

GROUPES - CORPS  
et  
THEORIE DE GALOIS  
résumés des TP

D. Guin et Th. Hausberger

mars 2008

**Table des matières**

<b>1</b>	<b>TP.I. ÉTUDE DE QUELQUES GROUPES DE PERMUTATIONS</b>	<b>2</b>
<b>2</b>	<b>TP.II. CLASSES, STRUCTURE QUOTIENT ET SYSTÈMES GÉNÉRATEURS FORTS</b>	<b>2</b>
<b>3</b>	<b>TP.IV.A. GÉNÉRATEURS ET RELATIONS, AUTOUR DE L'ALGORITHME DE TODD-COXETER</b>	<b>2</b>
<b>4</b>	<b>TP.IV.B. ACTIONS PLURI-TRANSITIVES, FORMULE DE BURNSIDE ET ÉNUMÉRATIONS DE POLYA</b>	<b>3</b>
<b>5</b>	<b>TP.VI.A. ALGORITHMES DE GAUSS-JORDAN, DE HERMITE ET DE SMITH</b>	<b>3</b>
<b>6</b>	<b>TP.VI.B. COURBES ELLIPTIQUES ET GROUPE DE MORDELL</b>	<b>4</b>
<b>7</b>	<b>TP.VIII. ENTIERS DE GAUSS ET SOMMES DE DEUX CARRÉS</b>	<b>4</b>
<b>8</b>	<b>TP.IX.A. FACTORISATION DES POLYNÔMES</b>	<b>5</b>
<b>9</b>	<b>TP.IX.B. LES QUATERNIONS DE HAMILTON</b>	<b>5</b>
<b>10</b>	<b>TP.XI. NOMBRES ALGÈBRIQUES ET POLYNÔME MINIMAL</b>	<b>6</b>
<b>11</b>	<b>TP.XII. CALCULS DANS LES CORPS DE NOMBRES</b>	<b>6</b>
<b>12</b>	<b>TP.XIV. AUTOUR DE LA CORRESPONDANCE DE GALOIS</b>	<b>6</b>
<b>13</b>	<b>TP.XV. RACINES DE L'UNITÉ DANS UN CORPS FINI ET CODES BCH</b>	<b>7</b>
<b>14</b>	<b>TP.XVI. THÉORIE DE GALOIS CONSTRUCTIVE</b>	<b>7</b>

## 1 TPI. ÉTUDE DE QUELQUES GROUPES DE PERMUTATIONS

Dans ce TP, on se propose de manipuler avec MAPLE quelques groupes de permutations, c'est-à-dire des sous-groupes du groupe symétrique  $S_n$ , pour différents entiers  $n$ . D'après le théorème de Cayley, tout groupe peut être vu comme un groupe de permutations, d'où l'importance de ces derniers. C'est l'occasion d'étudier la structure de groupe (la définition par des générateurs, le calcul du centre, de l'ordre des éléments) et d'appréhender sans formalisme la notion de présentation par générateurs et relations (qui sera étudiée en détail au TP.IV.A). En particulier, on s'intéressera aux deux groupes non abéliens d'ordre 8 : le groupe  $D_4$  des isométries du carré et le groupe quaternionique  $\mathcal{H}$ .

## 2 TP.II. CLASSES, STRUCTURE QUOTIENT ET SYSTÈMES GÉNÉRATEURS FORTS

On poursuit dans ce TP l'étude des groupes de permutations, autour des notions de classes et de quotient. On liste les classes de conjugaison, ce qui est l'occasion de discuter « l'équation aux classes » pour la conjugaison (voir le corollaire 2.8 du chapitre IV pour une version plus générale), puis les classes à gauche et à droite modulo un sous groupe afin d'illustrer la notion de sous-groupe distingué. En particulier, on regarde le quotient de  $S_4$  par le groupe de Klein  $V_4$ , quotient isomorphe à  $S_3$ . Pour finir, on répond au problème du calcul effectif de l'ordre et des éléments d'un groupe de permutations  $G$  défini par un système de générateurs, ainsi que du test d'appartenance à  $G$  d'un élément donné : quels algorithmes se cachent derrière les commandes `grouporder`, `elements` et `groupmember` de MAPLE, qui sont vraisemblablement plus performants que les algorithmes naïfs vus dans le cadre du TP.I?

