../...

DELHAYE Jean-Marc	C.E.N.G. (STT)
DUPUY Michel	C.E.N.G. (LETI)
JOUVE Hubert	C.E.N.G. (LETI)
NICOLAU Yvan	C.E.N.G. (LETI)
NIFENECKER Hervé	C.E.N.G.
PERROUD Paul	C.E.N.G.
PEUZIN Jean-Claude	C.E.N.G. (LETI)
TAIEB Maurice	C.E.N.G.
VINCENDON Marc	C.E.N.G.

LABORATOIRES EXTERIEURS

DEMOULIN Eric	C.N.E.T.
DEVINE	C.N.E.T. (R.A.B.)
GERBER Roland	C.N.E.T.
MERCKEL Gérard	C.N.E.T.
PAULEAU Yves	C.N.E.T.
GAUBERT C.	I.N.S.A. Lyon

A mon mari
à Imane et
à toute ma famille

Je tiens à exprimer toute ma reconnaissance à Monsieur Jean DELLA DORA pour m'avoir accueilli au sein de l'équipe Algorithmique Mathématique et de m'avoir guidé dans ce travail. Sa sympathie, ses conseils et ses services ont beaucoup compté pour moi.

Je suis très sensible à l'honneur que me fait Monsieur James H. DAVENPORT en acceptant de présider ce jury. Il m'a beaucoup enseigné et a su m'intéresser au problèmes des extensions par radicaux, qu'il me permette de lui exprimer ma respectueuse gratitude.

Je remercie vivement Mademoiselle Dominique DUVAL pour son travail de pionnier qu'elle a effectué, elle m'a beaucoup appris sur l'arithmétique et sur la théorie de Galois. Pendant d'innombrables heures, elle m'a soutenue, critiquée, encouragée et conseillée. Sans elle, il n'aurait jamais été question pour moi de faire une thèse sur les extensions de corps. Je lui suis très reconnaissante.

Mes remerciements vont également à Monsieur Marc DUC-JACQUET d'avoir bien voulu faire partie de ce jury.

Ce travail doit encore à Mesdemoiselles Evelyne TOURNIER et Claire DI-CRESCENZO qui m'ont initiées et beaucoup appris sur la programmation, qu'elles soient remerciées ici.

Je voudrais remercier très sincèrement Madame BICAIS qui a effectué avec compétence et amabilité la frappe de cette thèse, ainsi que le Service de Reprographie pour la qualité de leur travail.

Enfin, que tous les membres de l'équipe reçoivent mes sincères remerciements pour leur sympathie.

TABLE DES MATIERES

CHAPITRE 2 - ETUDE DES EXTENSIONS DE Q ENGENDREES PAR DES RADICAUX

INTRODUCTION GENERALE

Ce travail est consacré à l'étude des méthodes de calcul dans des corps engendrés par les rationnels et par un nombre fini d'éléments algébriques, c'est-à-dire de racines de polynômes à coefficients rationnels.

Le but est d'obtenir des algorithmes pour effectuer les opérations "arithmétiques" élémentaires : addition, multiplication, inverse d'un élément non nul, test d'égalité entre deux éléments.

Ce dernier problème (test d'égalité) est en fait le problème le plus important. Il faut par exemple reconnaître que les nombres algébriques $\sqrt{6}$ et $\sqrt{2}.\sqrt{3}$ sont égaux.

Exemple :

Soit E l'extension de Q engendrée par une racine du polynôme X^2-2, c'est-à-dire $E = Q(\sqrt{2})$.
Tout élément x de E s'écrit de manière unique sous la forme $x = a\sqrt{2}+b$ où a et b appartiennent à Q.

Les opérations élémentaires sur E sont définies par :

soit $x,y \in E$ avec $x = a\sqrt{2}+b$, $y = a'\sqrt{2}+b'$.

* $x = y \iff a = a'$ et $b = b'$
* $x + y = (ab'+ba')\sqrt{2} + bb' + 2aa'$
* si $x \neq 0$, $x^{-1} = \dfrac{1}{2a^2-b^2}(a\sqrt{2}-b)$ ($2a^2-b^2$ ne peut s'annuler sur Q que si $a = b = 0$ c'est-à-dire si $X = 0$).

Remargue :

On pourrait être tenté de dire qu'il suffit de prendre une bonne approximation numérique de $\sqrt{2}$ dans Q (en utilisant la méthode de Newton par exemple). Cette approche a été étudiée par M. Mignotte. Le plus difficile est de savoir, selon le problème posé, définir les "bonnes" approximations numériques des nombres algébriques.

Si on a à travailler dans une extension $Q(\alpha_1,\ldots,\alpha_n)$ de Q, où chaque α_i vérifie $P_i(\alpha_i) = 0$, $P_i \in Q[X]$ et degré $(P_i) = k_i$, alors : $Q(\alpha_1,\ldots,\alpha_n)$ a une structure d'espace vectoriel sur Q. De plus tout élément de $Q(\alpha_1,\ldots,\alpha_n)$ s'exprime sous forme de combinaison linéaire des quantités :

$\alpha_1^{i_1}.\ \alpha_2^{i_2}\ldots\ \alpha_n^{i_n}$ où $0 \leq i_j < k_j$ pour tout $j \in \{1,\ldots,n\}$.

Donc ces quantités forment une famille S génératrice du Q espace vectoriel $Q(\alpha_1\ldots\alpha_n)$. Cependant l'écriture d'un élément de $Q(\alpha_1\ldots\alpha_n)$ sous forme de combinaison linéaire des éléments de S n'est unique que si S est une base.

Cette unicité d'écriture est nécessaire car elle permet d'identifier un élément à zéro ; or ceci est la première chose à avoir pour décrire l'arithmétique dans un corps, parce que la structure d'un corps interdit la division par zéro et aussi parce que a=b si et seulement si a-b = 0.

Dans le premier chapitre, nous exposons la démarche mathématique usuelle, utilisant la notion d'élément primitif d'une extension. Elle est très simple à décrire, mais nous montrons que son application est très coûteuse. Nous énonçons aussi dans ce chapitre quelques résultats qui seront utiles par la suite.

Dans le deuxième chapitre, nous essayons de construire une base de $Q(\alpha_1,\ldots,\alpha_n)$ en factorisant successivement les polynômes P_i sur les corps $Q(\alpha_1,\ldots,\alpha_{i-1})$. Cette méthode fait intervenir de nombreuses factorisations de polynômes sur des corps de nombres algébriques, ce qui est encore assez coûteux.

Enfin, dans le troisième chapitre, qui constitue la partie essentielle de cette thèse, nous considérons le cas particulier, mais très courant, où les nombres algébriques qui engendrent l'extension étudiée sont tous des radicaux (non imbriqués) de rationnels. Nous proposons un nouvel algorithme, n'utilisant ni élément primitif ni factorisation, mais fondé sur un théorème de Schinzel. De façon schématique, l'idée utilisée dans ce chapitre est la suivante :

si n est un entier impair, si ξ est une racine nième "bien choisie", d'un rationnel a, et si n' est le degré de l'extension $Q(\xi)/Q$, alors il existe un rationnel a' tel que $\xi = \sqrt[n']{a'}$.

Les problèmes rencontrés dans ce travail proviennent du fait que c'est faux lorsque n est pair. Par exemple, $\sqrt[n]{-4}$ engendre une extension de degré 2 sur Q (car $\sqrt[n]{-4} = 1+\sqrt{-1}$) cependant ce n'est pas une racine carrée de rationnel.

Nous montrons qu'en travaillant sur le corps $Q(\sqrt[4]{-1})$ (noté K_0), qui contient également $\sqrt{2}$, ces difficultés peuvent être surmontées.

Nous insistons sur le fait que les radicaux étudiés sont des racines de rationnels, ce ne sont pas des racines d'éléments de K_0. Par exemple nous saurons reconnaître que $\sqrt[4]{-4}$ est dans K_0, mais nous ne saurons pas exprimer $\sqrt{9+4\sqrt{2}}$ (qui est la racine carrée d'un élément de K_0) comme $1+2\sqrt{2}$.

L'algorithme est explicité dans le cas de deux radicaux. Les démonstrations font intervenir de l'arithmétique et de la théorie de Galois et sont assez complexes. Par contre l'algorithme lui-même est très simple.

La généralisation à un nombre quelconque de radicaux ne devrait guère poser que des problèmes de notations. Cela constituera, avec l'implantation de l'algorithme le but d'un travail ultérieur.

QUELQUES EXEMPLES D'APPLICATION

1. Equations Différentielles

Soit Λ un opérateur différentiel $\Lambda = \sum_{i=0}^{n} a_i(x)\partial^i$, où $a_i \in Q[X]$, et $\partial = \frac{d}{dX}$. Les zéros de a_n et éventuellement le point à l'infini constituent les points singuliers des solutions de $\Lambda y = 0$.

Si on veut procéder numériquement, on ne pourra localiser les singularités du fait que les solutions sont analytiques dans le voisinage immédiat d'un point singulier, ce qui justifie un travail formel.

Supposons qu'on veuille travailler en une singularité λ, une démarche possible serait de se placer dans $Q(\lambda)$, et pour cela on peut faire le travail suivant : on décompose a_n en facteurs irréductibles dans Q, et on choisit un facteur $a_{n,\lambda}$, $a_{n,\lambda}$ étant irréductible dans Q c'est le polynôme minimal d'une racine λ de a_n et par suite $Q(\lambda)$ est isomorphe à $Q[X]/(a_{n,\lambda})$

Dans le cas où la singularité est régulière la solution est de la forme $y = x^{\mu}y^*$ où μ vérifie une équation polynomiale à coefficients dans $Q(\lambda)$. Soit $F_\lambda(\mu) = 0$. Cette équation se place donc dans $Q(\lambda,\mu)$ pour continuer la résolution de l'équation différentielle, dans ce cas $y^* \in Q(\lambda,\mu)\{X\}$ où $y^* \in Q(\lambda,\mu)\{X\}[\text{Log } X]$ (ie. polynôme en Log X à coefficients dans $Q(\lambda,\mu)\{X\}$).

Dans le cas d'une singularité irrégulière on obtient des développements en série de Laurent des solutions. On a les mêmes problèmes et on est ramené à travailler dans des extensions $Q(\lambda_1,\ldots,\lambda_k)$ de Q.

2. Forme de Jordan d'une matrice

Soit M une matrice carrée à coefficients dans Q, dont on veut déterminer la forme de Jordan. On procède généralement de la manière suivante : on cherche la forme de Smith de M, on en déduit les facteurs invariants. Soit $P_1,\ldots,P_r$. On les décompose en facteurs irréductibles pour avoir les diviseurs élémentaires. Si ces diviseurs élémentaires sont des puissances de polynômes de degré 1, on peut construire immédiatement la forme de Jordan de M, sinon, ce qui est le cas le plus fréquent puisque Q n'est pas algébriquement clos, on doit chercher les racines des diviseurs élémentaires.

Dans le premier chapitre l'étude faite consiste à déterminer une extension de Q engendrée par un seul élément où tous les diviseurs élémentaires se décomposent en polynôme de degré 1 et alors on peut déterminer la forme de Jordan de M.

CHAPITRE 1 - PREMIERE APPROCHE

ELEMENT PRIMITIF D'UNE EXTENSION ALGEBRIQUE DE $\mathbb{Q}$

INTRODUCTION

Etant donné une extension algébrique de degré fini de Q de la forme $Q(\alpha_1,\ldots,\alpha_n)$ où les α_i sont définis par $P_i(\alpha_i)=0$ avec $P_i(X) \in Q(\alpha_1,\ldots,\alpha_{i-1})[X]$. Nous allons essayer dans ce chapitre de construire un élément γ tel que $Q(\alpha_1,\ldots,\alpha_n) = Q(\gamma)$, et d'exprimer les α_i dans $Q(\gamma)$.

Ceci a l'avantage de simplifier les règles de calcul et d'exprimer toute expression dans $Q(\alpha_1\ldots\alpha_n)$ avec le seul paramètre γ .

En effet si R est le polynôme minimal de γ (cf. Rappel) dans Q et r = degré(R) alors $\{1,\gamma,\ldots,\gamma^{r-1}\}$ forme une base du Q-espace vectoriel $Q(\gamma)$. Pour déterminer les opérations élémentaires dans $Q(\gamma)$ nous allons utiliser l'isomorphisme entre $Q(\gamma)$ et $Q[X]/(R)$ qui se traduit par une représentation de γ par X avec la règle $R(X) \cong 0$.

I - NOTATION - RAPPEL

Extension de corps

Soit L et K deux corps. Si $K \subset L$ alors L est un surcorps de K.
On dit que L est une extension de K et on note L/K.
Exemple : $\mathbb{R}/Q$, $\mathbb{C}/\mathbb{R}$, $\mathbb{C}/Q$.

Degré d'une extension de corps

Soit L/K une extension de K, L peut être muni d'une structure d'espace vectoriel sur K.

On appelle degré de L/K et on note [L:K] la dimension du K-espace vectoriel L

Exemple : $[\mathbb{C}:\mathbb{R}]=2$.

Corps de décomposition d'un polynôme

Soit K un corps et $P \in K[X]$, un polynôme en X à coefficients dans K. Le corps de décomposition de P est la plus petite extension de K contenant toutes les racines de P, on la note $K(\alpha_1,\ldots,\alpha_n)$ où les α_i sont les racines de P. C'est aussi le plus petit surcorps de K obtenu en adjoignant à K les racines de P .

Exemple : $P(X) = X^2+X+1$; $P \in Q[X]$. Le corps de décomposition de P(X) est $Q(j) = \{a+bj\ ;\ a,b \in Q\}$, où $j = e^{\frac{2i\pi}{3}}$.

Polynôme minimal.

Soit K un corps et α un élément algébrique dans K (α vérifie une équation algébrique sur K). On appelle polynôme minimal de α dans K le polynôme $P \in K[X]$ unitaire, irréductible sur K et vérifiant $P(\alpha) =0$.

II - QUELQUES RESULTATS SUR LES EXTENSIONS ALGEBRIQUES DE CORPS

Extension algébrique

L/K est dite algébrique si tout élément de L est algébrique dans K, c'est à dire vérifie une équation algébrique à coefficients dans K.

Exemple : toute extension de degré fini est algébrique [Lan]
$Q(\sqrt{2})/Q$ est algébrique, $\mathbb{R}/Q$ n'est pas algébrique.

Extension galoisienne

L/K est dite galoisienne si L est le corps de décomposition d'un polynôme irréductible à coefficients dans K.

Exemple : $Q(\sqrt{2})/Q$ est galoisienne
$Q(\sqrt[3]{2})/Q$ n'est pas galoisienne car $P = X^3 - 2$ est le polynôme minimal de $\sqrt[3]{2}$ sur Q et $Q(\sqrt[3]{2})$ ne contient pas $j\sqrt[3]{2}$ qui est aussi racine de p.

Lemme 2.1

Soit K un corps, α un élément algébrique sur K et P le polynôme minimal de α SUR K.
Alors nous avons un isomorphisme entre $K(\alpha)$ et $K[X]/(P)$,
où (P) est l'idéal engendré par P.

Démonstration

Considérons l'homomorphisme Φ : $K[X] \to K(\alpha)$
$R(X) \to R(\alpha)$. $R \in K[X]$.

Φ est l'homomorphisme de K-algèbres de K[X] dans $K(\alpha)$ qui substitue α à X
le noyau de Φ est l'idéal engendré par P, noté (P).
En effet, $\Phi(P(X)) = P(\alpha) = 0$ et $\Phi(R(X)) = 0$ entraîne $R(\alpha) = 0$.
Or $R(\alpha) = 0$ et P est le polynôme minimal de α dans K entraîne que
P(X)/R(X) ou encore $R \in (P)$, d'où $K(\alpha)$ est isomorphe à $K[X]/(P)$
(il est facile de voir que Φ est surjectif).

Conséquence

Nous allons dans toute l'étude travailler souvent dans $K[X]/(P)$ au lieu de $K(\alpha)$. Ceci a l'avantage de représenter toutes les racines de P par X et par suite à faire une seule étude pour toutes les racines de P au lieu de refaire plusieurs fois le même calcul formel. Néanmoins ainsi on ne pourra "localiser" une racine formelle .

Propriété 2.2

Soit $P \in K[X]$, $d^\circ P = n$.
Si P est irréductible sur K[X] et si α est une racine de P alors :
$[K(\alpha) : K] = n$.

Démonstration : évidente en utilisant le lemme 2.1.
$K(\alpha)$ est isomorphe à $K[X]/(P)$ et $K[X]/(P)$ est un K-espace vectoriel de dimension le degré de P, d'où $[K(\alpha):K] = n$.

Propriété 2.3

Soit $P \in K[X]$ un polynôme irréductible de degré n et de racines $\alpha_1,\ldots,\alpha_n$. Alors on a : $[K(\alpha_1,\ldots,\alpha_n) : K] \leq n!$

Démonstration

Lemme

Soit K, L_1, L_2 3 corps tels que $K \subset L_1 \subset L_2$.
Alors $[L_2:K] = [L_2:L_1] \times [L_1:K]$ [Lan]

Nous avons puisque P est irréductible $[K(\alpha_1) : K] = n$.
α_2 vérifie dans $K(\alpha_1)$ l'équation $\frac{P(X)}{X-\alpha_1} = 0$ donc $[K(\alpha_1)(\alpha_2) : K(\alpha_1)] \leq n-1$
et ainsi de suite, α_i vérifie une équation de degré n-i+1 dans $K(\alpha_1,\ldots,\alpha_{i-1})$ donc $[K(\alpha_1,\ldots,\alpha_{i-1})(\alpha_i) : K(\alpha_1\ldots\alpha_{i-1})] \leq n-i+1$
d'où d'après le lemme :

$$[K(\alpha_1\ldots\alpha_n):K] = [K(\alpha_1\ldots\alpha_n):K(\alpha_1\ldots\alpha_{n-1})]\,[K(\alpha_1\ldots\alpha_{n-1}):K(\alpha_1\ldots\alpha_{n-2})]\ldots$$

$$\ldots\times [K(\alpha_1):K] \leq 1.2\ldots(n-i+1)\ldots n = n!$$

d'où $[K(\alpha_1\ldots\alpha_n):K] \leq n!$.

Remarque 2.4

L'égalité $[K(\alpha_1,\ldots,\alpha_n):K] = n!$ peut être atteinte : on verra que le corps de décomposition du polynôme $p = X^4+2X^3+5$ est de degré 24 (=4!).
En comparant les propriétés 2.2 et 2.3, on voit qu'il faut essayer, autant que possible, de travailler avec une seule racine de p. On sera dans un espace vectoriel de degré n, alors que le degré peut atteindre n! s'il faut travailler simultanément avec toutes les racines de p.

Le résultat suivant est à la base de la méthode étudiée dans ce chapitre :

Théorème de l'élément primitif

Soit K un corps de caractéristique nulle et L/K une extension algébrique de degré fini sur K (ie $[L:K] < \infty$).
Alors il existe un élément x appartenant à L tel que $L = K(x)$.
x est appelé un élément primitif de l'extension L/K [Lan]

III - RESULTANT DE DEUX POLYNÔMES

Définition 3.1

Soit p et q deux polynômes de Q[X], on appelle résultant de p et q par rapport à X et on note Résultant (p(X), q(X),X) le déterminant de la matrice de Sylvester associée à p et à q.

c'est à dire si $p = a_0X^n + \ldots + a_n$

$q = b_0X^m + \ldots + b_m$.

$$\text{Résultant } (p,q,X) = \begin{vmatrix} a_0 & \cdots & a_n & & \\ & a_0 & \cdots & a_n & \\ & & \ddots & & \\ & & a_0 & \cdots & a_n \\ b_0 & \cdots & b_m & & \\ & b_0 & \cdots & b_m & \\ & & \ddots & & \\ & & b_0 & \cdots & b_m \end{vmatrix} \begin{matrix} \\ \\ \\ \left.\vphantom{\begin{matrix}a\\a\\a\end{matrix}}\right\} m \text{ lignes} \\ \\ \\ \left.\vphantom{\begin{matrix}a\\a\\a\end{matrix}}\right\} n \text{ lignes} \end{matrix}$$

c'est un déterminant $(n+m) \times (n+m)$.

Propriété 3.2

Soit $P(X) = a_0X^n + \ldots + a_n$, $q(X) = b_0X^m + \ldots + b_m$.
$\alpha_1, \ldots \alpha_n, \beta_1, \ldots, \beta_m$ les racines respectives de p et q.
Alors

$$\text{Résultant}(p,q,X) = a_0^m \prod_{i=1}^{n} q(\alpha_i) = (-1)^{n*n} b_0^n \prod_{i=1}^{m} p(\beta_i) = a_0^m b_0^n \prod_{i,j} (\alpha_i - \beta_j)$$

Propriété 3.3

Si $q = q_1 \times q_2$, q_1, q_2 appartenant à Q[X].
alors Résultant(p,q,x) = Résultant (p,q_1,x). Résultant $(p.q_2,x)$.

IV - ELEMENT PRIMITIF D'UNE EXTENSION DE Q ENGENDREE PAR n ELEMENTS

Construction de l'élément primitif d'une extension de Q engendrée par deux éléments.

Dans ce paragraphe, on se propose de chercher l'élément primitif γ d'une extension $Q(\alpha,\beta)$ où α et β vérifient respectivement $p(\alpha) = 0$ et $q(\beta) = 0$ avec p et q deux polynômes de Q[X] de degrés respectifs n et m.

Nous voulons construire un polynôme $r \in Q[X]$ irréductible à partir des deux polynômes p et q et qui soit le polynôme minimal de γ. Nous aurons alors $Q(\alpha,\beta) = Q(\gamma) \simeq Q[X]/(r)$, et nous essaierons d'exprimer α et β dans $Q[X]/(r)$.
Nous cherchons γ sous la forme $\beta+s\alpha$, avec s entier.

Premier cas : p est irréductible dans Q[X].

p est alors le polynôme minimal de ses racines et par suite $Q(\alpha)$ est isomorphe à $Q[X]/(p)$.

Donc chercher l'élément primitif de $Q(\alpha,\beta)$ c'est chercher l'élément primitif de $Q[X]/(p)(\beta)$, β vérifiant $q(\beta) = 0$.

Or q(y) appartient à Q[Y] donc aussi à $Q[X]/(p)[Y]$.

On construira $r \in Q[Y]$ irréductible, tel que $Q[Y]/(r)$ soit isomorphe à $Q[X]/(p)(\beta)$.

Deuxième cas : p n'est pas irréductible dans Q[X].

On le décompose en facteurs irréductibles dans Q, et on choisit un facteur irréductible. On est ramené au premier cas.

Définition 4.1

Un polynôme $R \in Q[X]$ est dit quadratfrei si et seulement si pgcd(R,R') = constante où R' est la dérivée de R par rapport à X.

Cela revient à dire que la décomposition de R en produit de polynômes irréductibles dans Q[X] ne contient aucun facteur multiple.

Théorème 4.2

Soit $p \in Q[X]$ un polynôme irréductible et $F_X(Y) \in Q[X]/(P)[Y]$.
Alors l'ensemble des entiers s tels que Résultant $(p(X), G_X(Y), X)$ ne soit pas quadratfrei, où $G_X(Y) = F_X(Y-sX)$, est un ensemble fini.

On démontrera ce théorème à l'aide des deux lemmes suivants.

Lemme 1

Avec les mêmes hypothèses sur p
Si $G(Y) \in Q[Y]$ est quadratfrei alors l'ensemble :
{s entier tel que Résultant $(p(X), G(Y-sX), X)$ ait des racines multiples}
est fini.

Démonstration

Soit $\alpha_1, \alpha_2, \ldots, \alpha_n$; $\beta_1, \ldots, \beta_m$ les racines respectives de p et G($d°p = n$, $d°G = m$).
G quadratfrei entraîne que les racines de G sont toutes distinctes.
Les racines de $G(Y-sX)$ sont $(\beta_i + sX)_{i=1,m}$ puisque $G \in Q[Y]$.
D'où Résultant $(p(X), G(Y-sX), X) = a_o^m \prod_{i=1}^{n} G(Y-s\alpha_i)$ (cf. § IV).
(a_o est le coefficient directeur de p).
De ceci on déduit que les racines de R(Y) sont :

$$\beta_j + s\alpha_i \quad \text{pour } i = 1,n \text{ et } j = 1,m.$$

Par conséquent pour que R(Y) ne soit pas quadratfrei il faut qu'il existe des indices i,j,k,ℓ tels que $\beta_j + s\alpha_i = \beta_k + \alpha_\ell$ ou encore il existe i,j,k,ℓ tels que $s = \frac{\beta_j - \beta_k}{\alpha_\ell - \alpha_i}$.
Or ceci défini un nombre fini de valeur pour l'entier s, d'où le lemme.

Lemme 2

p étant toujours supposé irréductible dans Q[X].
Soit $F_X(Y) \in Q[X]/(P)[Y]$, $F_X(Y)$ quadratfrei.
Alors il existe un polynôme $g(Y) \in Q[Y]$ quadratfrei tel que
$F_X(Y)$ divise $g(Y)$, dans $Q[X]/_{(p)}$.

Démonstration

Soit R(Y) = Résultant $(p(X), F_X(Y), X)$.
Considérons la décomposition quadratfrei de R(Y) :

$$R(Y) = \prod_{i=1}^{k} g_i^{n_i}(Y) \quad (g_i(Y) \text{ quadratfrei et pgcd}(g_i(Y), g_j(Y)) = \text{constante si } i \neq j).$$

Posons $g(Y) = \prod_{i=1}^{k} g_i(Y)$.

Nous avons g(Y) est quadratfrei et $F_X(Y)$ divise g(Y). En effet $F_X(Y)$ divise R(Y), $F_X(Y)$ est quadratfrei et on n'a enlevé de R(Y) que les facteurs multiples.

□

Démonstration du théorème 4.2

$F_X(Y)$ quadratfrei entraîne d'après le lemme 2 qu'il existe un polynôme $g(Y) \in Q[Y]$ quadratfrei et tel que $F_X(Y) \mid g(Y)$.
g(Y) quadratfrei entraîne d'après le lemme 1 que l'ensemble

$$\{s \text{ entier} \mid \text{résultant } (p(X), g(Y-sX), X) \text{ n'est pas quadratfrei}\} \text{ est fini.}$$

Or $F_X(Y) \mid g(Y)$ entraîne que $F_X(Y-sX) \mid g(Y-sX)$ et alors

$$\underbrace{\text{Résultant } (p(X), F_X(Y-sX), X)}_{R_1} \mid \underbrace{\text{Résultant } (p(X), g(Y-sX), X)}_{R_2}$$

notons

Une racine multiple de R_1 serait forcément une racine multiple de R_2. D'où :

$$\{s \text{ entier} \mid \text{Résultant } (p(X), F_X(Y-sX), X) \text{ n'est pas quadratfrei}\}$$

est fini car inclus dans un ensemble fini.

Le théorème est donc démontré.

Exemples

. $p(X) = X^2+2$ irréductible dans Q[X].
$F_X(Y) = Y^2+3$ $\quad F_X(Y) \in Q[X]/(p)[Y]$.

- s = 0, Résultant $(p(X), F_X(Y), X) = Y^4+6Y^2+9 = (Y^2+3)^2$ n'est pas quadratfrei.
- s = 1, Résultant $(p(X), F_X(Y-X), X) = Y^4+10Y^2+1$ quadratfrei.

Remarque : Si $F_X(Y)$ ne dépend pas de X, alors s=0 ne marche jamais, car alors
Resultant $(p(X), F_X(Y), X) = F_X(Y)^{\text{degré } (p)}$.

. $p(X) = X^3+X^2-X+1$ irréductible dans $Q[X]$.
$F_X(Y) = Y^2+Y+1$ $F_X(Y) \in Q[X]/(p)[Y]$.

- S = 1 . Résultant $(p(X), F_X(Y-X),X) = Y^6+5Y^5+10Y^4+13Y^3+16Y^2+3Y+1$.
Résultant quadratfrei.

Proposition 4.3

Soit $p(X) \in Q[X]$ irréductible dans $Q[X]$ et α une racine de p.
Soit $F_X(Y) \in Q[X]/(p)[Y]$ irréductible dans $Q[X]/(p)[Y]$ et β une racine de F_X.
Si Résultant $(p(X), F_X(Y),X)$ est quadratfrei alors

$$Q(\alpha,\beta) = Q(\beta).$$

Lemme 3

Avec les hypothèses de la proposition 4.3.
Si Résultant $(p(X), F_X(Y),X)$ est quadratfrei alors :

pgcd$(p(X), F_X(\beta))$ est linéaire (le pgcd étant calculé dans $Q(\beta)$).

Démonstration

On a :

$F_X(Y) \in Q[X]/(p)[Y]$, $F_X(\beta) = 0$ et $Q[X]/(p)$ est isomorphe à $Q(\alpha)$.

D'où $F_\alpha(\beta) = 0$, ou encore α est une racine de $F_X(\beta)$ dans $Q(\beta)[X]$.
Or α est racine de P dans $Q[X]$ donc aussi dans $Q(\beta)[X]$. Par conséquent α est racine commune à $p(\alpha) = 0$ et $F_X(\beta) = 0$ dans $Q(\beta)$ ou encore
$X-\alpha \mid$ pgcd$(p(X), F_X(\beta))$.

Supposons pgcd$(p(X), F_X(\beta))$ ne soit pas linéaire.
Il existe alors une racine $\alpha_j \neq \alpha$ telle que $F_{\alpha_j}(\beta) = 0$.
D'autre part Résultant$(p(X),F_X(Y),X) = R(Y) = a_0^m \prod_{i=1}^{n} F_{\alpha_i}(Y)$
(m = degré en X de $F_X(Y)$, a_0 : coefficient de tête de p, $a_0 \neq 0$), et alors
$R(\beta) = a_0^m \prod_{i=1}^{n} F_{\alpha_i}(\beta)$. D'où avec la supposition de pgcd$(p(X), F_X(\beta))$non linéaire, β serait une racine double de R, ce qui est contradictoire avec l'hypothèse R quadratfrei.
Par conséquent pgcd$(p(X), F_X(\beta))$ est linéaire et a pour valeur $X-\alpha$.

Démonstration de la proposition 4.3

D'après le lemme 3 $X-\alpha = pgcd(p(X), F_\chi(\beta))$.
Le pgcd étant calculé dans $Q(\beta)$ ceci implique que $\alpha \in Q(\beta)$ et alors $Q(\alpha,\beta) = Q(\beta)$.

□

Construction de l'élément primitif d'une extension de Q engendrée par 2 éléments.

Soit p,q 2 polynômes de Q[X] de degré respectifs n et m.
Nous allons construire l'élément primitif de $Q(\alpha,\beta)$ où α et β sont racines respectives de p et q.
On procède ainsi :

1°) On factorise p dans Q[X] et on choisit un facteur irréductible de p qu'on note p_α (on utilise pour cette factorisation le programme existant dans le système Macsyma).

2°) On factorise q(Y) dans $Q[X]/(p_\alpha)[Y]$ et on choisit un facteur irréductible de q qu'on note $F_\chi(Y)$. (on utilise de même pour cette factorisation le programme existant dans le système macsyma).

3°) En appliquant le théorème 4.2, on sait qu'il existe s entier tel que Résultant$(p_\alpha(X),F_\chi(Y-sX),X)$ soit quadratfrei. Dans cette étape on cherche s vérifiant ceci.
Ceci, par essais successifs (s=0,1,2, etc...) comme les entiers s sont en nombre fini, cette méthode est justifiée. De plus dans la pratique très peu d'essais suffisent.

4°) Posons $G_\chi(Y) = F_\chi(Y-SX)$, S étant déterminé à l'étape 3°).
$G_\chi(Y)$ est alors irréductible dans $Q[X]/(p_\alpha)[Y]$ et admet $\beta+SX$ comme racine. D'où $G_\alpha(Y)$ est le polynôme minimal de $\beta+S\alpha$ dans $Q(\alpha)[Y]$.
D'autre part $R(Y)$=Résultant$(p_\alpha(X),G_\chi(Y),X)$ est quadratfrei, on peut alors appliquer la proposition 4.3. On obtient $Q(\alpha,\beta+S\alpha) = Q(\beta+S\alpha)$.
De plus $G_\alpha(Y) \mid R(Y)$ (puisque $R(Y) = C \prod_{\alpha_i \text{ racine de } P} G_{\alpha_i}(Y)$ où C est une constante appartenant à Q). Donc $\beta+S\alpha$ est une racine de R(Y) (puisque c'est une racine de $G_\alpha(Y)$).

Or $G_X(Y)$ irréductible et $R(Y)$ quadratfrei entraîne que $R(Y)$ est irréductible dans $Q[Y]$.
Par conséquent, $\beta+S\alpha$ a pour polynôme minimal $R(Y)$ dans $Q[Y]$, d'où $Q(\beta+S\alpha) = Q[Y]/_{(R)}$ à un isomorphisme près.
Or $Q(\alpha,\beta) = Q(\alpha,\beta+S\alpha)$, et $Q(\alpha,\beta+S\alpha) = Q(\beta+S\alpha)$.
Donc $Q(\alpha,\beta) = Q(\beta+S\alpha)$ et $\beta+S\alpha$ est l'élément primitif cherché, de plus $R(Y)$ = Résultant $(p_\alpha(X),G_X(Y),X)$ est le polynôme minimal de $\beta+S\alpha$.

D'autre part en posant $Q(\beta+S\alpha) = Q[Y]/_{(R)}$ on a les expressions de α et de β dans $Q[Y]/_{(R)}$. En effet :

- $\text{pgcd}(p_\alpha(Z), G_Z(\beta+S\alpha)) = Z-\alpha$ (cf. démonstration du lemme 3).
Donc le calcul du pgcd de $p_\alpha(Z)$ et de $G_Z(Y)$ dans $Q[Y]/_{(R)}[Z]$ nous donne l'expression de α dans $Q[Y]/_{(R)}$. Soit $\alpha=\Phi_1(Y)$.

- $Q(\beta+S\alpha) = Q[Y]/_{(R)}$ entraîne que $\beta+S\alpha= Y$, c'est à dire $\beta = Y-S\alpha = Y-S.\Phi_1(Y)$. Soit $\beta = \Phi_2(Y)$.

Ainsi nous avons obtenu les expressions d'une racine de p et d'une racine de q (p et q les polynômes de départ) dans $Q[Y]/_{(R)}$.
D'où $Q[Y]/_{(R)}$ est une extension de Q contenant une racine $\Phi_1(Y)$ de p et une racine $\Phi_2(Y)$de q.

Construction de l'élément primitif d'une extension de Q engendrée par n éléments ($n \geq 2$).

Soit $p_1,p_2,\ldots,p_n$ des polynômes de $Q[X]$.
Nous utilisons récursivement la construction explicitée ci-dessus dans le cas de deux éléments pour déterminer un polynôme irréductible $r \in Q[X]$ tel que $Q(\gamma)$ soit isomorphe à $Q(\alpha_1,\ldots,\alpha_n)$ (où α_i est une racine de p_i que l'on choisi au cours de l'algorithme, et γ une racine de r). Nous obtenons aussi l'expression de $\alpha_1,\ldots,\alpha_n$ en fonction de γ.

Algorithme 1:reso(p,q).

Données : p,q deux polynômes à coefficients dans Q .

résultats : *r ; polynôme irréductible à coefficients dans Q et tel que $Q[Y]/_{(r)}$ contienne une racine rp de p et une racine rq de q.
* expressions de rp et de rq dans $Q[Y]/_{(r)}$.

1- décomposer p en facteurs irréductibles dans Q.
1' p := premier facteur de p.

2- décomposer q(Y) en facteurs irréductibles dans $Q[X]/_{(p)}[Y]$.
2' q := premier facteur de q.

3- s:= 0, g:=q, r:=résultant (p,g,x),

4- tant que r n'est pas quadratfrei faire
4.1 s:=s+1, substituer y par (y-x) dans g,
4.2 r:=résultant (p,g,x)

5- rp:=racine de pgcd(p,g) = (pgcd calculé dans $Q[Y]/_{(r)}$),

6- rq:=Y-s.rp,

7- retourner (r,rp,rq).fin.

Programme et exemple

Le programme est écrit en Macsyma

```
(c19) batch("resolvent.mac");

(c20) factoris(p,r,x,y):=block([a],
                /* ce block permet de factoriser p dans q[y]/(r) meme si p n'es
t pas unitaire */
                  a:coeff(r,y,hipow(r,y)),
                p:subst(y/a,y,p),
                  r:subst(y/a,y,r),
                 r:r*a**(hipow(r,y)-1),
               /*factorisation*/
                        subst(y*a,y,factor(p,r)))$
Time= 6 msec.

(c21) resultlc(p,q,x):=block(
             /*donnees :x,y :indeterminees
                      p:polynome en x
                    q:polynome en y et x
              resultats : s:coeff de la subst
                           g:image de q par la subst
                          r:resultant (p,g,x)*/
              /*initialisation*/
              modresult : true,
               s:0,g:q , r:resultant(p,g,x),
               while not (hipow(gcd(r,diff(r,y)),y)=0) do
                 (s:s+1,
                  g:subst(y-x,y,g),
                          r:resultant(p,g,x)))$
Time= 6 msec.

(c22) pgcd(p,g,r,x,y):=block([d,d1],
                     /*ce block calcule le pgcd de p et de g dans
                       q[y]/(r)*/
                     algebraic:true,
                     tellrat(r),
                     d:g,d1:p,d2:p,
                     thru 10 while not (d=0) do
                     (d1:d2,d2:d,d:remainder(d1,d2,x)),
                     pgcd:d2)$
Time= 5 msec.

(c23) resolvent(p,q):=block(

                     /*donnees :  p:polynome en x
                                  q:polynome en y et x
                       resultats :  r:polynome en y
                                    rp:racine de p dans q[y]/(r)
                                    rq:racine de q dans q[y]/(r)
                      */
   p:2*factor(p)*z, p:first(rest(p,1))*p, p:first(first(rest(p,1))),
   q:2*factoris(q,p,y,x)*z, q:first(rest(q,1))*q,  q:first(first(rest(q,1))),
   if hipow(q,y) =1 then (r:p,rp:subst(y,x,x),rq:subst(y,x,rhs(first(linsolve(q,y))
   )))
                    else( resultlc(p,q,x),
                       rp:rhs(first(linsolve(pgcd(p,g,r,x,y),x))),
                       algebraic:false, rq:y-s*rp),
   print("r =",r,"rp =",rp, "rq =",rq))$
```

Exemple 1 : $p = X^2+2$; $q = Y^2+3$.

```
(c25) resolvent(x**2+2,y**2+3);
```

$$r = y^4 + 10\,y^2 + 1 ; rp = -\frac{y^3 + 9\,y}{2} ; rq = \frac{y^3 + 9\,y}{2} + y$$

```
Time= 1087 msec.
```

Donc $Q[Y]/_{(Y^4+1sY^2+1)}$ contient la racine $r_p = -\frac{Y^3+9Y}{2}$ de p et la racine $rq = \frac{Y^3+9Y}{2} + Y$.

Exemple 2 : $p = X^3+X^2-X+1$; $q = Y^2+Y+1$

```
resolvent(x**3+x**2-x+1,y**2+y+1);
(c26)
(c26)
```

$$r = y^6 + 5\,y^5 + 10\,y^4 + 13\,y^3 + 16\,y^2 + 3\,y + 1$$

$$rp = -\frac{26\,y^5 + 121\,y^4 + 230\,y^3 + 298\,y^2 + 297\,y - 5}{103}$$

$$rq = \frac{26\,y^5 + 121\,y^4 + 230\,y^3 + 298\,y^2 + 297\,y - 5}{103} + y$$

```
Time= 1825 msec.
```

Le polynôme p est irréductible dans Q[X]; le polynôme q est irréductible dans $Q[X]/_{(p)}[Y]$, on obtient un polynôme r de degré 6 égal au produit des degrés de p et q.

Exemple 3 : $p = X^4+2$; $q = Y^2+3$.

```
resolvent(x**4+2 ,y**2+3);
```

$$r = y^8 + 12\,y^6 + 58\,y^4 + 36\,y^2 + 121 ; rp = -\frac{15\,y^7 + 191\,y^5 + 1035\,y^3 + 551\,y}{1496}$$

$$rq = \frac{15\,y^7 + 191\,y^5 + 1035\,y^3 + 551\,y}{1496} + y$$

```
Time= 1595 msec.
```

On peut déjà remarquer la croissance des coefficients de r_p et de r_q par rapport à ceux de p et q.

Exemple 4 : $p = X^5-X^4+X^3+5X^2-5X+5$; $q = Y^2+Y.X-3$.

```
resolvent(x**5+5*x**2-x**4-5*x+x**3+5,y**2+y*x-3);
                                          3    2
     4    3      2                      y  + y  - 2 y - 3
r = y  + y  - 5 y  - 3 y + 9 rp = - ----------------- rq = y
                                            3
Time= 2995 msec.
```

p n'est pas irréductible dans Q X , on obtient une extension de degré 4 inférieure au produit des degrés de p et q.

Exemple 5 : $p = X^5-X^4+X^3+5X^2$; $q = 2.Y^5-6.Y^3+Y^2-3$.

```
resolvent(x**5-x**4+x**3+5*x**2-5*x+5,2*y**5+y**2-6*y**3-3);
                                          3      2                 3      2
     4      3      2                   2 y  - 3 y  + 8          2 y  - 3 y  + 8
r = y  - 2 y  - 3 y  + 4 y + 13 rp = --------------- rq = y - ---------------
                                            15                       15
Time= 2192 msec.
```

V - APPLICATIONS : CORPS DE DECOMPOSITION D'UN POLYNÔME DE Q[X].

C'est une application du paragraphe IV.