## 3 TP.IV.A. GÉNÉRATEURS ET RELATIONS, AUTOUR DE L'ALGORITHME DE TODD-COXETER

Les groupes définis par générateurs et relations constituent, avec les groupes de permutations, les deux principaux types de groupes pour lesquels MAPLE offre des commandes avancées dédiées à leur manipulation.

Si les groupes de permutations sont définis par des générateurs, les relations sont entièrement régies par la multiplication des cycles ; de plus, l'unicité de la décomposition en cycles définit un élément de façon univoque. Dans le cas des groupes présentés par générateurs et relations se posent des problèmes de « combinatoire des mots » : à supposer que le groupe soit fini, comment savoir si l'on a écrit tous les mots (et être sûr que ces mots correspondent à des éléments distincts modulo les relations) ?

Un des principaux algorithmes est dû à Todd et Coxeter : il permet, disposant d'une présentation de  $G$  et d'un sous-groupe  $H$  d'indice fini  $n$  (défini par des générateurs exprimés comme des mots en les générateurs de  $G$ ), de donner un système de représentants des classes modulo  $H$ .

Dans le cas où  $G$  est un groupe fini, en prenant  $H = \{\text{Id}\}$ , on obtient en particulier les éléments de  $G$ .

De plus, l'algorithme nous fournit un morphisme  $\rho : G \rightarrow \text{Aut}(G/H) \simeq S_n$  qui traduit l'action de  $G$  par translation sur les classes  $G/H$ . C'est d'ailleurs cette action qui est à la base de l'algorithme, d'où le choix de différer ce TP en fin de chapitre IV. On obtient ainsi, si  $\rho$  est injectif, une réalisation de  $G$  comme un groupe de permutations.

Les objectifs de ce TP sont multiples : d'une part, on apprend à manipuler les groupes définis par générateurs et relations (calcul du cardinal, du moins si ce dernier est fini, *etc.*) et fournit des présentations de quelques groupes usuels intéressants (par exemple le groupe des isométries directes du carré et celui du tétraèdre, isomorphes à  $S_4$  et  $A_4$  respectivement). On utilise MAPLE pour vérifier que l'on a bien obtenu toutes les relations, point difficile qu'il est fastidieux de réaliser à la main. D'autre part, c'est l'occasion, via l'algorithme de Todd-Coxeter, d'étudier l'opération de  $G$  sur  $G/H$  par translation. Apparaissent également, parmi les exemples choisis, plusieurs produits semi-directs.

#### 4 TP.IV.B. ACTIONS PLURI-TRANSITIVES, FORMULE DE BURNSIDE ET ÉNUMÉRATIONS DE POLYA

Ce TP fait suite au TP.II et termine l'étude des groupes de permutations. Un tel groupe de permutations  $G$ , de degré  $n$ , agit naturellement sur  $X_n = \{1, \dots, n\}$ . On en détermine les orbites et teste la transitivité de l'action pour différents groupes. Puis on généralise à l'action diagonale sur  $X_n^k$  afin de discuter la  $k$ -transitivité. Des limitations dues aux temps de calcul apparaissent rapidement et sont contournées par l'usage de la formule de Burnside. Cela permet de regarder des groupes de plus haut degré et, en particulier, de mentionner les fameux groupes de Mathieu. Pour finir, on procède à quelques dénombrements dits « de Polya », la formule d'énumération de Polya étant basée sur une généralisation de la formule de Burnside.

#### 5 TP.VI.A. ALGORITHMES DE GAUSS-JORDAN, DE HERMITE ET DE SMITH

On se propose de passer en revue quelques algorithmes classiques de manipulation des matrices à coefficients dans  $\mathbb{Z}$ . Les résultats obtenus sont à interpréter dans le cadre de la théorie des groupes abéliens de type fini ou, de manière équivalente, des  $\mathbb{Z}$ -modules de type fini.