Soit $P \in Q[X]$, on supposera d'abord P irréductible. Le principe est de construire un polynôme $R[Y] \in Q[Y]$ irréductible, tel que si γ est une racine de R, on puisse exprimer toutes les racines de P en fonction de γ, et γ en fonction des racines de P. Le corps de décomposition de P est alors $Q(\gamma)$, où $Q[Y]/(R)$ à un isomorphisme près.

Méthode

Le corps de décomposition de P est le corps $Q(\alpha_1,\ldots,\alpha_n)$ où les α_i sont les racines de P.

Notre méthode consiste à utiliser l'algorithme 1 de façon itérée. On a vu que $Q[X]/_{(P)}$ est une extension de Q contenant au moins une racine α_1 de P. On peut écrire dans $Q(\alpha_1)[Y]$: $P(Y) = (Y-\alpha_1)F_{\alpha_1}(Y)$, ce qui se transforme dans $Q[X]/_{(P)}[Y]$ en :

$$P(Y) = (Y-X)F_X(Y).$$

Soit α_2 une deuxième racine de P, α_2 est alors racine de $F_X(Y)$ dans $Q[X]/_{(P)}[Y]$.

On applique l'algorithme 1 à P(X) et à $F_X(Y)$ on obtient une extension $Q[X]/_{(r_1)}$ contenant une racine $\hat{\alpha}_1(X)$ de P et une racine $\hat{\alpha}_2(X)$ de $F_X(Y)$, c'est-à-dire deux racines $\hat{\alpha}_1(X)$ et $\hat{\alpha}_2(X)$ de P.

Dans $Q[X]/_{(r_1)}[Y]$ P s'écrit alors :

$$P(Y) = (X-\hat{\alpha}_1(X))(Y-\hat{\alpha}_2(X))\ F_{1X}(Y).$$

$\hat{\alpha}_1(X)$, $\hat{\alpha}_2(X)$ sont les expressions de deux racines de P dans $Q[X]/_{(r_1)}$, $F_{1_X}(Y) \in Q[X]/_{(r_1)}[Y]$.

On répètera le même processus cette fois pour $r_1(X)$ et $F_{1_X}(Y)$.

On factorisera $F_{1_X}(Y)$ dans $Q[X]/_{(r_1)}[Y]$. S'il y a des termes linéaires ceci prouve que l'extension $Q[X]/_{(r_1)}$ contient d'autres racines de P que $\alpha_1'(X)$ et $\alpha_2'(X)$. S'il en est ainsi on ajoute les racines des termes linéaires trouvés à l'ensemble des racines et on considère un facteur irréductible de $F_{1_X}(Y)$ dans

$Q[X]/_{(r_1)}[Y]$ qui ne soit pas linéaire. Soit $F'_{1_X}(Y)$ ce facteur.

On applique l'algorithme 1 à $r_1(X)$ et $F'_{1_X}(Y)$ on obtient une extension $Q[X]/_{(r_2)}$ de Q dans laquelle P s'écrit au moins sous la forme :
$P(Y) = (Y-\alpha_1^2(X))\ (Y-\alpha_2^2(X))\ (Y-\alpha_3^2(X))\ F_{2_X}(Y)$, c'est à dire que $Q[X]/_{(r_2)}$ contient au moins 3 racines de P.

On voit qu'en répétant ce processus on arrivera à une extension $Q[X]/_{(r_j)}$ de Q dans laquelle P se décompose en facteurs linéaires seulement :

$$P(Y) = (Y-\alpha_1^j(X))\ (Y-\alpha_2^j(X))\ \ldots\ (Y-\alpha_n^j(X))$$

j étant le nombre de pas qu'on a effectué : $j < n$.

Exemples

Nous allons commencer par un exemple simple pour illustrer le déroulement de l'algorithme :

Soit $P(X) = X^3-2$, P est irréductible dans Q[X].

$Q[X]/_{(P)}$ est une première extension de Q dans laquelle P(Y) s'écrit $P(Y) = (Y-X)\ F_X(Y)$.

$F_X(Y) = \frac{Y^3-2}{Y-X} = Y^2+XY+X^2$. (division euclidienne sachant que $X^3-2=0$).

On applique l'algorithme 1 à P(X) et $F_X(Y)$, on obtient :

$r_1(X) = X^6+108$, $\alpha_1(X) = -\frac{X^4-18X}{36}$, $\alpha_2(X) = \frac{X^4}{18}$

donc $Q[X]/_{(r_1)}$ est une extension de Q dans laquelle P(Y) s'écrit :

$P(Y) = Y+\frac{X^4-18X}{36})\ (Y-\frac{X^4}{18})\ F_{2_X}(Y)$

$F_{2_X}(Y) = \frac{F_X(Y)}{Y-\frac{X^4}{18}} = Y+\frac{X^4+18X}{36}$

d'où $P(Y) = (Y+\frac{X^4-18X}{36})\ (Y-\frac{X^4}{18})\ (Y+\frac{X^4+18X}{36})$ dans $Q[X]/_{(r_1)}[Y]$.

On conclue que $Q[X]/_{(X^6+108)}$ est le corps de décomposition de $P(Y) = Y^3-2$ et que $\alpha_1 = -\frac{X^4-18X}{36}$, $\alpha_2 = \frac{X^4}{18}$, $\alpha_3 = -\frac{X^4+18X}{36}$ sont les racines de $P(Y)$.

Ceci veut dire aussi que si γ est une racine de X^6+108 alors $\alpha_1(\alpha)$, $\alpha_2(\gamma)$, $\alpha_3(\gamma)$ sont les racines réelles ou complexes de Y^3-2. En effet $r(X) = X^6+108$ donc $\gamma = i\ \sqrt[3]{2}.\sqrt{3}$ est une racine de r.

$$\alpha_1(\gamma) = \frac{1}{2}\, i^3\sqrt{2}\sqrt{3} - \frac{1}{4.3^2}\,(i\ \sqrt[3]{2}\sqrt{3})^4 = \sqrt[3]{2}(i\,\frac{\sqrt{3}}{2} - \frac{1}{2}) = j\ \sqrt[3]{2}\ ;$$

$$\underline{\alpha_1 = j\ \sqrt[3]{2}}$$

$$\alpha_2(\gamma) = \frac{1}{4.3^2}\,(i\ \sqrt[3]{2}\sqrt{3})^4 = \sqrt[3]{2}\ ; \qquad \underline{\alpha_2 = \sqrt[3]{2}}$$

$$\alpha_3(\gamma) = -\frac{1}{2}\, i^3\sqrt{2}\sqrt{3} - \frac{1}{4.3^2}\,(i^3\sqrt{2}\sqrt{3})^4 = j^2\sqrt[3]{2}\ ; \quad \underline{\alpha_3 = j^2\ \sqrt[3]{2}}$$

On retrouve bien les trois racines de P à partir d'une racine de r.

Algorithme 2 : Cordecomp(p)

Entrée : p : un polynôme appartenant à Q[X].

Sortie : r : un polynôme de Q[Y] tel que P(Y) se décompose en facteurs linéaires dans $Q[X]/_{(r)}[Y]$.
rac : la liste des racines de p dans $Q[X]/_{(r)}$.

1- {Initialisation}
rac:=[X], r:= substituer X par Y dans P, rp:=X, rq:=X, q:=r,

2- pour i:=0 jusqu'à d°P-2 faire
21.q:= substituer X par rq dans q, s:= substituer Y par X dans r,

22.q:= quotient de la division de q par Y-rp (division dans $Q[X]/_{(s)}[Y]$).

23.reso(s,q)

24.mise à jour de rac (substituer X par rp dans rac et ajouter rq).

3- retourner (r,rac).

4- fin.

PROGRAMMES ET EXEMPLES

Le programme est écrit en Macsyma.

```
(c1) batch("cordecomp.mac");

(c2) factoris(p,r,x,y):=block([a],
                a:coeff(r,y,hipow(r,y)),
                p:subst(y/a,y,p),
            r:subst(y/a,y,r),
               r:r*a**(hipow(r,y)-1),
               subst(y*a,y,factor(p,r)))$
Time= 35 msec.

(c3) resultlc(p,q,x):=block(
              modresult:true,
             s:0,g:q,r:resultant(p,g,x),
            while not (hipow(gcd(r,diff(r,y)),y)=0) do
              (s:s+1, g:subst(y-x,y,g), r:resultant(p,g,x)))$
Time= 5 msec.

(c4) pgcd(p,g,r,x,y):=block([d1,d2,d],
           algebraic:true,  tellrat(r),
           d:g, d1:p ,d2:p,
           thru 10 while not (d=0) do
             (d1:d2,d2:d,d:remainder(d1,d2,x)),
          pgcd:d2,  print("pgcd =  ",d2))$
Time= 5 msec.

(c5) reso(p,q):=block(
         q:num(q),  q1:2*part(2*q,2)*q,  q1:part(q1,2,1),
        if hipow(q1,y)=1 then (rp:x, rq:rhs(first(linsolve(q1,y))))
                         else(
                             resultlc(p,q1,x),
                          rp:rhs(first(linsolve(pgcd(p,g,r,x,y),x)))
                          , algebraic:false,
                       rq:y-s*rp, rp:ratsimp(subst(x,y,rp)),
                      rq:ratsimp(subst(x,y,rq))),
                     print("r =",r,"rp = ",rp ,"rq = ",rq))$
Time= 5 msec.

(c6) cordecomp(p):=block([s,r,q,rp,rq,y,z],
                  rac:[x], r:subst(y,x,p),  rp:x, rq:x,  q:r,
for i:0 thru (hipow(p,x)-2) do (
       q:subst(rp,x,q)  , s:subst(x,y,r),
           q:quotient(q,y-rq,y),print("q =",q),
          q:factoris(q,s,y,x), print("q =",q),
          reso(s,q),
           rac:map(lambda([u],subst(rp,x,u)),rac),
           rac:endcons(rq,rac)),
            a:1,  for f in rac  do a:a*(y-f),
             print("p(y)=  ",a,"      ecriture de p(y) dans q[x]/(",s,")"))$
Time= 5 msec.
```

Exemple 1: $P = X^3+3X^2-5$;

Corpdecomp (X**3+3*X**2-5) ;

$$P(Y) = (Y+\frac{X^4+12X^3+39X^2-9X-45}{54})\ (Y-\frac{X^4+12X^3+39X^2+18X-45}{27})$$

$$(Y+\frac{X^4+12X^3+39X^2+45X+117}{54})$$

écriture de p(Y) dans $q[X]/(X^6+18X^5+117X^4+324X^3+324X^2+135)$.

Exemple 2 : $P = X^4+2X^3+5$;

(c8) cordecomp (x**4+2*x**3+5) ;

Après un temps d'exécution assez long (300 sec.) nous avons obtenu une extension intermédiaire $Q[X]/_{(r)}$ de degré 12, avec l'expression de deux racines de p : r_p et r_q ainsi que le polynôme $q(Y) = \frac{P(Y)}{(Y-r_p)(Y-r_q)}$.

```
CTRL/]
CTRL/]
CTRL/]
392835 msec.
```

$$r = y^{12} + 18\,y^{11} + 132\,y^{10} + 504\,y^{9} + 991\,y^{8} + 372\,y^{7} - 3028\,y^{6} - 6720\,y^{5} + 11435\,y^{4} + 91650\,y^{3} + 185400\,y^{2} + 194400\,y + 164525$$

$$r_p = (81301269\,x^{11} + 1074321858\,x^{10} + 5698843986\,x^{9} + 18339383773\,x^{8} + 43146653538\,x^{7} + 49497745854\,x^{6} - 40645117620\,x^{5} - 112513860438\,x^{4} + 868600999605\,x^{3} + 1564133987000\,x^{2} + 16896437578970\,x + 18975726988525)/18349835759240$$

$$r_q = -(81301269\,x^{11} + 1074321858\,x^{10} + 5698843986\,x^{9} + 18339383773\,x^{8} + 43146653538\,x^{7} + 49497745854\,x^{6} - 40645117620\,x^{5} - 112513860438\,x^{4} + 868600999605\,x^{3} + 1564133987000\,x^{2} + 7721519699350\,x + 18975726988525)/9174917879620$$

$$q = (33671647239108302724537760 0\, y^2 + (- 14918649331677904755 60\, x^{11}$$

$$- 19713629646861557467920\, x^{10} - 10457285116063261793064 0\, x^9$$

$$- 33652468016022119081252 0\, x^8 - 79173400598313146219112 0\, x^7$$

$$- 90827550687350265219096 0\, x^6 + 74583123274199180180880 0\, x^5$$

$$+ 20646108596753511289471 20\, x^4 - 15938685683063438115100200\, x^3$$

$$- 28701601766895233289880000\, x^2 + 26669617900732789838194800\, x$$

$$+ 32523147113055445234803420 0)\, y + 19829689023031083\, x^{22}$$

$$+ 524062382219026812\, x^{21} + 6242441851098625896\, x^{20} + 45680446997487323550\, x^{19}$$

La taille des coefficients des résultats est déjà remarquable.
Nous avons essayé de faire sortir seulement l'expression du corps de décomposition de p, nous avons obtenu :

```
(c11) resultant(r,q,x);
Time= 96508 msec.
(d11) 5969612282264147949017478499781776672645719395697926331928954355344486389#

821574344537886918958444459877493561629112488477034858943155535176139062378496 0#

00000000000 y^24 + 5182200684433912933782551202385909361524876295569569163715628#

845818499246714975710414560647355821846854576927667910508772187212319536828111 4#

267931901952000000000000 y^23 - 2007803431489087399075460988180683062563843384 58#

402745671389383388465430177428792828881592532750688030552429531081180060609433#

126224353941137486242853683200000000000 y^22 - 27866591815308182067119915084019 7#

730079833387033357215560813150000473033665394169896282508234270048996934828647 0#

679847983395103815784113010227368097821491200000000000 y^21 + 86926954619491913#

678822569360105135186710407046123928184487223417335860978357707287552920613820 1#

592202240041217164185022610666250015678145175154280787188121600000000000 y^20 + 4#

865520839371680685419825974792740240366134062839517750673018566412768636771122 8#
```

$$0000000000\,y^{19} + 67897200465305554097568145864274292149492927776629910986926643\#$$

$$27567444665213318059557508342999465101566941800825739922823518430034741498641 77\#$$

$$43075098929638932480000000000\,y^{18} + 51431007272228533755697287775525917738174 08\#$$

$$91475272880736588897152878225751754347971053234393153053607769630488306796605 68\#$$

$$75866386151350358073086642723522556723200000000000\,y^{17} + 15389138212777211690239\#$$

$$12305293728771061082270183068052038862867411381789855685137143832209156907312 19\#$$

$$48483360754507621210389257112200548348698069579486443832606720000000000\,y^{16} - 77\#$$

$$94128716123229611742928677795785841964680097293481542485932641591921895746211 64\#$$

$$37483245395600481471668442379370401251113379958093356725953080279781585656731 40\#$$

$$224000000000\,y^{15} - 10282007153859834528370553908785428592300764925258746119 0740\#$$

$$41760722952222964603331372027648944253822359094446122153500788203737582997927 67\#$$

$$18375976969220233277808312320000000\,y^{14} - 38332993130381520936898229767738189 69\#$$

$$30691336000086154588164516918704596117202613747113294397695145135243998160245 89\#$$

$$74229923445457542292240700630928645935692389967462400000000\,y^{13} + 690627645478 89\#$$

$$78741875784199168711471684541562502483249467345614512406070605713512118623290 54\#$$

$$86357938245915037376779247753812669963856393612608410814840539687151363686400 00\#$$

$$00\,y^{12} + 10916697521205660543139166404777899563857401730638314746411531634888 63\#$$

$$29023263735812831674497974641892489980075133180738144520033055662212919389785 78\#$$

$$938449554253287522304000000\,y^{11} + 22769144252967609153423739934592350061057284 4\#$$

$$35079463416216128743042103316631849778475882768233224736231760284318665864564 63\#$$

$$71107478776226105733315525372463181426657067008000000\,y^{10} - 85952946247423701 657\#$$

$$99656479917890130108644588507985521567852397951410965694692768115076355746671 73\#$$

$$67485959744965907164521491831676047646695658756737830683940281340788736000000\,y^{9}$$

Expression is too wide to be displayed.

VI - INTERPRETATION ET CONCLUSION

Interprétation des exemples

Pour un polynôme P de degré 3 l'exécution du programme se déroule bien, on obtient l'expression du corps de décomposition et la décomposition de p sur ce corps.

Cependant lorqu'on passe à un polynôme p de degré 4, les calculs se compliquent, le temps d'exécution s'accroît très rapidement.

Pour $p = X^4+2X^3+5$, on obtient une première extension $Q[X]/_{(r)}$, dans laquelle p s'écrit $p(Y) = (Y-rp) \times (Y-rq) \times q$ où r_p et r_q sont des polynômes de degré 11 en X à coefficients comportant 11 chiffres, q un polynôme de degré 2 en Y et 11 en X à coefficients comportant 27 chiffres.

Nous avons interrompu l'exécution qui devenait longue, et nous avons essayé d'avoir l'expression du corps de décomposition seulement. On a obtenu alors un polynôme à coefficients énormes (de l'ordre de 198 chiffres pour le coefficient de X^{24} et 207 pour celui de X^9). On n'a pas pu avoir la suite vu que l'espace de travail était déjà épuisé.

CONCLUSION

D'après les exemples il est assez clair que le corps de décomposition, même si on réussit à l'obtenir, ne peut servir pour simplifier des expressions.

Pour l'exemple $p = X^4+2X^3+5$, si on note $\alpha_1,\alpha_2,\alpha_3$ et α_4 les racines de p dans le corps de décomposition $Q[X]/_{(r)}$, une expression toute simple $E(\alpha_1,\ldots,\alpha_4)$ sera transformée en $E'(X)$: polynôme de degré 23 à coefficients énormes, on ne pourra donc dire que E'(X) est l'écriture simplifiée de $E(\alpha_1,\ldots,\alpha_4)$.

Avant de juger définitivement cette méthode, nous allons voir si on ne peut pas améliorer l'écriture d'une extension.

Remarque :

$Q[X]/_{(9X^2+120X+398)}$ est la même que $Q[Y]/_{(Y^2-2)} \simeq Q(\sqrt{2})$, en posant $Y = 3X+20$.

Nous avons donc d'une part $Q(\sqrt{2}) \simeq Q[X]/_{(9X^2+120X+398)}$ et $Q(\sqrt{2}) \simeq Q[X]/_{(X^2-2)}$.

Cette remarque nous laisse l'espoir de dire que le polynôme r qu'on a trouvé dans l'exemple $p = X^4+2X^3+5$ n'est peut être pas le plus simple.

Nous avons essayé d'exploiter cette remarque en cherchant une substitution $Y = S(X)$ où S est un polynôme de Q[X] de degré 23.
Nous avons aussi essayé d'utiliser la méthode de Tschirnaüs (1683) pour faire disparaitre des termes d'une équation [Ser].
Le problème c'est que l'on obtient un polynôme assez creux mais à coefficients plus grands que ceux du polynôme de départ, ce qui n'est pas exactement ce qu'on espérait.

CHAPITRE 2 - DEUXIEME APPROCHE

FACTORISATION DANS DES EXTENSIONS ALGEBRIQUES DE Q

INTRODUCTION

Etant donné une extension algébrique de degré fini de Q de la forme $Q(\alpha_1,\ldots,\alpha_n)$, nous allons essayer dans ce chapitre de définir les règles, vérifiées par les α_i, nécessaires pour la simplification des expressions dans $Q(\alpha_1,\ldots,\alpha_n)$. Ceci sans passer par l'algorithme de l'élément primitif.

Cette approche est basée sur une méthode de factorisation dans les extensions algébriques de Q, donnée par Trager [Tra].

I - FACTORISATION DANS UNE EXTENSION ALGÉBRIQUE DE Q.

Dans ce paragraphe nous allons énoncer un algorithme de factorisation dans une extension $K[X]/_{(P)}$ de K où P est un polynôme irréductible à coefficients dans K et K une extension algébrique de Q sur laquelle existe déjà un algorithme de factorisation des polynômes à une indéterminée.

Le principe de cette méthode est le suivant : si $F_X \in K[X]/_{(P)}[Y]$, alors sa norme [LAN] (relative à l'extension $(K[X]/_{(P)})/K$) est dans K[Y] et peut donc être factorisée.

Le théorème 1.1 prouve que cela suffit "souvent" à déterminer la factorisation de F_X dans $K[X]/_{(P)}[Y]$, et la remarque 1.3 indique comment se tirer d'affaire dans tous les cas.

Dans tout ce qui suit on ne parle pas de normes mais de résultants, car la norme de F_X relative à l'extension $(K[X]/_{(P)})/K$ est égale au résultant de p(X) et $F_X(Y)$ par rapport à la variable X.

Théorème 1.1

Si P est irréductible dans $K[X]$ et $F_\chi \in K[X]/_{(P)}[Y]$.
Si $R(Y)$ = Résultant $(P(X), F_\chi(Y), X)$ est quadratfrei.
Alors : Si $R(Y) = \pi R_i(Y)$ est une décomposition en facteurs irréductibles de R ($R \in K[Y]$), on a $F_\chi(Y) = \pi_i$ pgcd $(F_\chi(Y), R_i(Y))$. Et les pgcd sont irréductibles sur $K[X]/_{(p)}$. [Tra]

Lemme 1.2

Si F_χ est irréductible dans $K[X]/_{(P)}[Y]$ alors :
Résultant $(P(X), F_\chi(Y), X)$ est une puissance d'un facteur irréductible dans $K[Y]$. [Tra]

Démonstration

Posons R = Résultant $(p(X), F_\chi(Y), X)$.
Supposons que $R = R_1.R_2$ avec pgcd(R_1, R_2) = constante dans K.(ie. supposons que le lemme soit faut). Nous avons $R(Y) = a_0^m \pi_i F_{\alpha_i}(Y)$ (cf. proposition 3.2 chapitre 1).

F_χ étant irréductible dans $K[X]/_{(P)}[Y]$, $F_{\alpha_i}(Y)$ est irréductible dans $K(\alpha_i)[Y]$.
D'où $F_{\alpha_1}(Y) | R_1(Y)$ ou $F_{\alpha_1}(Y) | R_2(Y)$.
Supposons $F_{\alpha_1} | R_1$ alors $\exists\, g \in K(\alpha_1)[Y]$ tel que $R_1 = F_{\alpha_1} \times g$. Montrons qu'alors $F_{\alpha_i} | R_1$ pour tout i.
$K(\alpha_1)$ et $K(\alpha_i)$ étant canoniquement isomorphes :
Notons ϕ_i cet isomorphisme entre $K(\alpha_1)$ et $K(\alpha_i)$.
En appliquant ϕ_i à l'égalité $R_1 = F_{\alpha_1} \times g$.
On obtient $\phi_i(R_1) = \phi_i(F_{\alpha_1}) \times \phi_i(g)$ ou encore $R_1 = F_{\alpha_i} \times \phi_j(g)$

D'où $F_{\alpha_i} | R_1$ et ceci pour tout i par conséquent $\pi F_{\alpha_i} | R_1$
Or $R = a_0^m \pi F_{\alpha_i}$ donc $R | R_1$ ou encore $R_2 | R_1$ ($R = R_1.R_2$) donc R_2 = constante dans K.
Nous avons montré que R ne peut être produit de deux polynômes non constants et premiers entre eux, c'est donc une puissance d'un polynôme irréductible.

□

Démontrons le théorème 1.1.

Considérons R = Résultant $(P(X), F_X(Y), X)$ et sa factorisation en polynômes irréductibles dans K[Y] : $R(Y) = \prod R_i(Y)$.

Soit $F_X(Y) = \prod F_X^i(Y)$ la décomposition en facteurs irréductibles de $F_X(Y)$, dans $K[X]/_{(P)}[Y]$.

Il faut montrer que $F_X^i(Y) = \text{pgcd}\,(F_X(Y).R_1(Y))$.
D'après le lemme ci-dessus :

$F_X^i(Y)$ irréductible donc Résultant $(F_X^i(Y), P(X), X) = U^k(Y)$ où U(Y) est un polynôme irréductible dans K[Y].

$F_X^i(Y) | F_X(Y)$ entraîne que Résultant $(P(X), F_X^i(Y), X) |$ Résultant$(P(X), F_X(Y), X)$ c'est-à-dire $U^k | R$.

Or R est supposé quadratfrei donc k = 1, et alors U est un facteur irréductible de R donc c'est un R_i. D'autre part, puisque $F_X(Y) = \pi F_X^i(Y)$ alors $R(Y) = \pi$ Résultant $(P(X), F_X^i(Y))$. Donc chaque R_i est un résultant d'un facteur irréductible de $F_X(Y)$. De plus $F_X^i(Y) | F_X(Y)$ et $F_X^i(Y) | R_i(Y)$ = Résultant $(P(X), F_X^i(Y))$ entraîne que $F_X^i(Y) | \text{pgcd}\,(F_X(Y), R_i(Y))$.

Or $\text{pgcd}(F_X(Y), R_i(Y))$ est irréductible. En effet :
sinon il existe $j \neq i$ tel que $F_X^j(Y) | \text{pgcd}(F_X(Y), R_i(Y))$
et ceci entraîne que $F_X^j(Y) | R_i(Y)$ ou encore

$$\underbrace{\text{Résultant } (P(X), F_X^j(Y), X)}_{R_j(Y)} \mid \text{Résultant } (P(X), R_i(Y), X) = a_o^m R_i^n(Y)$$

et alors $R_j(Y) | R_i^n(Y)$. Seulement R_i et R_j sont deux facteurs irréductibles de R qui est quadratfrei d'où l'impossibilité car on aurait $R_i^2(Y) | R(Y)$.
Par conséquent $F_X^i(Y) | \text{pgcd}(F_X(Y), R_i'(Y))$ et $\text{pgcd}(F_X(Y), R_i(Y)$ est irréductible donc $F_X^i(Y) = \text{pgcd}(F_X(Y), R_i(Y))$, et alors

$$F_X(Y) = \prod_i \text{pgcd}(F_X(Y), R_i(Y)).$$

□

Remarque 1.3

On peut toujours se ramener à Résultant $(P(X), F_X(Y), X)$ quadratfrei par une substitution sur Y du type $Y \to Y-SX$ pour S convenablement choisi (cf. théorème 4.2, chapitre I).

Conséguence

Ce théorème nous permet de factoriser un polynôme à coefficients dans $K[X]/_{(P)}$ en utilisant la factorisation des polynômes à coefficients dans K d'une part et l'algorithme d'Euclide dans l'extension $K[X]/_{(p)}$ pour calculer les pgcd d'autre part.

II - ALGORITHME D'EUCLIDE ET INVERSE D'UN ELEMENT DANS UNE EXTENSION ALGEBRIQUE DE Q

On se propose de chercher l'inverse d'un élément q appartenant au corps $K[X]/_{(P)}$, sachant que p n'est pas nul.

Proposition 2.1

Soit q un élément non nul de $K[X]/_{(P)}$. On définit l'inverse de q par $q^{-1} = S.$ où S est donné par l'identité de Bezout entre p(X) et q(X) dans K[X] : $S.q + Rp = 1$.

Démonstration

q étant un élément non nul de $K[X]/_{(p)}$, q et p sont deux polynômes de K[X] premiers entre eux.

L'identité de Bezout appliquée à p et q dans K[X] entraîne l'existence de $S,R \in K[X]$,

$$S(X)\, q(X) + R(X).p(X) = 1,$$

En se plaçant dans $K[X]/_{(p)}$ l'égalité ci-dessus devient

$$S(X)\, q(X) = 1 \qquad (p = 0)$$

d'où $$q^{-1}(X) = S(X) \quad .$$

□

III - PRESENTATION DE LA DEUXIEME APPROCHE

Etant donné une extension algébrique de Q de la forme $Q(\alpha_1,\ldots,\alpha_n)$ où les α_i sont définis par $p_i(\alpha_i) = 0$ avec $p_i(X) \in Q(\alpha_1,\ldots,\alpha_{i-1})[X]$. Pour obtenir une base du corps $Q(\alpha_1,\ldots,\alpha_n)$ on procède de la manière suivante :

1°) Factoriser $p_1(X)$ dans $Q[X]$, choisir un facteur q_1 de p_1 et noter α_1 une racine de q_1 ;

2°) Factoriser $p_2(X)$ dans $Q(\alpha_1)[X]$, choisir un facteur q_2 de p_2 et noter α_2 une racine de q_2 ;

3°) Pour i = 3 à n, factoriser $p_i(X)$ dans $Q(\alpha_1,\ldots,\alpha_{i-1})[X]$, choisir un facteur q_i de p_i et noter α_i une racine de q_i.

Alors $Q(\alpha_1,\ldots,\alpha_n)$ est un corps et les quantités $\alpha_1^{i_1}.\alpha_2^{i_2}\ldots.\alpha_n^{i_n}$ où $0 \leq ij < \deg q_j$ pour $1 \leq j \leq n$, en forment une base sur Q.

Les factorisations des étapes 1°) et 2°) peuvent être faites en utilisant le système Macsyma. Pour celles de l'étape 3°), on utilise l'algorithme présenté ci-dessus pour se ramener à des factorisations dans $Q(\alpha_1)[X]$, où Macsyma peut être utilisé.

Nous allons maintenant détailler le cas particulier où $P_1 = P_2 = \ldots = P_n$ est un polynôme irréductible P de degré n, et où l'on veut que les α_i parcourent toutes les racines de P, afin que le corps obtenu soit le corps de décomposition de P.

IV - CORPS DE DECOMPOSITION D'UN POLYNOME

1. Détermination des règles de calcul

Etant donné un polynôme p irréductible dans Q[X], on veut étudier son corps de décomposition.
Si p est de degré n et de racines notées $\alpha_1,\ldots,\alpha_n$, son corps de décomposition est $Q(\alpha_1,\ldots,\alpha_n)$.
En notant $Q(\alpha_1,\ldots,\alpha_n) = [\ldots[\,[Q(\alpha_1)](\alpha_2)]\ldots](\alpha_n)$; nous allons chercher les règles de simplification de α_1 dans Q, de α_2 dans $Q(\alpha_1)$ et ainsi de suite jusqu'à α_n dans $Q(\alpha_1)\ldots(\alpha_{n-1})$.

En fait si $P = a_0X^n + \ldots + a_n$, α_n s'exprime linéairement en fonction de $\alpha_1,\alpha_2,\ldots$ et α_{n-1} par : $\alpha_n = -\left(\frac{a_1}{a_0} + \alpha_1+\alpha_2+\ldots+\alpha_{n-1}\right)$. Donc il suffit de s'intéresser à $\alpha_1,\alpha_2,\ldots,\alpha_{n-1}$.

. Dans Q, α_1 vérifie $P(\alpha_1) = 0$
P irréductible entraîne $Q(\alpha_1) \simeq Q[X]/_{(p)}$ et par suite les règles de simplification dans $Q(\alpha_1)$ sont celle de $Q[X]/_{(p)}$ qui sont connues.

. Dans $Q(\alpha_1)$, P s'écrit $P(X) = (X-\alpha_1)\,F_{\alpha_1}(X)$.
Donc α_2 vérifie $F_{\alpha_1}(\alpha_2) = 0$, $F_{\alpha_1}(X)$ est de degré (n-1) en X.
Si $F_{\alpha_1}(X)$ est irréductible alors $Q(\alpha_1)(\alpha_2) \simeq (Q[X]/_{(P)})[Y]/_{(F_X)}$
Si $F_{\alpha_1}(X)$ n'est pas irréductible on peut le factoriser. On prendra alors un des facteurs irréductibles de $F_X(Y)$ au lieu de $F_X(Y)$.

. Ainsi de suite dans $Q(\alpha_1,\ldots,\alpha_i)$, P s'écrit $P(X) = (X-\alpha_1)\ldots(X-\alpha_i)F_{\alpha_1..\alpha_i}(X)$.
Donc α_{i+1} vérifie $F_{\alpha_1..\alpha_i}(X) = 0$ dans $Q(\alpha_1..\alpha_i)$.
On peut factoriser $F_{\alpha_1..\alpha_i}(X)$ en utilisant le théorème 1.1 un nombre de fois convenable .
$Q(\alpha_1,\ldots,\alpha_i)(\alpha_{i+2}) \simeq (Q[X_1]/_{(P)}\,[X_2]/_{(F_{X_1})}\cdots[X_i]/_{(F_{X_1..X_{i-1}})})[X_{i+1}]/_{(f_{X_1..X_i})}$

où $f_{X_1..X_i}(X_{i+1})$ est un facteur irréductible de $F_{(X_1\ldots X_i)}(X_{i+1})$.

Exemple

$P(X) = X^4+2X^3+5$. P est irréductible dans $Q[X]$.

. Soit α_1 une première racine de P.
α_1 vérifie $\alpha_1^4+2\alpha_1^3+5 = 0 \Rightarrow Q(\alpha_1) = Q[X_1]/(X_1^4+2X_1^3+5)$.

α_2 vérifie dans $Q(\alpha_1)$ l'équation $\frac{X^4+2X^3+5}{X-\alpha_1} = X^3+(2+\alpha_1)X^2+(\alpha_1^2+2\alpha_1)X + \alpha_1^3+2\alpha_1^2 = F_{\alpha_1}(X)$.

Ou encore α_2 vérifie $\alpha_2^3+(\alpha_1+2)\alpha_2^2+(\alpha_1^2+2\alpha_1)\alpha_2+\alpha_1^3+2\alpha_1^2 = 0$.
On peut vérifier que $F_{\alpha_1}(X)$ est irréductible dans $Q(\alpha_1)$ et alors

$$Q(\alpha_1)\ (\alpha_2) \simeq Q[X_1]/(p))[X_2]/(F_{X_1}).$$

. α_3 vérifie dans $Q(\alpha_1)(\alpha_2)$ l'équation $\frac{F_{\alpha_1}(X)}{X-\alpha_2} = 0 = F_{\alpha_1\alpha_2}(X)$.

On trouve $F_{\alpha_1\alpha_2}(X) = X^2+(\alpha_1+\alpha_2+2)X+\alpha_1^2+(2+\alpha_2)(\alpha_1+\alpha_2)$.
Donc α_3 vérifie

$$\alpha_3^2+(\alpha_1+\alpha_2+2)\alpha_3+\alpha_1^2+(2+\alpha_2)(\alpha_{1+}\alpha_2) = 0$$

On peut vérifier de même que le polynôme $F_{\alpha_1\alpha_2}(X)$ est irréductible dans $Q(\alpha_1,\alpha_2)[X]$, et alors

$$Q(\alpha_1)(\alpha_2)(\alpha_3) \simeq ((Q[X_1]/(p))[X_2]/(F_{X_1}))[X_3]/(F_{X_1,X_2})$$

. α_4 vérifie dans $Q(\alpha_1,\alpha_2,\alpha_3)$ l'équation $X+2+\alpha_1+\alpha_2+\alpha_3 = 0$; $\alpha_4 \in Q(\alpha_1,\alpha_2,\alpha_3)$.
D'où en conclusion

$$Q(\alpha_1,\alpha_2,\alpha_3,\alpha_4) \simeq ((Q[X]/(p))[X_2]/(F_{X_1}))[X_3]/(F_{X_1,X_2})$$

Etant donné un polynôme P irréductible de Q[X] ayant pour racines $\alpha_1,\ldots,\alpha_n$. En appliquant la deuxième approche on aboutit à une expression de $Q(\alpha_1,\ldots,\alpha_n)$ de la forme :

$$Q(\alpha_1,\ldots,\alpha_n) = Q[X_1]/_{(P)}[X_2]/_{(F_{X_2})} \cdots [X_{n-1}]/_{(F_{X_{n-2}})}$$

2 - Simplification d'une expression

Si on a à simplifier une expression E polynomiale en les α_i on pourra procéder ainsi :

1°) on remplace α_n par $-(\frac{a_o}{a_1} + \sum_{i=1}^{n-1} \alpha_i)$.

2°) on simplifie E par rapport à α_{n-1} en tenant compte que $F_{\alpha_1\ldots\alpha_{n-2}}(\alpha_{n-1}) = 0$.

3°) On simplifie E par rapport à α_{n-2} en tenant compte que $F_{\alpha_1\ldots\alpha_{n-3}}(\alpha_{n-2}) = 0$.

4°) On continue ainsi jusqu'à la simplification par rapport à α_1.

3 - Inverse d'un élément

Soit $q(\alpha_1,\ldots,\alpha_{n-1})$ un polynôme en les α_i à inverser. On peut procéder ainsi :

1°) on s'assure que $q \neq 0$.

2°) on considère $q(\alpha_1,\ldots,\alpha_{n-2},X)$ dans $Q(\alpha_1\ldots\alpha_{n-2})[X]$.

. On applique l'algorithme d'Euclide à $q(\alpha_1\ldots\alpha_2,X)$ et $F_{\alpha_1\ldots\alpha_{n-2}}(X)$. On obtient deux polynômes $S_{\alpha_1\ldots\alpha_{n-2}}(X)$ et $R_{\alpha_1\ldots\alpha_{n-2}}(X)$ de $Q(\alpha_1\ldots\alpha_{n-2})[X]$ et une constante $t(\alpha_1\ldots\alpha_{n-2})$ dans $Q(\alpha_1\ldots\alpha_{n-2})$ tels que

$$S_{\alpha_1\cdots\alpha_{n-2}}(X).q(\alpha_1\cdots\alpha_{n-2},X)+R_{\alpha_1\cdots\alpha_{n-2}}(X)F_{\alpha_1\cdots\alpha_{n-2}}(X) = t(\alpha_1\cdots\alpha_{n-2}).$$

En remplaçant X par α_{n-1} on obtient

$$q(\alpha_1\cdots\alpha_{n-2},\alpha_{n-1})^{-1} = S_{\alpha_1\cdots\alpha_{n-2}}(\alpha_{n-1})t.(\alpha_1\cdots\alpha_{n-2})^{-1}.$$

Nous avons ramené ainsi le calcul de l'inverse de $q(\alpha_1\cdots\alpha_{n-1})$ dans $Q(\alpha_1\cdots\alpha_{n-1})$ au calcul de l'inverse de $t(\alpha_1,\ldots,\alpha_{n-2})$ dans $Q(\alpha_1,\ldots,\alpha_{n-2})$. On recommence le même procédé pour $t(\alpha_1,\ldots,\alpha_{n-2})$ avec $F_{\alpha_1\cdots\alpha_{n-3}}$.

On obtient $$t(\alpha_1\cdots\alpha_{n-1})^{-1} = S_{\alpha_1\cdots\alpha_{n-2}}(\alpha_{n-2})K(\alpha_1\cdots\alpha_{n-3})^{-1}$$

où $$S_{\alpha_1\cdots\alpha_{n-3}}(X) \in Q(\alpha_1\cdots\alpha_{n-3})[X] \text{ et } K(\alpha_1\cdots\alpha_{n-3}) \in Q(\alpha_1\cdots\alpha_{n-3}).$$

ou encore $$q(\alpha_1\cdots\alpha_{n-1})^{-1} = S_{\alpha_1\cdots\alpha_{n-2}}(\alpha_{n-1}).S_{\alpha_1\cdots\alpha_{n-3}}(\alpha_{n-2})K(\alpha_1\cdots\alpha_{n-3})^{-1}.$$

En itérant le procédé on arrive à :

$$q(\alpha_1\cdots\alpha_{n-1})^{-1} = S_{\alpha_1\cdots\alpha_{n-2}}(\alpha_{n-1}).S_{\alpha_1\cdots\alpha_{n-3}}(\alpha_{n-2})\cdots S(\alpha_1)$$

où $$S_{\alpha_1,\ldots,\alpha_i}(X) \in Q(\alpha_1,\ldots,\alpha_i)[X].$$

On obtient ainsi l'inverse de q.

V - CONCLUSION

Pour un polynôme de degré n on aura à manipuler des polynômes à plusieurs variables donc il y aura certainement des problèmes de factorisation et d'inversion.

Nous avons repris ci-dessus le dernier exemple du premier chapitre ($P = X^4+2X^3+5$). Les résultats obtenus sont beaucoup plus satisfaisants que ceux obtenus au premier chapitre.

Donc par rapport à la première approche, nous avons gagné du côté de la taille des nombres rencontrés, néanmoins il reste à discuter plus profondément l'algorithme de factorisation car ce n'est certainement pas le plus efficace. Nous avons utilisé l'algorithme de Trager, en fait, il en existe d'autre que nous citons par exemple, celui de Lenstra [Len] et celui de Weinberger [Wei].

CHAPITRE III - ETUDE DES EXTENSIONS DE Q ENGENDREES PAR DES RADICAUX

INTRODUCTION

On se propose dans ce chapitre de déterminer les règles nécessaires de calcul dans une extension de Q engendrée par des radicaux.

Jusqu'à présent, beaucoup de travaux mathématiques ont été faits pour résoudre ce problème et en particulier pour déterminer le degré d'une telle extension (A. Capelli, J.J. Mordell, M. Kneser, A. Schinzel etc..).

Ici on s'intéresse à rendre ces théorèmes sous forme algorithmique .

Notre étude est basée sur deux théorèmes (l'un de Capelli et l'autre de Schinzel)

I - HISTORIQUE, THEOREMES DE A. CAPELLI ET DE A. SCHINZEL

. En 1898, A. Capelli a démontré le théorème suivant :

Théorème

Soit K un corps de caractéristique nulle, n un entier strictement positif et a un élément non nul de K.

$[K(\sqrt[n]{a}):K] < n \iff$ 1) il existe un diviseur premier p de n tel $a = \gamma^p$ pour un γ appartenant à K ou

2) $4|n$ et $a = -4\gamma^4$ pour un γ appartenant à K. [Cap]

la condition 2) provient du fait que $X^4+4 = (X^2-2X+2)(X^2+2X+2)$.

Remarque

Ce théorème n'est valable que pour un seul radical.