On rappelle pour commencer l'algorithme de Gauss-Jordan, qui s'applique aux matrices à coefficients dans  $\mathbb{Q}$ , puis on modifie cet algorithme en n'autorisant que des opérations « réversibles » dans  $\mathbb{Z}$  et en utilisant notamment la structure *euclidienne* de  $\mathbb{Z}$  (c'est-à-dire l'existence d'une division euclidienne des entiers). Cela permet de répondre de manière effective à des problèmes pratiques d'algèbre linéaire (résolution d'équations linéaires, extraction d'une base à partir d'un système générateur, comparaison de sous-espaces vectoriels, recherche d'une base du noyau et de l'image d'une application linéaire donnée) et de voir comment ces méthodes se transposent au cas des  $\mathbb{Z}$ -modules. Enfin, l'algorithme de Smith est appliqué au calcul des facteurs invariants (voir également TR VI.C). Cela constitue une preuve algorithmique du théorème de structure des groupes abéliens de type fini.

## 6 TP.VI.B. COURBES ELLIPTIQUES ET GROUPE DE MORDELL

Les courbes elliptiques sont des objets mathématiques très riches à la fois du point de vue théorique (ils interviennent dans la preuve du fameux théorème de Fermat) et des applications pratiques (factorisation des entiers, cryptographie,...). De plus, ces objets se prêtent aux calculs.

Nous allons, dans ce TP, nous intéresser au groupe de Mordell  $E(\mathbb{Q})$  des points rationnels d'une courbe elliptique définie sur  $\mathbb{Q}$ . C'est un groupe abélien de type fini dont il est aisé de calculer, grâce au théorème de Nagell-Lutz, la partie de torsion  $E(\mathbb{Q})_{tors}$ . C'est l'occasion d'illustrer par des exemples (guère accessibles à la main) des énoncés célèbres. Enfin, on s'intéressera au problème des nombres congruents (ce sont les entiers s'interprétant comme l'aire d'un triangle rectangle dont les trois côtés sont rationnels), qui, de manière assez inattendue a priori, est relié au calcul du rang du groupe  $E(\mathbb{Q})$  pour certaines courbes elliptiques.

## 7 TP.VIII. ENTIERS DE GAUSS ET SOMMES DE DEUX CARRÉS

Les anneaux des entiers des corps de nombres constituent, avec les anneaux de polynômes, les deux grands types d'anneaux qui intéressent particulièrement les arithméticiens. Un exemple est l'anneau  $\mathbb{Z}[i] \subset \mathbb{C}$  des entiers de Gauss, constitué des nombres complexes à coordonnées entières. Son corps des fractions est  $\mathbb{Q}(i) \subset \mathbb{C}$ , qui est le  $\mathbb{Q}$ -espace vectoriel de base  $\{1, i\}$ , et  $\mathbb{Z}[i]$  joue pour le corps de nombres  $\mathbb{Q}(i)$  le même rôle que joue  $\mathbb{Z}$  pour  $\mathbb{Q}$ . Pour déterminer les inversibles de l'anneau  $\mathbb{Z}[i]$ , on introduit la norme  $N$  définie par  $N(a + ib) = a^2 + b^2$ . C'est aussi le produit  $z\bar{z}$ , où  $z = a + ib$ , d'où résulte la multiplicativité de la norme :  $N(zz') = N(z)N(z')$ . Il est alors facile de voir que les unités sont  $\mathbb{U}(\mathbb{Z}[i]) = \{z, N(z) = 1\} = \{\pm 1\}$ .

Dans  $\mathbb{Q}[x]$ , étant donné deux polynômes  $f$  et  $g$  non nuls, il existe un unique couple  $(q, r)$  de polynômes tels que  $f = gq + r$ . L'existence de cette division euclidienne implique la primalité de  $\mathbb{Q}[x]$ . Nous allons voir que  $\mathbb{Z}[i]$  possède également un algorithme euclidien, d'où résultent les propriétés arithmétiques de l'anneau. Il est alors possible de décomposer tout élément de  $\mathbb{Z}[i]$  en produit d'irréductibles et cette décomposition est unique (à permutation près des facteurs) si l'on choisit un système de représentants des irréductibles (modulo les inversibles).