. En 1953, L.J. Mordell a démontré le résultat suivant :

Théorème

Soit K un corps de nombres algébriques ; $a_1,\ldots,a_r$ des éléments de K ; $n_1,\ldots,n_r$ des entiers strictement positifs ; et $\xi_1,\ldots,\xi_r$ des éléments d'une closure algébrique de K tels que $\xi_i^{n_i} = a_i$.

Si $(\prod_{i=1}^{r} \xi_i^{x_i} \in K$ entraîne que $x_i \equiv 0 \bmod n_i)$ et (si ξ_i est réel ou K contient les racines $n_i^{\text{ième}}$ de l'unité $(1 \leq i \leq r)$) alors

$[K(\xi_1,\ldots,\xi_r) : K] = n_1 \ldots n_r$ [Mor]

Notons que ce théorème nous donne seulement une condition suffisante.

. M. Kneser a travaillé sur ce dernier résultat pour donner le théorème suivant :

Théorème

Soit K un corps, $K(\xi_1,\ldots,\xi_r)$ une extension séparable finie de K et $K^*<\xi_1,\ldots,\xi_r>$ le groupe multiplicatif engendré par les ξ_i.

$[K(\xi_1\ldots,\xi_r) : K] = [K^*<\xi_1,\ldots,\xi_r> : K^*]$ <=>

1- pour tout nombre premier p, $\mathcal{S}_p \in K^*<\xi_1,\ldots,\xi_p>$ implique $\mathcal{S}_p \in K^*$,

2- 1- $\mathcal{S}_4 \in K^*<\xi_1,\ldots,\xi_r>$ entraîne $\mathcal{S}_4 \in K^*$. [Kne]

où $[K^*<\xi_1,\ldots,\xi_r>:K^*]$ est l'index de K^* dans $K^*<\xi_1,\ldots,\xi_r>$ [Lan].
et $\mathcal{S}_p$ est une racine primitive $p^{\text{ième}}$ de l'unité.

Théorème de Schinzel

Soit K un corps. On considère l'extension $K(\xi_1,\ldots,\xi_r)/K$ où $\xi_i^{n_i} = a_i$, $a_i \in K^*$ et la caractéristique de K ne divise pas les n_i $(1 \le i \le r)$.

On note I_p l'ensemble des indices i tels que p divise n_i. Alors :

$[K(\xi_1,\ldots,\xi_r) : K] = n_1\ldots n_r$ <=>

i) pour tout nombre premier p, si $\prod_{i\in I_p} a_i^{\gamma_i} = \gamma^p$ pour un élément γ de K et des entiers x_i, alors p^p divise x_i pour tout i dans I_p.

ii) si $\prod_{i\in I_2} a_i^{x_i} = -4\gamma^4$ pour un élément γ de K et des entiers x_i tels que 4 divise $n_i x_i$ pour tout $i \in I_2$ alors 4 divise x_i pour tout $i \in I_2$. [Sch].

Nous donnons une idée de la démonstration afin d'éclaircir un peu les conditions i) et ii) :

En général, nous avons $[K(\xi_1,\ldots,\xi_r):K] \le [K^*<\xi_1\ldots\xi_r>:K^*] \le n_1\ldots n_r$.
Donc $[K(\xi_1,\ldots,\xi_r):K] = n_1\ldots n_r$ <=> $[K(\xi_1,\ldots,\xi_r):K] = [K^*<\xi_1,\ldots,\xi_r>:K^*]$,
et $[K^*<\xi_1,\ldots,\xi_r>:K^*] = n_1\ldots n_r$.

Or $[K^*<\xi_1,\ldots,\xi_r>:K^*] = n_1\ldots n_r$ <=>

(1) $\nexists\, y_i \in \mathbb{N}$, $\gamma \in K$, $\gamma\pi\xi_i^{y_i} = 1$ => $y_i \equiv 0\ [n_i]$.

et d'après le théorème de Kneser

$[K(\xi_1,\ldots,\xi_r):K] = [K^*<\xi_1\ldots\xi_r>:K^*]$ <=>

(1') pour tout premier p $\nexists\, y_i, \gamma$ tels que $\gamma\pi\xi_i^{y_i} = \mathcal{S}_p$ => $\mathcal{S}_p \in K^*$

(2') $\nexists\, y_i, \gamma$ tels que $\gamma\pi\xi_i^{y_i} = 1+\mathcal{S}_4$ => $\mathcal{S}_4 \in K^*$.

Les points (1) et (1') nous donne la condition (i) du théorème et le point (2') nous donne la condition (ii).

Remargue

Notre étude consiste à déterminer les relations de dépendances entre les ξ_i ; d'après la démonstration ci-dessus les deux conditions du théorèmes de Schinzel proviennent de relations éventuelles entre les ξ_i.

Notre première approche était d'étudier les conditions du théorème de Schinzel pour une extension $Q(\xi_1,\ldots,\xi_r)/Q$ et d'en déduire les relations sur les ξ_i, nous avons écrit un algorithme que nous avons exposé à EUROSAM 84 à Cambridge. Seulement on ne pouvait montrer que les relations obtenues étaient suffisantes pour faire du calcul dans $Q(\xi_1,\ldots,\xi_r)$. [Naj]

Nous allons présenter ici une deuxième approche qui nous assure des relations nécessaires et suffisantes en utilisant une méthode progressive.

II - ETUDE D'UNE EXTENSION DE Q ENGENDREE PAR DES RADICAUX : INTRODUCTION

On se propose dans ce paragraphe d'étudier les relations de dépendance dans une famille $\{\xi_1,\ldots,\xi_r\}$ de radicaux sur Q ($\xi_i^{n_i} = a_i$, $a_i \in Q^*$ et $n_i \in \mathbb{N}$). Ceci en étudiant d'abord ξ_1 sur Q puis les relations de dépendance éventuelles dans $\{\xi_1,\xi_2\}$ et ainsi de suite jusqu'à $\{\xi_1,\ldots,\xi_r\}$.

Etant donné $X^n-a = 0$, $a \in Q^*$ $(Q\setminus\{0\})$ et $n \in \mathbb{N}$, on considèrera la racine de a d'ordre n définie ainsi :

Si $a > 0$, alors $\sqrt[n]{a}$ désigne la racine réelle positive d'ordre n de a.

Si $a < 0$, alors $\sqrt[n]{a}$ désigne $\sqrt[n]{-1}.\sqrt[n]{|a|}$.

où

$$\sqrt[n]{-1} = \begin{cases} -1 & \text{Si n est impair} \\ \sqrt[2^\alpha]{-1} & \text{Si } n = 2^\alpha.m \text{ et } m \text{ impair.} \end{cases}$$

et $\sqrt[2^\alpha]{-1} = \mu_\alpha^{2\ell+1}$ où $\mu_\alpha = e^{i\pi/2^\alpha}$ et $0 \leq \ell < 2^\alpha$ (autrement dit $\sqrt[2^\alpha]{-1}$ est une racine quelconque de (-1) d'ordre 2^α).

$\xi = \sqrt[n]{a}$ sera défini par la donnée de a, de n et de ℓ.

Remarque

Cette définition de $\sqrt[n]{a}$ a été faite pour éviter les racines de l'unité qui risquent d'introduire plus de difficultés.

Nous avons cependant, permis les racines d'ordre 2^α de (-1) qui, elles, s'imposent sans ajouter de difficultés supplémentaires comme nous allons voir dans l'étude.

Plan de cette étude

Nous commençons (partie III) par rappeler les théorèmes de Capelli et de Schinzel ainsi que certains de leurs corollaires qui seront constamment utilisés par la suite.

Dans la partie IV nous introduisons le corps $K_0 = Q(\sqrt[4]{-1}) = Q(\sqrt{\sqrt{-1}},\sqrt{2})$ sur lequel les théorèmes de Capelli et de Schinzel ont un énoncé beaucoup plus simple.

Nous pouvons alors (partie V) étudier les extensions de la forme $K_0(\sqrt[n]{a})/K_0$ pour $a \in Q^*$. C'est en fait la partie la plus importante de l'étude elle fait intervenir dans les démonstrations de l'arithmérique et de la théorie de Galois. Nous aboutissons à un algorithme simple, dont nous montrons le fonctionnement sur un exemple.

La partie VI est consacrée à l'étude des extensions de K par deux radicaux ξ_1, ξ_2 de nombres rationnels. Nous obtenons un algorithme en deux parties : la première relation entre ξ_1 et ξ_2 est obtenue en étudiant la "grande" extension $K_0(\xi_1,\xi_2)/K_0$, ensuite les relations suivantes sont obtenues en étudiant la "petite" extension $K_0(\xi_1,\xi_2)/K_0(\xi_1)$.
Là encore les algorithmes sont simples et explicités par des exemples.

Nous concluons dans la partie VII en indiquant comment ces algorithmes peuvent se généraliser à un nombre quelconque de radicaux.

III- RESULTATS PRINCIPAUX UTILISES

Théorème 3.1 : Théorème de Capelli

Soit K un corps de caractéristique nulle.
Soit ξ un radical dans K défini par $\xi^n = a$ où n est entier et a un élément non nul de K. Alors :

$[K(\xi):K] < n$ <=> (i) $\exists$ pln p : premier tel que $a = \gamma^p$ pour un $\gamma \in K$

ou (ii) $4|n$ et $a = -4\gamma^4$ pour un $\gamma \in K$.

Théorème 3.2 : Théorème de Schinzel

Soit K un corps de caractéristique nulle.
Soit $(\xi_i)_{i=1;r}$, une famille de radicaux sur K définis par :
pour tout i $\xi_i^{n_i} = a_i$; $n_i \in \mathbb{N}$; et $a_i \in K^*$. Alors :

$[K(\xi_1,\ldots,\xi_r):K] = n_1 \ldots n_r$ <=>

(i) pour tout p premier,

Si $\prod_{i\in I_p} a_i^{x_i} = \gamma^p$ pour un $\gamma \in K^*$ et des $x_i \in \mathbb{Z}$, alors

$x_i \equiv 0[p]$ pour tout $i \in I_p$.

et (ii) Si $\prod_{i\in I_2} a_i^{x_i} = -4\gamma^4$ pour un $\gamma \in K^*$ et des $x_i \in \mathbb{Z}$ et

si $n_i x_i \equiv 0[4]$ pour tout $i \in I_2$, alors $x_i \equiv 0[4]$ pour tout $i \in I_2$.

Remarque 3.3

Dans l'énoncé du théorème 3.2, on peut supposer que les x_i appartiennent à $\{0,1,\ldots,p-1\}$ pour la condition (i) et à $\{0,1,2,3\}$, pour la condition (ii).

Démonstration :

Supposons que pour la condition (i) il existe x_{i_o} tel que $x_{i_o} < 0$ ou $x_{i_o} \geq p$.
On peut écrire $x_{i_o} = kp + r_{i_o}$ avec $0 \leq r_{i_o} < p$, et alors $\prod_{i \in I_p} a_i^{x_i} = \gamma^p$ devient :

$$(\prod_{\substack{i \in I_p \\ i \neq i_o}} a_i^{x_i}) . a_{i_o}^{r_{i_o}} . (a_{i_o}^{k})^p = \gamma^p$$

D'où

$$(\prod_{\substack{i \in I_p \\ i \neq i_o}} a_i^{x_i}) . a_{i_o}^{r_{i_o}} = \gamma'^p \quad (\text{où } \gamma' = \gamma a_{i_o}^{-k} \in K).$$

Nous pouvons donc remplacer x_{i_o} par r_{i_o} appartenant à $\{0,\ldots,p-1\}$.
Donc nous pouvons supposer tous les x_{i_o} dans $\{0,\ldots,p-1\}$.
Même chose pour la condition (ii).

□

Nous utiliserons souvent le cas particulier suivant du théorème de Schinzel.

Corollaire 3.4

Avec les notations et les hypothèses du théorème de Schinzel,

si $[K(\xi_1,\ldots,\xi_{r-1}):K] = n_1 \ldots n_{r-1}$ alors :

$$[K(\xi_1,\ldots,\xi_{r-1},\xi_r):K] < n_1 \ldots n_r \iff$$

(i') il existe un nombre p premier divisant n_r, des entiers $x_i \in \{0,\ldots,p-1\}$ (pour $i \in I_p$) avec $x_r \neq 0$ et un élément γ de K^*, tels que $\prod_{i \in I_p} a_i^{x_i} = \gamma^p$.

ou

(ii') $2 | n_r$, il existe des entiers $x_i \in \{0,1,2,3\}$ (pour $i \in I_2$) avec $x_r \neq 0$, et un élément γ de K^*, tels que $n_i x_i \equiv 0[4]$ pour tout $i \in I_2$ et $\prod_{i \in I_2} a_i^{x_i} = -4\gamma^4$.

Démonstration

Les conditions (i') et (ii') sont les négations des conditions (i) et (ii) du théorème de Schinzel avec en plus la condition $x_r \neq 0$.
En fait si $x_r = 0$, la condition (i') (resp. (ii') est la négation de (i) (resp. (ii')) pour $[K(\xi_1,\ldots,\xi_{r-1}):K]$, ce qui contredit $[K(\xi_1,\ldots,\xi_{r-1}):K] = n_1,\ldots,n_{r-1}$.
D'où nécessairement $x_r \neq 0$.

□

Corollaire 3.5

. Soit K une extension de Q engendrée par des réels et des racines de (-1) d'ordre une puissance de 2.

. Soit $a \in K^*$, et ξ un complexe vérifiant :

1) $\exists\, n \in \mathbb{N} \;/\; \xi^n = a$ et

2) $\exists\, N \in \mathbb{N}$ et $b \in Q^*$ tels que $\xi^N = b$ et ξ vérifie le choix fait dans l'introduction.

. Soit p un diviseur premier de n.

En notant $a^{1/p}$ la racine $p^{ième}$ de a définie par $a^{1/p} = \xi^{n/p}$, nous avons

$$a \in K^{*p} \iff a^{1/p} \in K^*.$$

Lemme 3.5.1.

Soit K une extension de Q de la forme $K = K'(\sqrt[2^\alpha]{-1})$ avec $K' \subset \mathbb{R}$ et α entier ($\alpha \geq 1$), et soit $K'' = K \cap \mathbb{R}$.
Alors $K = K''(i)$, de plus, la conjugaison dans K/K" (i.e : l'unique K"-automorphisme de K différent de l'identité) coïncide avec la conjugaison complexe, et $|\gamma|_C \in K''$ pour tout $\gamma \in K$.
(où $|\gamma|_C$ désigne la norme complexe de γ).

Démonstration

Posons $\nu = \sqrt[2^\alpha]{-1}$ (une racine quelconque de (-1) d'ordre 2^α).
Il est clair que K contient i car $i = \pm \nu^{2^{\alpha-1}}$.

Par ailleurs K contient $\frac{1}{\nu}$, et donc aussi $\lambda = \nu + \frac{1}{\nu}$.

Comme ν est de module (complexe) 1, son conjugué complexe est $\frac{1}{\nu}$.
Par suite $\lambda \in \mathbb{R} \cap K = K"$. Comme ν est racine du polynôme $X^2-\lambda X+1$, ($X^2-\lambda X+1 \in K"[X]$) le degré K/K" est au plus 2. Or K contient K"(i) et le degré de K"(i)/K" est 2, donc K = K"(i).

Le conjugué de i dans K/K" est (-i), donc la conjugaison σ de K/K" coïncide avec la conjugaison complexe à la fois sur l'élément i et sur le corps K" (où les deux sont l'identité). Comme K = K"(i) cela prouve que σ coïncide avec la conjugaison complexe sur K.

Enfin pour tout $\gamma \in K$, la norme de γ égale à $\gamma.\sigma(\gamma)$ dans l'extension K/K" appartient à K", donc par ce qui précède égale à $|\gamma|^2_{\mathbb{C}}$, d'où le lemme.

Démonstration du corollaire 3.5

L'implication (<=) et l'équivalence dans le cas p = 2 sont triviales.
Supposons donc $a \in K^{*p}$ et $p \neq 2$. Nous avons :

$a \in K^{*p}$ implique qu'il existe un élément γ de K^* et une racine $\mathcal{S}_p$ de l'unité d'ordre p tels que $a^{1/p} = \mathcal{S}_p.\gamma$.

Posons n' = n/p, et utilisons l'hypothèse 2) :

ξ s'écrit : $\xi = \nu^{\varepsilon N}\sqrt{|b|}$ avec $\varepsilon = 0$ ou 1 et ν est une racine d'ordre une puissance de 2 de (-1). Par suite $\xi^{n'} = \mathcal{S}_p\gamma$ entraîne que $\nu^{\varepsilon n'}(\sqrt[N]{|b|})^{n'} = \mathcal{S}_p$
$\gamma \in K^*$ donc $|\gamma|^2_{\mathbb{C}} \in K^*$ d'après le lemme 2.5.1, si K n'est pas réel, sinon c'est évident.
D'où $\nu^{\varepsilon n'}(\sqrt[N]{|b|})^{n'}/\mathcal{S}_p \in K^*$ et $(\sqrt[N]{|b|})^{2n'} \in K^*$.

En élevant le premier de ces deux éléments de K^* au carré et en faisant le rapport avec le deuxième, il vient $\nu^{2\varepsilon n'} / \mathcal{J}_p^2 \in K^*$.
Or, $\exists \beta$ entier tel que $\nu^{2^\beta} = -1$ donc $\mathcal{J}_p^{2^\beta} \in K$.
$\mathcal{J}_p^{2^\beta} \in K$ et $p \neq 2$ entraîne que $\mathcal{J}_p \in K$ (en utilisant l'identité de Bezout entre p et 2^β).

Nous avons donc montré que :

$a \in K^{*p} = \exists \gamma \in K^*, \exists \mathcal{J}_p \in K^*$ tels que $a^{1/p} = \mathcal{J}_p . \gamma$.

D'où $\mathcal{J}_p . \gamma \in K^*$ ou encore $a^{1/p} \in K^*$.

□

Corollaire 3.6

Sous les mêmes hypothèses que le corollaire 3.5 nous avons :
$[K(a^{1/p}):K] = 1$ ou p.

Démonstration

On applique le théorème de Capelli à l'extension $K(a^{1/p})/K$, on obtient :

$$[K(a^{1/p}):K] < p \iff a \in K^{*p}.$$

Or d'après le corollaire 3.5, $a \in K^{*p}$ équivaut à $a^{1/p} \in K^*$.
D'où $[K(a^{1/p}):K] < p \iff [K(a^{1/p}):K] = 1$.

Remarque : □

Ce résultat n'est pas évident, contrairement à ce qu'on pourrait croire, car c'est le cas non-Kummer et donc l'ordre de l'extension $K(a^{1/p})$ n'est pas nécessairement un diviseur de p.

IV - LE CORPS K_0

IV.1 - Introduction

Soit à étudier un radical $\xi = \sqrt[n]{a}$, n entier et a rationnel ($a \neq 0$). On peut utiliser le théorème de Capelli :

$[Q(\xi) : Q] < n \iff$ (i) $\nexists$ pln, p premier tel que $a = \gamma^p$ pour un $\gamma \in Q^*$.

ou

(ii) $4|n$ et $a = -4\gamma^4$ pour un $\gamma \in Q^*$.

Si la condition (ii) est vérifiée alors n/4 est entier et $\xi^{n/4} = \mathcal{S}_4 . \xi_0 . \sqrt{2} . \gamma$. où $\xi_0 = e^{i\pi/4}$ (la première racine de (-1) d'ordre 4 rencontrée en parcourant le cercle unité dans le sens positif) et $\mathcal{S}_4$ est une racine de l'unité d'ordre divisant 4.

Or les quatre nombres complexes $\mathcal{S}_4 \xi_0 \sqrt{2}$ sont les racines du polynôme X^4+4 qui se factorise sur Q[X] en :

$$X^4+4 = (X^2+2X+2)\ (X^2-2X+2).$$

D'où ξ vérifie une équation du type $X^{n/2} \pm 2\gamma X^{n/4} + 2\gamma^2 = 0$.
ξ est donc de degré $\leq n/2$ sur Q mais n'y est plus exprimé comme un radical.

Exemple : $\xi = \sqrt[4]{-324}$.

ξ vérifie $X^4+324 = 0$ mais aussi $X^2 \mp 6X+18 = 0$ (le signe $\mp$ dépend du choix de la racine 4ième de -1).

Notre méthode consistant à traiter seulement des radicaux, ceci consiste à priori un problème.

IV.2 - Définition du corps K_0

Nous proposons la possibilité suivante :
Puisque l'équation non radicielle obtenue provient d'une équation de la forme $\xi^{n/4} = \mathcal{J}_4 \cdot \xi_0 \sqrt{2} \cdot \gamma$, nous allons considérer le corps K_0 défini par $K_0 = Q(\xi_0)$.

Ce corps est une extension de Q de degré 4 (le polynôme minimal de ξ_0 sur Q est X^4+1). Il contient $\sqrt{2} = \xi_0(1-\xi_0^2)$ et les racines 4ième de l'unité, et donc les racines 4ièmes de (-4).

Nous allons poser dans toute la suite $\xi_0' = \sqrt{2}$.

Remarque

Nous considérons souvent K_0 comme $Q(\xi_0,\xi_0')$, car nous allons voir qu'en écrivant :
$\sqrt[4]{-4} = \mathcal{J}_4 \cdot \xi_0 \cdot \xi_0'$ au lieu de $\sqrt[4]{-4} = \mathcal{J}_4(1+\xi_0^2)$ (la première expression est multiplicative tandis que la deuxième est additive), toute relation éventuelle entre les ξ_i (additive, multiplicative ou composée des deux) se ramène à une relation multiplicative.

En fait on utilisera les deux écritures $K_0 = Q(\xi_0,\xi_0')$ et $K_0 = Q(\xi_0)$ et ce sont ces deux formes de K_0 qui vont nous permettre de résoudre la majorité des problèmes.

IV.3 - Enoncé des théorèmes de Schinzel et de Capelli sur un corps K contenant K_0.

Proposition 4.3.1

Soit K une extension de Q contenant K_0.
Soit $(\xi_i)_{i=1;r}$ des radicaux sur K définis par $\xi_i^{n_i} = a_i$.
Si la première condition du théorème de Schinzel est vérifiée pour p = 2, alors la deuxième condition est vérifiée.

Démonstration

La première condition du théorème de Schinzel pour p = 2 s'énonce :
Si $\prod_{i\in I_2} a_i^{x_i} = \gamma^2$ pour un $\gamma \in K$ et des $x_i \in \{0,1\}$ (cf. remarque 2.3)
alors $x_i = 0$ pour tout $i \in I_2$.

Supposons cette condition vérifiée, montrons que la deuxième condition du théorème de Schinzel est vérifiée.

Supposons qu'il existe des $x_i \in \{0,1,2,3\}$ (pour $i \in I_2$) et un $\gamma \in K$ tels que $\prod_{i\in I_2} a_i^{x_i} = -4\gamma^4$ et $n_i x_i \equiv 0[4]$ pour tout $i \in I_2$.

Nous avons $-4\gamma^4 = (\xi_0\xi_0'\gamma)^4$, et $\xi_0\xi_0'\gamma \in K$ (puisque $\gamma \in K$, et $\xi_0\xi_0' \in K_0 \subset K$).

D'où en posant $\gamma' = \xi_0\xi_0'\gamma$ il vient :

$$\prod_{i\in I_2} a_i^{x_i} = (\gamma'^2)^2, \quad \gamma' \in K \text{ et } x_i \in \{0,1,2,3\}.$$

Or d'après la première condition pour p = 2 ceci entraîne que $x_i \equiv 0[2]$ pour tout $i \in I_2$.

Et puisque $x_i \in \{0,1,2,3\}$ on peut dire que $x_i \in \{0,2\}$.

Posons $I_2' = \{i \in I_2 \text{ tel que } x_i = 2\}$.

$\prod_{i\in I_2} a_i^{x_i} = (\gamma'^2)^2$ se ramène à $\prod_{i\in I_2'} a_i^2 = (\gamma'^2)^2$ ou encore

$\prod_{i\in I_2'} a_i = \pm \gamma'^2 = ((i\gamma')^2$ ou $\gamma'^2)$ or $i\gamma' \in K$ (puisque $\gamma' \in K$ et $i \in K_0 \subset K$).

Donc il existe $\gamma'' \in K$ tel que $\prod_{i\in I_2'} a_i = \gamma''^2$. Ceci entraîne que $\prod_{i\in I_2} a_i^{x_i} = \gamma''^2$. D'où d'après la première condition pour p = 2, I_2' est vide et alors $x_i = 0$, pour tout $i \in I_2$, ou encore la deuxième condition du théorème de Schinzel est vérifiée.

□

Corollaire 4.3.2

On a le résultat analogue suivant pour les conditions du théorème de Capelli :
Pour un corps K contenant K_0, et un radical ξ vérifiant $\xi^n = a$ dans K. Si la première condition du théorème de Capelli n'est pas vérifiée pour p = 2 alors il en est de même pour la deuxième condition.

Démonstration :

La deuxième condition pour $K(\xi)/K$ s'écrit :

(ii) $4|n$ et $a = -4\gamma^4$ pour un $\gamma \in K^*$.

K contient K_0 donc toutes les racines 4ièmes de (-4), d'où (ii) s'écrit $4|n$ et $a = (\gamma'^2)^2$, $\gamma'^2 \in K^*$ et ceci est la condition (i) pour p = 2.

□

Conclusion

En se plaçant dans un corps K contenant K_0 on n'aura à étudier que les premières conditions des théorèmes de Schinzel et de Capelli.

V - ETUDE D'UN RADICAL DANS K_0, ALGORITHME ET EXEMPLES

Soit à étudier le radical ξ vérifiant $\xi^n = a$ (n, entier, $q \in Q^*$), sur K.

ξ vérifiant le choix énoncé dans l'introduction.

Le théorème de Capelli s'écrit :

$$[K_0(\xi) : K_0] < n \iff \nexists\ p \text{ premier, } p|n, \text{ tel que } a \in K_0^{*p}.$$

Remarque 5.1

Avec le choix fait sur $\sqrt[n]{a}$ et la structure de K_0, on peut appliquer le corollaire 3.5. Par conséquent

$$a \in K_0^{\,p} \iff a^{1/p} \in K_0^* \qquad \text{(ceci pour tout premier p divisant n).}$$

Proposition 5.2

Soit $a \in Q^*$.

$$a \in K_0^{*p} \iff \begin{cases} \text{si } p \neq 2, & a \in Q^{*p}. \\ \text{si } p = 2, & a = \varepsilon a' \text{ avec } \varepsilon \in \{+1,-1,2,-2\} \text{ et } a' \in Q^{*2}. \end{cases}$$

Démonstration

$a \in K_0^{*p} \iff a^{1/p} \in K_0^*$ (Remarque 5.1).

L'implication(<=) est immédiate.

Regardons (=>).

$a^{1/p} \in K_0^*$, $K_0 = Q(\xi_0)$ entraîne que $Q(a^{1/p}) \subset Q(\xi_0)$. Alors $[Q(a^{1/p}) : Q]$ divise $[Q(\xi_0) : Q]$.

$[Q(a^{1/p}):Q] = 1$ ou p (corollaire 2.6) et $[Q(\xi_0):Q] = 4$.

* Si $p \neq 2$ $[Q(a^{1/p}):Q] \mid [Q(\xi_0):Q]$ entraîne nécessairement $[Q(a^{1/p}):Q] = 1$, car pX4, et alors $a^{1/p} \in Q^*$ ou $a \in Q^{*p}$.

* Si p = 2 $a^{1/2} \in Q(\xi_0)$ entraîne $[Q(a^{1/2},\xi_0):Q] < 8$.

D'où en appliquant le corollaire du théorème de Schinzel à $Q(\xi_0,a^{1/2})/Q$ l'une au moins des deux conditions est vérifiée.

Nous avons donc soit :

1) première condition vérifiée :
$\exists x_1,x_2 \in \{0,1\}$, $\gamma \in Q^*$ tels que $(-1)^{x_1} a^{x_2} = \gamma^2$ et $x_2 = 1$,
d'où $a = (-1)^{-x_1}\gamma^2$ c'est-à-dire $a = \varepsilon a'$, $\varepsilon = \pm 1$ et $a' \in Q^{*2}$.

2) deuxième condition vérifiée :
$\exists\, x_1,x_2 \in \{0,1,2,3\}$ $\gamma \in Q^*$ tels que $(-1)^{x_1} a^{x_2} = -4\gamma^4$ avec $2x_2 \equiv 0[4]$, et $x_2 \neq 0$, donc $x_2 = 2$.
Alors $a^2 = \pm 4\gamma^4$. En fait $a^2 = 4\gamma^4$ (puisque a^2 et γ^4 sont positifs), d'où $a = \varepsilon a'$ avec $\varepsilon = \pm 2$ et $a' \in Q^{*2}$.

Conclusion :

$a^{1/2} \in K_0^*$ => $a = \varepsilon a'$ avec $\varepsilon \in \{1,-1,2,-2\}$ et $a' \in Q^{*2}$.

□

Cette proposition nous amènera à étudier les extensions de la forme $K_0(\xi)/K_0$ où $\xi^n = a$, avec non plus a rationnel mais $a = \xi_0^{\alpha}.\xi_0^{\beta}.a'$ où $a' \in Q^*$, nous aurons alors besoin du résultat suivant :

Notation :

Notons v_2 la "valuation 2-adique" sur Q, c'est à dire l'application de Q dans $Z \cup \{+\infty\}$ définie par :

. $v_2(0) = +\infty$.

. si n est entier, $n = 2^{v_2(n)}.m$ avec m impair

. $v_2(n_1/n_2) = v_2(n_1)-v_2(n_2)$ si n_1 et n_2 sont entiers.

Remarque : si a est entier, $v_2(a) = 0$ équivaut à : a est impair.

Proposition 5.3

Dans K_0 soit $a = \xi_0^{\alpha}\xi_0'^{\beta}a'$ avec $a' \in Q^{*+}$ et $v_2(a') = 0$.
a vérifiant les conditions du corollaire 3.5 (ie. $a = \xi^n$ avec $\xi = \sqrt[N]{b}$, $b \in Q$).
Alors pour tout premier p divisant n :

$$a \in K_0^{*p} \iff \begin{cases} p|\alpha \ , \ p|\beta \ \text{ et } a' \in Q^{*p} & \text{si } p = 2 \\ p|\beta \ \text{ et } a' \in Q^{*p} & \text{si } p \neq 2. \end{cases}$$

où Q^{*+} est l'ensemble des rationnels strictement positifs.

Notations 5.3

Pour tout entier $n \geq 1$ nous notons désormais :

* $\xi_0'^{1/n}$ le réel positif $2^{1/2n}$.

* $\xi_0^{1/n}$ le nombre complexe :

. $e^{i\pi/2^{\alpha+2}}$ si $n = 2^{\alpha}$,

. $e^{i\pi k/2^{\alpha+2}}$ si $n = 2^{\alpha}m$ avec m impair,
où K est l'inverse de m modulo 8
(donné par l'égalité de Bezout $1=mk+8k'$).

Justifions ces notations

Il est clair que

$$(\xi_0'^{1/n})^n = \xi_0' \quad \text{et que} \quad (\xi_0^{1/2^{\alpha}})^{2^{\alpha}} = \xi_0 \ ;$$

si $n = 2^{\alpha}.m$ avec m impair, alors

$$\xi_0^{1/n} = (\xi_0^{1/2^{\alpha}})^m \quad \text{donc} \quad (\xi_0^{1/n})^n = (\xi_0^{1/2^{\alpha}})^{2^{\alpha}km} = \xi_0^{km} = \xi_0.$$

Lemme 5.3.1

Pour tout nombre premier p, nous avons :

$$[K_0(\xi_0^{1/p}):K_0] = \begin{cases} 2 & \text{si } p = 2, \\ 1 & \text{si } p \neq 2 \end{cases}$$

et

$$[K_0(\xi_0^{1/p},\xi_0'^{1/p}):K_0(\xi_0^{1/p})] = p.$$

Démonstration

. $\xi_0^{1/p} = \xi_0^k$ où k est l'inverse de p modulo 8 pour $p \neq 2$.
Donc $\xi_0^{1/p} \in K_0$ et par suite $[K_0(\xi_0^{1/p}):K_0] = 1$.

. $\xi_0^{1/2} = e^{i\pi/8}$, donc $[Q(\xi_0^{1/2}):Q] = 8$ d'où $[K_0(\xi_0^{1/2}) : K_0] = \frac{8}{4} = 2$.

. Posons $K = K_0(\xi_0^{1/p})$. D'après le corollaire 3.6, $K(\xi_0'^{1/p})/K$ est de degré 1 ou p.

Supposons $[K(\xi_0'^{1/p}):K] = 1$ alors $\xi_0'^{1/p} \in K$.
D'autre part $K = K_0(\xi_0^{1/p}) = Q(\xi_0^{1/p})$ qui est une extension cyclotomique sur Q donc abelienne.

D'où $Q(\xi_0'^{1/p})/Q$ est aussi abelienne donc galoisienne. Par suite $Q(\xi_0'^{1/p})/Q$ contient tous les conjugués de $2^{1/2p}$ c'est-à-dire aùssi les racines de l'unité d'ordre 2p qui ne sont pas des nombres réels.
Or $Q(2^{1/2p}) \subset \mathbb{R}$, d'où la contradiction, et donc $[K(\xi_0'^{1/p}):K] = p$.

Démonstration de la proposition 5.3

L'implication (<=) est immédiate, vu que $\xi_0^{1/p} \in K_0^*$ pour $p \neq 2$.
Montrons (=>) :

Soit $a = \xi_0^{\alpha}\xi_0'^{\beta} a'$, un élément de K_0 avec a' un rationnel strictement positif et $v_2(a') = 0$.

$a \in K_0^{*p}$ entraîne qu'il existe un élément γ de K_0 tel que :
$\xi_0^{\alpha}\beta_0'^{\beta} a' = \gamma^p$.

Soit ℓ un nombre premier différent de 2.
L'idéal engendré par ℓ dans Q noté (ℓ) ne se ramifie pas dans K_0.
En effet, seuls les idéaux engendrés par les diviseurs du discriminant de K_0/Q se ramifient. Or $\Delta K_0/Q$ divise 4^4, [Sam], donc seul (2) se ramifie et $\ell \neq 2$.

Soit $\mathcal{L}$ un idéal premier de K_0 divisant (ℓ). On peut définir la valuation $\mathcal{L}$-adique sur K_0 de manière analogue à la valuation 2-adique sur Q [Sam].

Par suite, l'égalité $\xi_0^{\alpha}\xi_0'^{\beta}a' = \gamma^p$ donne $\alpha v_{\mathcal{L}}(\xi_0)+\beta v_{\mathcal{L}}(\xi_0')+v_{\mathcal{L}}(a') = pv_{\mathcal{L}}(\gamma)$.
Il est clair que $v_{\mathcal{L}}(\xi_0) = v_{\mathcal{L}}(\xi_0') = 0$, d'où $v_{\mathcal{L}}(a') = pv_{\mathcal{L}}(\gamma)$.
Or $v_{\mathcal{L}}(a') = v_{\ell}(a')$ car $a' \in Q^*$, et (ℓ) non ramifié.

$v_{\ell}(a') = pv_{\mathcal{L}}(\gamma)$ entraîne que $v_{\ell}(a')$ est un multiple de p et ceci pour tout nombre premier $\ell \neq 2$.
Puisque $v_2(a') = 0$, alors c'est que $a' \in Q^{*p}$.
Nous avons donc montré que

$a \in K_0^{*p}$ et $a = \xi_0^{\alpha}\xi_0'^{\beta} a'$ entraîne que $a' \in Q^{*p}$, et alors

$\xi_0^{\alpha}\xi_0'^{\beta} \in K_0^{*p}$.

Or ceci entraîne que p/β et (p/α si $p = 2$) d'après le lemme 5.3.1 et le théorème de Schinzel.

□

ALGORITHME 1 - EXEMPLE

Algorithme 1 : Redrad

Entrée : a, n, ℓ : $a \in Q^*$; n, $\ell \in \mathbb{N}$ tels que $\xi = \sqrt[n]{a}$, et ℓ est lié au choix éventuel de $\sqrt[n]{-1}$ précisé dans l'introduction de ce sous-paragraphe.

Sortie : t, t', b, n : $b \in Q^*$; t,t',n $\in \mathbb{N}$ tels que $\xi^n = \xi_0^t \xi_0'^{t'} b$ et $[K_0(\xi) : K_0] = n$.

1- {on étudie la première condition du théorème de Capelli pour $p \neq 2$}.
pour p = 3 jusqu'à n et p premier faire :

1.1 tant que $p|n$ et $a^{1/p} \in Q$ faire
$n \leftarrow n/p$, $a \leftarrow a^{1/p}$,

2- {on étudie la première condition du théorème de Capelli pour p = 2}
{théorème de Capelli pour p = 2 et $a \in Q^*$}.
Si $2|n$ et si $a = (-1)^t 2^{t'} b^2$ avec $b > 0$, $v_2(b) = 0$ et $t \in \{0,1\}$ faire

2.1 $n \leftarrow n/2$, $t \leftarrow 2t(2\ell+1)m$ (m tel que $n = 2^{\alpha}.n$ et $2 \nmid m$)

2.2 {théorème de Capelli pour p = 2 et $a \in K_0^*$}
tant que $2|n$ et $2|t$ et $2|t'$ et $b^{1/2} \in Q$ faire
$n \leftarrow n/2$, $t \leftarrow t/2$, $t' \leftarrow t'/2$, $b \leftarrow b^{1/2}$.

3- Sinon $t \leftarrow 0$, $t' \leftarrow 0$, $b \leftarrow a$;

4- retourner (t,t',b,n). fin.

Explications sur l'algorithme 1

Etape 1

On ne considère que les diviseurs premiers p de n différents de 2.
$a \in K_0^{*p}$ avec $a \in Q^*$ équivaut à : $a \in Q^{*p}$ (proposition 5.2).
Pour tester si $a \in Q^{*p}$ on peut procéder ainsi :

$a \in Q^{*p}$ et $a = \alpha/\beta$; $\alpha,\beta \in \mathbb{Z}\setminus\{0\}$ si et seulement si $\alpha \in \mathbb{Z}^p$ et $\beta \in \mathbb{Z}^p$.
Pour tester si $\alpha \in \mathbb{Z}^p$ on propose de calculer la partie entière de la racine pième réelle de α et de l'élever à la puissance p.
Si on retrouve α c'est que $\alpha \in \mathbb{Z}^p$ sinon $\alpha \notin \mathbb{Z}^p$.
Un algorithme plus efficace est donné par Cavines [Cav]
Si le test $a \in Q^{*p}$ est positif, c'est que $\xi^n = a$ peut s'écrire de façon plus réduite $\xi^{n/p} = a^{1/p}$ et alors $[K_0(\xi):K_0] \leq n/p < n$.
Dans ce cas on change n en n/p et a en $a^{1/p}$.

Si p divise encore n on refait le test pour les nouveaux n et a, lorsque p ne divise plus n ou lorsque le test devient négatif, on passe à un autre p.

Etape 2

A la fin de la première étape on a une expression de ξ sous la forme $\xi = \sqrt[n]{a}$ avec $a \notin Q^{*p}$ pour tout diviseur premier p de n différent de 2.

Si $2 \mid n$ et $a \in Q^*$.

$a \in K_0^{*2} \Leftrightarrow a = \varepsilon a'$ avec $\varepsilon \in \{+1,-1,2,-2\}$ et $a' \in Q^{*2}$ (propo. 5.2)

$\varepsilon \in K_0^{*2}$ pour tout $\varepsilon \in \{+1,-1,2,-2\}$.

Or $a = \varepsilon a'$ si et seulement si a est de la forme $a = (-1)^t.2^{t'}.b^2$ avec $t \in \{0,1\}$ et b est un rationnel strictement positif et $v_2(b) = 0$.
Dans ce cas on peut écrire $\xi^n = a$ de façon plus réduite.

$\xi^{n/2} = \xi_0^{2tm(2\ell+1)}.\xi_0^{t'}.b$ (où m est tel que $n = 2^\alpha m$ et 2Xm).

En effet :

ξ est défini par : $\xi = \mu_\alpha^{t(2\ell+1)} \sqrt[n]{|a|}$ (cf. introduction du § I).

$0 \leq \ell < 2^\alpha$, α est tel que $n = 2^\alpha.m$, 2Xm.
t vaut 0 si a est positive et 1 si a est négatif.
$\mu_\alpha = e^{i\pi/2^\alpha}$ et $\sqrt[n]{|a|}$ est la racine réelle positive de $|a|$.
si $a = (-1)^t 2^{t'} b^2$ avec $t \in \{0,1\}$.
Alors :

$$\xi = \mu_\alpha^{t(2\ell+1)} \sqrt[n]{2^{t'} b^2}$$

et

$$\xi^{n/2} = \mu_\alpha^{t\frac{n}{2}(2\ell+1)} \sqrt[n]{2^{t'} b^2}.$$

$$= \mu_\alpha^{t.2^{\alpha-1}.m(2\ell+1)} \xi_0^{t'} b. \qquad (n = 2^\alpha.m)$$

$$= \xi_0^{2tm(2\ell+1)} \xi_0^{t'} b.$$

Et alors on change n en n/2, on affecte à t la valeur $2tm(2\ell+1)$, on ne change pas t'.

On obtient une expression de a sous la forme $a = \xi_0^t \xi_0^{t'} b$.
Si 2 divise le nouveau n, on applique la proposition 5.3 pour tester si $a \in K_0^{*2}$:

$$a \in K_0^{*2} \iff 2|t,\ 2|t' \text{ et } b \in Q^{*2}.$$

Dans ce cas $\xi^n = a$ peut s'écrire $\xi^{n/2}_{n_0} = \xi_0^{t/2} \xi_0^{t'} b^{1/2}$
en effet, notons n_0, a_0, t_0 tels que $\xi^{n_0} = a_0 \in Q$ et
$\xi = \mu_\alpha^{t_0(2\ell+1)} \sqrt[n_0]{|a_0|}$.

On a $n = n_0/2$, $t = 2\, t_0 m(2\ell+1)$ et $a_0 = (-1)^{t_0} \xi_0^{2t'} b^2$.
Donc

$$\xi^{n/2} = \xi^{n_0/4} = \mu_\alpha^{t_0 2^{\alpha-2} m(2\ell+1)} \sqrt[n_0]{|a_0|}$$

$$= \xi_0^{t_0 m(2\ell+1)} \sqrt[n_0]{|a_0|} \qquad (\xi_0 = \mu_\alpha^{2^{\alpha-2}})$$

$$= \xi_0^{t/2} \cdot \xi_0^{t'/2} \cdot b^{1/2} \qquad \alpha \geq 2 \text{ car } 2|n.$$

$\xi^{n/2} = \xi_o^{t/2}\, \xi_o'^{t'/2}\, b^{1/2}$, on change alors n en n/2, t en t/2, t' en t'/2 et b en $b^{1/2}$.
On obtient les relations suivantes $n = \frac{n_o}{4}$, $t = t_o m(2\ell+1)$ et $a_o = (-1)^{t_o}\, \xi_o'^{4t}\, b^4$.

On continue jusqu'à ce que l'une des conditions : $2 \mid n$, $2 \mid t$ $2 \mid t'$ ou $b \in Q^{*2}$ ne soit plus vérifiée. On retourne les valeurs de t, t', b et n qui vérifient alors $\xi^n = \xi_o^t\, \xi_o'^{t'}\, b$ et $[K_o(\xi):K_o] = n$. En effet :

A la fin de l'étape 1 on a ξ sous la forme $\xi^N = B \in Q$ avec pour tout diviseu premier p de N différent de 2 $B \notin Q^{*p}$.

A la fin de l'étape 2 on a ξ sous la forme $\xi^n = \xi_o^t\, \xi_o'^{t'}\, b$ avec l'une des conditions $2 \mid n$, $2 \mid t$, $2 \mid t'$, $b \in Q^{*2}$ n'est pas vérifiée.

Supposons qu'il y ait une relation avec $p \neq 2$, c'est que

$$p \mid n \text{ et } \xi_o^t\, \xi_o'^{t'}\, b \in K_o^{*p}.$$

. $p \mid n$ entraîne que $p \mid N$ puisque $N = n.2^\beta$ $\beta \geq 0$ et $p \neq 2$.

. $\xi_o^t\, \xi_o'^{t'}\, b \in K_o^{*p}$ entraîne que $p \mid t'$ et $b \in Q^{*p}$ (proposition 4.3).
$N = n.2^\beta$ et $\xi^n = \xi_o^t\, \xi_o'^{t'}\, b$ entraîne que

$$\xi^N = B = [\xi_o^t\, \xi_o'^{t'}\, b]^{2^\beta} = \xi_o^{t.2^\xi}\, \xi_o'^{t'2^\xi}\, b^{2^\beta}$$

$$= (\mp 1)\, 2^{t'2^{\beta-1}}\, b^{2^\beta}$$

$p \mid t'$ et $b \in Q^{*p}$ entraîne alors que $B \in Q^{*p}$, or $p \mid n$.
Donc $B \in Q^{*p}$ ne peut avoir lieu et par suite il n'y a plus de relation avec $p \neq 2$.
On conclut que $[K_o(\xi) : K_o]$ = la nouvelle valeur de n.

Exemple :

Reprenons l'exemple du paragraphe IV

.$\xi = \sqrt[4]{-324}$ avec $\ell = 0$, c'est-à-dire $\xi = \xi_0 \sqrt[4]{324}$.

* $n = 4$, $a = -324$, $\ell = 0$.
  Le seul diviseur premier de n est 2.
  $p = 2$, $2 \mid n$, et $a = -2^2.9^2$ $(t = 1, t' = 2, b = 9)$.
  donc
  $n \leftarrow n/2 = 4/2 = 2$
  $t \leftarrow 2t(2\ell+1) = 2$
  $t' \leftarrow t' = 2$
  $b \leftarrow b = 9$

* $n = 2$, $a = \xi_0^2.\ \xi_0'^2.3^2$ $(t = 2, t' = 2, b = 3)$
  donc
  $n \leftarrow n/2 = 2/2 = 1$
  $t \leftarrow t/2 = 1$
  $t' \leftarrow t'/2 = 1$
  $b \leftarrow b = 3$

* $n = 1$, $a = \xi_0.\xi_0'.3$.
  $n = 1$, donc on s'arrête et alors $\underline{[K_0(\xi):K_0] = 1}$ et $\underline{\xi = 3\xi_0\xi_0'}$.

VI- ETUDE DE DEUX RADICAUX SUR K_0

VI-1 INTRODUCTION

Soit à étudier l'extension $K_0(\xi_1,\xi_2)/K_0$ où ξ_1 et ξ_2 sont définis par : $\xi_1^{n_1} = a_1$, $\xi_2^{n_2} = a_2$; où a_1, a_2 sont des rationnels non nuls, n_1 et n_2 des entiers strictement positifs et ξ_1, ξ_2 vérifient le choix fait dans l'introduction.

En appliquant l'algorithme "redradical" à ξ_1 et à ξ_2 on obtient de nouvelles expressions pour ξ_1 et ξ_2 de la forme :

* $\xi_1^{n_1} = a_1$, avec $a_1 = \xi_0^{t_1}\xi_0'^{t_1'} a_1'$ et $[K_0(\xi_1):K_0] = n_1$

* $\xi_2^{n_2} = a_2$, avec $a_2 = \xi_0^{t_2}\xi_2'^{t_2'} a_2'$ et $[K_0(\xi_2):K_0] = n_2$

et où t_1, t_1', t_2, t_2' sont des entiers relatifs et a_1', a_2' sont des nombres rationnels avec $v_2(a_1') = v_2(a_2') = 0$.

Dans ce paragraphe on se propose d'étudier dans K_0 deux radicaux de la forme ci-dessus.

L'application du théorème de Schinzel à l'extension $K_0(\xi_1,\xi_2)/K_0$ permet de trouver une relation entre ξ_1 et ξ_2, ou de prouver qu'il n'en existe pas (voir § VII.2).

Dans le premier cas, l'existence d'autres relations entre ξ_1 et ξ_2 est étudiée en appliquant le théorème de Capelli à l'extension $K_0(\xi_1,\xi_2)/K_0(\xi_1)$. (§ VI.3).

VI-2 Théorème de Schinzel pour une extension $K_0(\xi_1,\xi_2)/K_0$. Algorithmes et Exemples.

Le théorème de Schinzel appliqué à $K_0(\xi_1,\xi_2)/K_0$ s'énonce :

$[K_0(\xi_1,\xi_2):K_0] = n_1.n_2$ <=> pour tout diviseur premier p commun à n_1 et n_2.
Si $a_1^{x_1}.a_2^{x_2} = \gamma^p$ pour un $\gamma \in K_0$ et $x_1, x_2 \in \{0,1,\ldots,p-1\}$ alors $x_1 = x_2 = 0$.

Remarque 6.2.1

Si n_1 et n_2 sont premiers entre eux alors $[K_o(\xi_1,\xi_2):K_o] = n_1 \cdot n_2$.

Remarque 6.2.2

Il existe une décomposition de a_1' et a_2' en facteurs q_i entiers telle que :

$$a_1' = q_1^{s_{11}} \cdot q_2^{s_{12}} \cdots q_\ell^{s_{1\ell}} .$$

et

$$a_2' = q_1^{s_{21}} \cdot q_2^{s_{22}} \cdots q_\ell^{s_{2\ell}}$$

Les s_{ij} sont des entiers relatifs et les $(q_i)_{i=1;\ell}$ vérifient $(q_i,q_j) = 1$ pour $i \neq j$ et $q_i \notin Q^{*p}$ pour tout nombre premier p et tout i. (cf. Algorithme 2).

Proposition 6.2.3.

En utilisant la décomposition de a_1 et a_2 sur $\{\xi_o,\xi_o',q_1,\ldots,q_\ell\}$, nous avons :

$$a_1^{x_1} a_2^{x_2} = \gamma^p \text{ pour un } \gamma \in K_o \text{ et pour } x_1,x_2 \in \{0,\ldots,s-1\} \Leftrightarrow S^T X \equiv 0[p].$$

Où $X = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ et

$$S = \begin{cases} \begin{bmatrix} t_1 & t_1' & s_{11} & \cdots & s_{1\ell} \\ -t_2 & t_2' & s_{22} & \cdots & s_{2\ell} \end{bmatrix} & \text{si } p = 2 \\ \begin{bmatrix} t_1' & s_{11} & \cdots & s_{1\ell} \\ t_2' & s_{21} & \cdots & s_{2\ell} \end{bmatrix} & \text{si } p \neq 2 \end{cases}$$

Démonstration

Nous avons $$a_1 = \xi_o^{t_1} \xi_o'^{t_1'} q_1^{s_{11}} \cdots q_\ell^{s_{1\ell}}$$

et

$$a_2 = \xi_o^{t_2} \xi_o'^{t_2'} q_1^{s_{21}} \cdots q_\ell^{s_{1\ell}}$$

donc $a_1^{x_1}a_2^{x_2}$ est de la forme $\xi_o^t \xi'^{t'}_o q$ avec :

$$t = x_1t_1+x_2t_2$$
$$t' = x_1t'_1+x_2t'_2$$
$$q = q_1^{x_1s_{11}+x_2s_{21}} \dots q_\ell^{x_1s_{1\ell}+x_2s_{2\ell}}.$$

a_1 et a_2 vérifient les hypothèses du corollaire 2.5 donc $a_1^{x_1}a_2^{x_2}$ vérifie aussi ces hypothèses. Par suite en appliquant la proposition 4.3 on obtient :

$$a_1^{x_1}a_2^{x_2} \in K_o^{*p} <=> \begin{cases} p/t,\ p/t' \text{ et } q \in Q^{*p} & \text{si } p = 2 \\ p/t' \text{ et } q \in Q^p & \text{si } p \neq 2 \end{cases}$$

$p|t$ équivaut à $x_1t_1+x_2t_2 \equiv 0[p]$.
$p|t'$ équivaut à $x_1t'_1+x_2t'_2 \equiv 0[p]$.
$q \in Q^{*p}$ équivaut à $x_1s_{1_i} + x_2s_{2_i} \equiv 0[p]$ pour $i = 1;\ell$ (puisque $(q_i,q_j)=1$ pour $i\neq j$ et $q_i \notin Q^{*p}$ pour tout i).

On obtient donc un système linéaire modulaire en x_1,x_2 qui s'écrit $S^TX \equiv 0[p]$, X et S comme décrit dans l'énoncé de la proposition.

□

Algorithme 2 : "formq"

Entrée : a[1:r] un tableau d'entiers

Sortie : q[1:ℓ] le vecteur des facteurs premiers entre eux.
s[1:r,1:ℓ] tableau d'entiers tel que

$$a[i] = \prod_{j=1}^{\ell} q[j] \uparrow s[i,j] \quad \text{pour } i = 1 \text{ jusqu'à } r$$

(1) q[1] := -1, pour i:=1:r faire s[i,1]:=si a[i] < 0 alors 1 sinon 0

(2) pour i:=2 : r+1 faire
(2.1) q[i] := |a[i-1]| (| | : valeur absolue)
(2.2) pour j:=2 : r+1 faire s[i-1,j] = δ_i^j (δ_i^j = 1 si i=j, 0 sinon)

(3) ℓ := r+1, pour i:=1 : ℓ-1 faire

(3.1) pour j:=i+1:ℓ faire
(3.1.1) tant que j ≤ ℓ et q[i] = q[j] faire
- supprimer q[i]
- ième colonne := ième colonne+jième colonne (colonnes de S)
- ℓ:= ℓ-1,

(3.1.2) b:=si j ≤ ℓ alors pgcd(q[i],q[j]) sinon 1
tantque b≠1 faire
q[i]:=q[j]/b, q[j]:=q[j]/b
si q[i]≠1
alors si q[j]≠1
alors - ℓ:=ℓ+1, q[ ]:=b
- ℓème colonne:=ième colonne+jième colonne
sinon - q[j]:=b
- jème colonne:=ième colonne+jième colonne
sinon - q[i]:=b
- ième colonne:=jième colonne+ième colonne
b:=pgcd(q[i],q[j]).

Remargue : siàla sortie $q_i \in Q^{*p}$ on remplace q_i par $q_i^{1/p}$ et s[i,j] par p.s[i,j] (pour j=1;r) et ceci tant que $q_i \in Q^{*p}$.

Algorithme

Algorithme 2 : "drad"

Entrée : $a_1, n_1 : n_1 \in \mathbb{N}$, a_1 donné par (t_1, t_1', a_1')
$a_2, n_2 : n_2 \in \mathbb{N}$, a_2 donné par (t_2, t_2', a_2')

Sortie : ou bien $K_0(\xi_1, \xi_2) : K_0 = n_1 . n_2$
ou bien (x_1, x_2, p, γ) tels que $a_1^{x_1} . a_2^{x_2} = \gamma^p$
où p est un diviseur premier de n_1 et n_2, $p \nmid x_1$, $p \nmid x_2$ et $\gamma \in K_0$

1°) si $\text{pgcd}(n_1, n_2) = 1$ alors retourner $([K_0(\xi_1, \xi_2) : K_0] = n_1 . n_2)$ fin.

2°) former les facteurs q_i et la matrice S du système.

3°) pour tous les diviseurs premiers p communs à n_1 et à n_2 faire
3.1 si p = 2 alors résoudre $S^T X \equiv 0[2]$
sinon résoudre $S'^T X \equiv 0[p]$ (S' désigne S privée de la premièr
colonne)

4°) si $X \not\equiv 0[p]$ alors
calculer γ et retourner (x_1, x_2, p, γ) fin

5°) retourner (le test $[K_0(\xi_1, \xi_2) : K_0] = n_1 . n_2$ est vrai) fin.

Remarque

Cet algorithme peut être appliqué à un nombre quelconque de radicaux de la même forme.

Exemples

EX1 $\xi_1 = \sqrt[4]{-9}$ avec pour choix $\sqrt[4]{-1} = \xi_0$ $(\ell=0)$
$\xi_2 = \sqrt{6}$

1°) Etude de ξ_1 dans K_0

- $n_1 = 4$, $a_1 = -3^2$
- le seul diviseur premier de n_1 est 2.

. p=2 $2 | n_1$ et $a_1 = -3^2$ $(t=1, t'=2, b=3^2)$
$b \in Q^{*2}$ donc $n \leftarrow n/2 = 2$
$t \leftarrow 2t(2K+1)=2$
$t' \leftarrow t' = 2$
$b \leftarrow b^{1/2} = 3$
$\Rightarrow n=2$, $a_1=\xi_0^2.3$.

. p=2 $2 | n_1$ et $a_1 = \xi_0^2.3$ $(t=2, t'=0, b=3)$.
$b \in Q^{*2}$ donc on ne peut pas réduire.

- D'où $[K_0(\xi_1):K_0] = 2$ et $\xi_1^2 = 3\xi_0^2$

2°) Etude de ξ_2 dans K_0

- $n_2=2$, $a_2 = 6 = 2.3$
- le seul diviseur premier de n_2 est 2

. p=2 $2/n_2$ et $a_2 = \xi_0'^2.3$ $(t=0, t'=2, b=3)$
$b \notin Q^{*2}$ donc on ne peut pas réduire.

- D'où $[K_0(\xi_2):K_0]= 2$ et $\xi_2^2 = 3\xi_0'^2$

3°) Etude de ξ_1, ξ_2 dans K_0

$a_1 = 3\xi_0^2$ $n_1 = 2$
$a_2 = 3\xi_0'^2$ $n_2 = 2$
entraîne $S = \begin{bmatrix} 2 & 0 & 1 \\ 0 & 2 & 1 \end{bmatrix}$ $(q_1=3)$

- p=2. $2|n_1$ et $2|n_2$

$$S^T \begin{pmatrix} -1 \\ 1 \end{pmatrix} = \begin{pmatrix} -2 \\ 2 \\ 0 \end{pmatrix} \equiv 0[2]$$

d'où $x_1 = -1$, $x_2 = 1$, $\gamma = \xi_0^{-1}\xi_0'$

c'est-à-dire $a_2 = a_1(\xi_0^{-1}\xi_0')^2$

ou encore $\xi_2 = \xi_1\xi_0^{-1}\xi_0'$

Donc $\xi_2 \in K_0(\xi_1)$ c'est-à-dire

$$\underline{[K_0(\xi_1,\xi_2):K_0] = [K_0(\xi_1):K_0] = 2 \text{ et } \xi_2 = \xi_1.\xi_0^{-1}.\xi_0'}.$$

Remarque

On a obtenu une relation de dépendance entre ξ_2 et ξ_1 exprimée multiplicativement dans K_0.
Si on veut déterminer la relation entre ξ_2 et ξ_1 qui s'ensuit dans Q on obtient :

$$\xi_2 = \xi_1(1 - \frac{1}{3}\xi_1^2) \text{ qui est une relation additive.}$$

De plus $[Q(\xi_1,\xi_2):Q] = [Q(\xi_1):Q] = 4$.

Conclusion

$$\underline{\sqrt{6} = \sqrt[4]{-9}\,(1 - \frac{1}{3}\sqrt[4]{-9}) \text{ avec } \sqrt[4]{-9} = e^{i\frac{\pi}{4}}.\sqrt[4]{9}.}$$

EX2

Si on change le choix de $\sqrt[4]{-1}$ dans l'exemple 1 en prenant :

$$\xi_1 = \sqrt[4]{-9} \text{ et } \sqrt[4]{-1} = \xi_0^3 \quad (\ell = 1)$$

on obtient :

1- $n_1 = 2$, $a_1 = 3\xi_0^6$

2- ne change pas

3- $S = \begin{bmatrix} 6 & 0 & 1 \\ 0 & 2 & 1 \end{bmatrix}$,

$S^T X \equiv 0[2]$ nous donne $x_1 = -1$, $x_2 = 1$, et $\gamma = \xi_0^{-3}\xi_0'$.

d'où la relation de dépendance entre ξ_1 et ξ_2.

$$\underline{\xi_2 = \xi_1 \xi_0^{-3} \xi_0'}$$

Cette relation se traduit sur Q par :

$$\underline{\xi_2 = \xi_1 \left(\frac{1}{3}\xi_2^2 - 1\right)}$$: l'opposé de la relation de l'exemple 1.

Conclusion 6.2.4.

En appliquant l'algorithme "drad" à ξ_1 et ξ_2 dans K_0 nous avons deux possibilités d'arrêt :

1°) soit $K_0(\xi_1,\xi_2):K_0 = n_1.n_2$; dans ce cas la famille $\{\xi_1^i \xi_2^j,\ 0 \le i \le n_1-1,\ 0 \le j \le n_2-1\}$ est une famille minimale qui engendre $K_0(\xi_1,\xi_2)/K_0$.

2°) Soit on trouve une relation liant a_1 et a_2 de la forme :
$a_1^{x_1} a_2^{x_2} = \gamma^p$ $\gamma \in K_0$ et γ se décompose aussi sur $(\xi_0,\xi_0', q_1,\ldots,q_\ell)$.
Ceci entraîne une relation sur ξ_1,ξ_2 de la forme

$$\xi_1^{n_1 x_i/p} \cdot \xi_2^{n_2 x_2/p} = \gamma$$

ou encore

$$\xi_2^{x_2 x_2/p} = \gamma . \xi_1^{-n_1 x_1/p}$$

En posant $t_{21} = -\frac{n_1 x_1}{p}$ et en changeant n_2 en $n_2 x_2/p$ et a_2 en $\gamma . \xi_1^{-n_1 x_1/p}$ on obtient que ξ_2 vérifie $X^{n_2} - a_2 = 0$ avec $a_2 \in K_0(\xi_1)$ et $a_2 = \gamma \xi_1^{t_{21}}$.

Nous sommes donc amené à étudier les extensions de la forme $K_1(\xi)/K_1$ où $K_1 = K_0(\xi_1)$, $\xi^n = a$ et a se décompose sur $(\xi_0,\xi_0', q_1,\ldots,q_\ell,\xi_1)$.

En effet, en utilisant les expressions de ξ_1 et de ξ_2 initiales dans Q on affirme que $\xi_1^{n_1 x_1/p} . \xi_2^{n_2 x_2/p}$ se décompose sur ξ_o, ξ_o' et des rationnels donc $\xi_1^{n_1 x_1/p} . \xi_2^{n_2 x_2/p} = \delta_p \gamma$ entraîne $\delta_p = 1$ car :

si $p \neq 2$, $\delta_p \in K_o = Q(\xi_o)$ entraîne $\delta_p = 1$.

si $p=2$, $\delta_p = 1$ (cf. explication de l'algorithme 1).

VI-3 Théorème de Capelli pour une extension $K_o(\xi_1,\xi)/K_o(\xi_1)$ Algorithme et Exemples

Le théorème de Capelli appliqué à $K_o(\xi_1,\xi)/K_o(\xi_1)$ où ξ est défini par $\xi^n = a$ avec $a \in K_o(\xi_1)$ et a se décompose sur $(\xi_o,\xi_o',q,\ldots q_\ell,\xi_1)$ s'énonce :

$$[K_o(\xi_1,\xi):K_o(\xi_1)] < n \iff \nexists\ p \text{ : premier pln et } a \in K_o(\xi_1)^{*p}.$$

Dans toute la suite on posera $K_1 = K_o(\xi_1)$.

Proposition 6.3.1.

Soit K un corps contenant K_o.
Soit ξ_1 un radical sur K défini par $\xi_1^{n_1} = a_1$ ($a_1 \in K$) et $[K(\xi_1):K] = n_1$.
Soit p un nombre premier tel que $a_1^{1/p} \notin K$.
Un élément a de la forme $b.\xi_1^{t_1}$ ($b \in K$, t_1 entier) est une puissance pième dans $K(\xi_1)$ si et seulement si il existe α ($0 \leq \alpha < p$) tel que ba_1^α est une puissance pième dans K et $t_1 \equiv n_i\alpha[p]$.

En d'autres termes

$a = b\xi_1^{t_1}$, $a \in K(\xi_1)^{*p} \iff \exists\ \alpha (0 \leq \alpha < p)$ tel que $ba_1^\alpha \in K^{*p}$ et $t_1 \equiv n_i\alpha[p]$.

Remarque

Cette proposition permet de ramener un test de puissance dans $K^{*}_{<\xi_1>}$ en un test de puissance dans K.

Lemme 6.3.2

Dans un corps K contenant K_0
soit a et b deux éléments K, p un nombre premier et n entier tel que $p \mid n$. Nous avons

$$b^{1/p} \in K(a^{1/n}) \iff K(b^{1/p}) = K(a^{1/p}) \quad \text{ou} \quad b^{1/p} \in K.$$

Démonstration

L'implication (<=) est immédiate.
Démontrons (=>).

$b^{1/p} \in K(a^{1/n})$ entraîne que $[K(b^{1/p},a^{1/n}):K] < p.n.$

Donc en appliquant le corollaire du théorème de Schinzel :
il existe $x_1,x_2 \in \{0,1,\ldots,p-1\}$, $\gamma \in K$ tels que $b^{x_1}.a^{x_2} = \gamma^p$ et $x_1 \neq 0$,
d'où $b^{x_1} = a^{-x_2}\gamma^p$.

$0 < x_1 < p$ entraîne que $(p,x_1) = 1$ et alors en appliquant l'identité de Bezout à x_1 et à p : il existe 2 entiers k_1,k_2 tels que $k_1x_1+k_2p = 1$, d'où
$b = b^{k_1x_1+k_2p} = a^{-x_2k_1}\gamma'^p$ où $\gamma' = \gamma^{k_1} b^{k_2} \in K$.

Par suite :

$b^{1/p} \in K(a^{1/n})$ entraîne qu'il existe α entier, $\gamma' \in K$ tels que $b = a^{\alpha}\gamma'^p$ $(\alpha = -x_2k_1)$.

. Si $p \mid \alpha$ alors $b \in K^{*p}$

. Si $p \nmid \alpha$ alors $\alpha = k.p+r$; $r \neq 0$ et $r < p$
et $b = a^r.\gamma''^p$ $(\gamma'' = \gamma' a^k)$

ce qui est équivalent à $K(b^{1/p}) = K(a^{1/p})$.

□

Remarque 6.3.3.

Ceci est vrai même si pXn car dans ce cas nécessairement $b^{1/p} \in K$ (en utilisant le théorème de Capelli par exemple).

Lemme 6.3.4.

Avec les hypothèses de la proposition 6.3.1. :
si $p|n_1$ alors :

$$a \in K_1^{*p} \Rightarrow p|t_1.$$

Démonstration

$a = b\xi_1^{t_1}$

$a \in K_1^{*p}$, entraîne $a^{1/p} \in K_1^*$ (a et p vérifient les hypothèses du corollaire 3.5)

$a^{1/p} = b^{1/p}\xi_1^{t_1/p}$ (pour une certaine racine pième de b et une certaine racine pième de $\xi_1^{t_1}$).

1er cas : p|n1

D'après le lemme 6.3.4, p divise alors t_1
$p|t_1$ et $b^{1/p}\ \xi_1^{t_1/p} \in K_1$ entraînent que $b^{1/p} \in K_1$.
Or $K_1 = K(a_1^{1/n_1})$, donc $K(b^{1/p}) \subset K(a_1^{1/n_1})$.
D'où d'après le lemme 6.3.2 $b^{1/p} \in K$ ou $K(b^{1/p}) = K(a_1^{1/p})$,
c'est-à-dire il existe α entier $0 \leq \alpha < p$ tel que $ba_1^{\alpha} \in K^{*p}$ et
puisque $p|n_1$ et $p|t_2$ alors $t_1 \equiv n_1\alpha[p]$.

2ème cas : ptn1

- si $p|t_1$ alors $b^{1/p} \in K_1 = K(a_1^{1/n_1})$

et puisque ptn1 alors $b^{1/p} \in K$ (remarque 6.3.3).
Dans ce cas $\alpha = 0$, $ba^{\alpha} \in K^{*p}$ et $t_1 \equiv n_1\alpha[p]$.

- Supposons $pt t_1$ alors $\xi_1^{1/p} \in K_1(b^{1/p})$

ceci entraîne que $K_1(\xi_1^{1/p}) \subset K_1(b^{1/p})$.
Les degrés de $K_1(\xi_1^{1/p})/K_1$ et de $K_1(b^{1/p})/K_1$ ne peuvent prendre que les valeurs 1 ou p (corollaire 3.6), compte tenu de l'inclusion on a 2 possibilités.

1) $[K_1(\xi_1^{1/p}):K_1] = 1$.

2) $[K_1(\xi_1^{1/p}):K_1] = [K_1(b^{1/p}):K_1] = p$ et dans ce cas

$K_1(\xi_1^{1/p}) = K_1(b^{1/p})$.

Etudions ces deux cas :

1°) $[K_1(\xi_1^{1/p}):K_1] = 1$ entraîne que $[K(a_1^{1/pn_1}):K] = n_1$

Or $[K(a_1^{1/pn_1}):K] = [K(a_1^{1/pn_1}):K(a_1^{1/p})].[K(a_1^{1/p}):K]$

donc $[K(a_1^{1/p}):K]$ divise $[K(a_1^{1/pn_1}):K] = n_1$

et puisque $p\nmid n_1$ et $K(a_1^{1/p})/K$ est de degré 1 ou p alors

$[K(a_1^{1/p}):K] = 1$ ou encore $a_1^{1/p} \in K$.

Or par hypothèse $a_1^{1/p} \notin K$, donc cette possibilité ne peut avoir lieu.

2°) $K_1(\xi_1^{1/p}) = K_1(b^{1/p})$.

Ceci entraîne que $b^{1/p} \in K_1(\xi_1^{1/p}) = K(a_1^{1/pn_1})$

$b^{1/p} \in K(a_1^{1/pn_1})$ entraîne (lemme 6.3.2) que $K(b^{1/p}) = K(a_1^{1/p})$.

Puisque $[K_1(b^{1/p}):K_1] = p$.

$b^{1/p} = K(a_1^{1/p})$ entraîne qu'il existe α entier, $0 \leq \alpha < p$, tel que

$ba_1^{\alpha} = \gamma^p$ pour $\gamma \in K^*$.

$ba_1^{\alpha} = \gamma^p$, $\gamma \in K^*$ entraîne $b\xi_1^{n_1\alpha} = \gamma^p$

d'où si $t_1 \equiv n_1\alpha[p]$ alors $b\xi_1^{t_1} \in K_1^{*p}$

□

Remarque

$a = b\xi_1^{t_1} \in K_1^{*p}$ entraîne donc :

si $p\mid n_1$ alors p/t_1 et $\exists$ α entier, $0 \leq \alpha < p$ tel que $ba_1^{\alpha} \in K^{*p}$.

si $p\nmid n_1$ alors $\exists$ α entier, $0 \leq \alpha < p$ tel que $ba_1^{\alpha} \in K^{*p}$ et $t_1 \equiv n_1\alpha[p]$.

En fait dans ce cas $(p,n_1) = 1$ et d'après l'identité de Bezout il existe 2 entiers k_p et k_{n_1} tels que $k_p.p+k_{n_1}.n_1 = 1$.

D'où $t_1 = k_p t_1.p+k_{n_1}.t_1.n_1$

et alors $t_1 \equiv k_{n_1}.t_1.n_1[p]$.

Puisque $0 \leq \alpha < p$, $t_1 \equiv n_1\alpha\ [p]$ et ptn1 alors α est le reste de la division de $k_{n_1}.t_1$ par p.

Algorithme

Soit à étudier le radical $\xi = \sqrt[n]{a}$, $a \in K_1 = K_0(\xi_1)$, n entier avec

1) $\xi_1 = \sqrt[n_1]{a_1}$ et $[K_1 : K_0] = n_1$.

2) a est de la forme $a = b\xi_1^{t_1}$ ou $b = \xi_0^{t_0}\xi_0'^{t_0'} q_1^{s_1}\ldots q_\ell^{s_\ell}$

a_1 " $a_1 = \xi_0^{t_{01}}\xi_0'^{t_{01}'} q_1^{s_{11}} \ldots q_\ell^{s_{1\ell}}$

On peut écrire a et a_1 dans le tableau suivant :

	ξ_0	ξ_0'	q_1	$\cdots$	q_ℓ	ξ_1
a_1	t_{01}	t_{01}'	s_{11}	$\cdots$	$s_{1\ell}$	0
a	t_0	t_0'	s_1	$\cdots$	s_ℓ	t_1

Posons $S : \begin{bmatrix} t_{01} & t_{01}' & s_{11} & \cdots & s_{1\ell} & 0 \\ t_0 & t_0' & s_1 & \cdots & s_\ell & t_1 \end{bmatrix}$ et S/ξ_1 : S privé de la colonne ξ_1.

Le théorème de Capelli pour $K_1(\xi)/K_1$ s'énonce :

$[K_1(\xi) : K_1] < n \iff \nexists\, p$: premier pln et $a \in K_1^{*p}$.

On a deux cas :

* $\underline{p|n_1}$ alors $p|t_1$ et $S^T/\xi_1\binom{\alpha}{1} \equiv 0[p]$ a une solution α .

* $\underline{p\nmid n_1}$ alors $S^T/\xi_1\binom{k_{n_1}.t_1}{1} \equiv 0[p]$.

où k_{n_1} est défini par l'identité de Bezout pour (p,n_1)
$(k_{n_1}.n_1+k_p.p=1)$.

Algorithme 3 : Redradk1

Entrée : a_1, n_1 , a_1 donné par le tableau $(t_{o1}, t'_{o1}, s_{11}, \ldots, s_{1\ell})$

a, n, a donné par le tableau $(t_o, t'_o, s_1, \ldots, s_\ell, t_1)$

Sortie : a,n tels que a donné par le tableau $(t_o, r'_o, s_1, \ldots, s_\ell, t_1)$ et $[K_1(\xi):K_1] = n$.

1- Pour p=2 jusqu'à n faire

1.1 tant que $p|n$ et p premier faire

1.1.1 si $p|n_1$ alors

si p t_1 et $S^T/\xi_1(\alpha_1) \equiv 0[p]$ a une solution α alors

- calculer γ (tel que $ba_1^\alpha = \gamma^p$)

- faire $n \leftarrow n/p$, $t_1 \leftarrow \frac{t_1 - n_1\alpha}{p}$, $b \leftarrow \gamma$.

sinon $p \leftarrow p+1$.

sinon trouver k_{n_1} , k_p tels que $k_{n_1}.n_1 + k_p.p = 1$

si $S^T/\xi_1, \begin{pmatrix} k_{n_1} t_1 \\ 1 \end{pmatrix} \equiv 0[p]$ alors

- calculer γ (tel que $ba_1^{k_{n_1} t_1} = \gamma^p$).

- faire $n \leftarrow n/p$, $b \leftarrow \gamma$, $t_1 \leftarrow k_p.t_1$

sinon $p \leftarrow p+1$.

2- retourner (a,n).

Explication sur l'algorithme

1) si $p|n_1$, $p|t_1$ et si $S^T/\xi_1(\overset{\alpha}{1}) \equiv 0[p]$ a une solution α alors $ba_1^{\alpha} = \gamma^p$

γ se décompose sur $(\xi_0,\xi_0',q_1,\ldots,q_\ell)$.

ce qui entraîne que $b\xi_1^{n_1,\alpha} = \gamma^p$ ou encore $b = [\gamma.\xi_1^{-n_1\ \alpha/p}]^p$ ($\frac{n_1\alpha}{p}$ est entier

d'où $b\xi_1^{t_1} = [\gamma.\xi_1^{\frac{t_1-n_1\alpha}{p}}]^p$.

Donc $a^{1/p} = \mathcal{J}_p.\gamma.\xi_1^{\frac{t_1-n_1\alpha}{p}}$

On montre que $\mathcal{J}_p = 1$ de la même manière que dans la conclusion 6.2.4.

et par suite

$$\xi^{n/p} = \gamma.\xi_1^{(t_1-n_1\alpha)/p}, \quad \gamma \in K_0 \text{ et } \gamma \text{ se décompose sur } (\xi_0,\xi_0'\ q_1,\ldots,q_\ell).$$

On change en $\alpha \leftarrow n/p$, b en γ et t_1 en $(t_1-n_1\alpha)/p$ on est dans une situation analogue au départ.

2) Si pXn_1, $k_{n_1}.n_1+k_p.p = 1$ et $S^T/\xi_1\ (\overset{k_{n_1}.t_1}{1}) \equiv 0[p]$.

alors $b.a_1^{k_{n_1}.t_1} = \gamma^p$, γ se décompose sur $(\xi_0,\xi_0',q_1,\ldots,q_\ell)$, ce qui entraîne que

$$b\ \xi_1^{t_1} = b\ \xi_1^{k_{n_1}.n_1.t_1}.\ \xi_1^{k_p.p.t_1}$$

$$= b.a_1^{k_{n_1}.t_1}.\ [\xi_1^{k_p.t_1}]^p$$

$$= [\gamma.\xi_1^{k_p.t_1}]^p$$

Donc $a^{1/p} = \gamma.\ \xi_1^{k_p.t_1}$ ($\mathcal{J}_p = 1$ comme pour le premier cas). Par suite

$$\xi^{n/p} = \gamma.\ \xi_1^{k_p.t_1}$$

On change n en n/p, b en γ et t_1 en $k_p.t_1$ et on est dans une situation analogue à celle du départ.

Exemple :

ξ_1 : $n_1 = 4$, $a_1 = -3^2 5^8$, $\ell_1 = 0$.

ξ_2 : $n_2 = 6$, $a_2 = 2.3.5^2$, $\ell_2 = 0$.

. Etude de ξ_1 dans K_0 (Algorithme 1)

$n_1 = 4$, $a_1 = -(3.5^4)^2$

- p=2, on peut réduire $n_1 \leftarrow n_{1/2} = 2$
  $a_1 \leftarrow \xi_0^2.3.5^4$.

- $3.5^4 \notin Q^{*2}$ donc on ne peut plus réduire

.. Etude de ξ_2 dans K_0 (Algorithme 1)

$n_2 = 6$, $a_2 = 2.3.5^2$

- p=2 est le seul diviseur premier de n_2
  $3.5^2 \notin Q^{*2}$ dont on ne peut pas réduire
  D'où $n_2 = 6$, $a_2 = \xi_0'.3.5^2$.

... Etude de ξ_1, ξ_2 dans K_0 (Algorithme 2)

	ξ_0	ξ_0'	3	5
a_1	2	0	1	4
a_2	0	2	1	2

- p=2
  $a_2 = a_1.\xi_0^{-2}\xi_0' 5^{-2}$.
  d'où $n_2 \leftarrow n_2/2 = 3$
  $a_2 \leftarrow \xi_1.\ \xi_0^{-1}\xi_0' 5^{-1}$.

- p=3 $p \mid n_2$ mais $p \nmid n_1$
  Il n'y a pas d'autres diviseurs premiers de n_1 et n_2.

Etude de ξ_2 dans $K_0(\xi_1)$ (Algorithme 3).

	ξ_0	ξ_0'	3	5	ξ_1
a_1	2	0	1	4	
a_2	-1	1	0	-1	1

- p=3 est le seul diviseur premier de n_2.
  p=3, pXn_1 (n_1=2) donc on détermine k_n et k_p par l'identité de Bezout 3-2 = 1 entraîne que $k_n = -1$ et $k_p = 1$.

$$S^T/\xi_1 \begin{pmatrix} k_n t_1 \\ 1 \end{pmatrix} = S^T/\xi_1 \begin{pmatrix} -1 \\ 1 \end{pmatrix} = (-1 \quad 1 \quad -1 \quad -5) \not\equiv 0[3].$$

Nous avons donc $S^T/\xi_1 \begin{pmatrix} k_n t_n \\ 1 \end{pmatrix} \not\equiv 0[3]$ donc on ne peut pas réduire

Et par suite $[K_0(\xi_1)(\xi_2) : K_0(\xi_1)] = n_2$, c'est-à-dire que

$n_2 = 3$, $a_2 = \xi_1 \xi_0^{-1} \xi_0' .5^{-1}$ et $\xi_2^{n_2} = a_2$ est l'écriture réduite de ξ_2 dans $K_0(\xi_1)$.

Conclusion : $[K_0(\xi_1,\xi_2):K_0] = 2.3$

avec $\xi_1^2 = \xi_0^2 .3.5^4$ (dans K_0)

et $\xi_2^3 = \xi_1 . \xi_0^{-1} \xi_0' \, 5^{-1}$ (dans $K_0(\xi_1)$).

Relation sur Q

On obtient $[Q(\xi_1,\xi_2):Q] = 4.3$.
Avec

$$\xi_1^4 = -3^2.5^8 \quad \text{et} \quad \xi_2^3 = \frac{1}{5}\left(\xi_1 - \frac{1}{3.5^4}\,\xi_1\right).$$

VII- CONCLUSION

Nous avons étudié le cas de deux radicaux. On remarque malgré toutes les preuves complexes qu'on a dû faire, l'algorithme proposé est très simple et ne fait intervenir que des calculs de pgcd d'entiers (pour la formation des q_i) et des résolutions de systèmes linéaires sur des corps finis ce qui évite tout problème de croissance (des nombres rencontrés) et de précision.

L'extension à plus de deux radicaux se fait par récurrence en utilisant la proposition 6.3.1. Il n'y a pas de difficulté supplémentaire seulement la notation devient assez obscure.

Nous n'avons pas poussé l'étude de la complexité, mais ceci fera l'objet de notre prochain travail, ainsi que la généralisation à plusieurs radicaux etson implantation.

BIBLIOGRAPHIE

[Cap] A. Capelli 1897, Sulla riduttibilità delle equazioni algelbriche. Nota Prima, Rend. Accad. Sc. fis. Mat, Soc. Napoli (3), 3, pp. 243-252.

[Cav] B.F. Caviness
More on Computing Roots of Integers
SIGSAM Bulletin 9 (1975) 3 pp. 18-20, 229

[Kne] M. Kneser
Lineare Abhängigkeit Von Wurzeln
Acta Arithmetica 26 (1975) pp. 307-308.

[Lan] S. Lang
Algebra
Addison-Wesley Publishing Company, Inc

[Len] A.K. Lenstra
Lattices and factorization of polynomials over algebraic number fields,
Proceedings EUROCAM 82, LNCS, 144 pp. 32-39.

[Mor] L.J. Mordell
On the linear independence of algebraic numbers
J. Math 3 (1953) pp. 625-630.

[Naj] H. Najid-Zejli
Computation in radical extensions
Proceedings EUROSAM 84, LNCS. 174, pp. 115-122.

[Sam] P. Samuel
Theorie algébrique des nombres,
Hermann, 1971.

[Sch] A. Schinzel
On linear dependence of roots
Acta Arithmetica 28 (1975), pp. 161-175.

[Ser] J.A. Serret
Algèbre supérieure
Tome premier
Gauthier Villars et Cie, Editeurs, 1928.

[Tra] M. Trager
Algebraic factoring and rationnel function integration.
Proceedings of the 1976 ACM Symposium on Symbolicand algebraic computation, pp. 219-226.

[Wai] P.J. Weinberger, L.P. Rothschild
Factoring polynomials over algebraic number fields,
ACM Trans. Math. Software 2
(1976) pp. 335-350.

DERNIERE PAGE D'UNE THESE

3È CYCLE, DOCTEUR INGÉNIEUR OU UNIVERSITÉ

Vu les dispositions de l'arrêté du 16 avril 1974,

Vu les rapports de M. ~~J.H. Davenport~~.....

M. J. Della Dora.....

M.me NAJID-ZEJLI.....Hakima..... est autorisée à présenter une thèse en vue de l'obtention du grade de DOCTEUR de 3ème Cycle.. Maths. Appliquées.....

Grenoble, le 13 JUIN 1985

Le Président de l'Université Scientifique et Médicale

M. TANCHE