L'anneau  $\mathbb{Z}$  est un sous-anneau de  $\mathbb{Z}[i]$  et l'on peut se demander quand est-ce qu'un irréductible de  $\mathbb{Z}$  reste irréductible dans  $\mathbb{Z}[i]$  ou, au contraire, se décompose : par exemple,  $5 = 2^2 + 1^2 = (2 + i)(2 - i)$ . La décomposition d'un nombre premier de  $\mathbb{Z}$  est liée à son écriture en somme de deux carrés :

**Proposition 1.** *Si  $p$  est un nombre premier vérifiant  $p \equiv 1 \pmod{4}$  ou  $p = 2$  alors il existe des entiers naturels  $x$  et  $y$  tels que  $p = x^2 + y^2 = (x + iy)(x - iy)$ . Si par contre  $p \equiv -1 \pmod{4}$  alors  $p$  reste irréductible dans  $\mathbb{Z}[i]$  et cette équation n'admet pas de solution en entiers.*

On en déduit facilement :

**Proposition 2.** *Les irréductibles de  $\mathbb{Z}[i]$  sont les nombres premiers  $p$  tels que  $p \equiv -1 \pmod{4}$  et les éléments de norme première.*

(Décomposer  $N(z) \in \mathbb{N}$  en irréductibles). Il en résulte également :

**Théorème 1.** *Un entier naturel  $n$  est somme de deux carrés d'entiers naturels si et seulement l'exposant de  $p$  dans la décomposition en produit d'irréductibles dans  $\mathbb{Z}$  est pair pour tout nombre premier  $p \equiv -1 \pmod{4}$ .*

Vous verrez par contre au cours du TR IX.B que tout nombre entier naturel est somme de quatre carrés d'entiers naturels (théorème obtenu en travaillant dans l'anneau non commutatif des quaternions de Hurwitz).

Le but de ce TP est de donner une preuve constructive de la première assertion de la proposition 1 et d'écrire la décomposition en irréductibles sur quelques exemples (le cas général pouvant bien sûr être implémenté en machine par un étudiant qui est à l'aise avec la programmation en MAPLE). On implémentera un algorithme efficace qui fournit une écriture  $p = x^2 + y^2$  et est particulièrement intéressant compte tenu des notions algébriques utilisées.

## 8 TP.IX.A. FACTORISATION DES POLYNÔMES

Vous avez étudié au sein des TR VIII.A et VIII.B des critères permettant de vérifier l'irréductibilité de polynômes. Si ces derniers permettent de traiter des cas de degré arbitrairement grand, ils ne s'appliquent cependant pas à n'importe quel polynôme que l'on se donne explicitement. Par contre, MAPLE sait factoriser dans  $\mathbb{Q}[x]$  (commande `factor` ou `factors`, selon l'affichage souhaité) tout polynôme, pourvu que le degré ne soit pas tel que l'on dépasse les capacités de la machine. Le but de ce TP est de comprendre et de réimplémenter l'algorithme qui se cache derrière la commande MAPLE (ou du moins un algorithme efficace qui réalise la factorisation).

Quitte à multiplier par un entier suffisamment grand, on peut toujours supposer que le polynôme  $P$  appartient à  $\mathbb{Z}[x]$ . On peut alors réduire  $P$  modulo un nombre premier  $p$  et se poser la question de la factorisation du polynôme  $\bar{P}$  obtenu dans  $\mathbb{F}_p[x]$  (où  $\mathbb{F}_p$  désigne le corps fini  $\mathbb{Z}/p\mathbb{Z}$ ). La commande MAPLE correspondante est `Factor(P) mod p` (ou `Factors(P) mod p`). Nous allons décrire un algorithme de factorisation sur un corps fini, dû à Berlekamp, qui utilise essentiellement de l'algèbre linéaire et le morphisme de Frobenius (*cf.* TR.IX.A). Pour simplifier, nous nous limiterons à  $\mathbb{F}_p$ . Signalons également qu'il existe d'autres algorithmes (Cantor-Zassenhaus, *etc.*); le lecteur trouvera dans [G-G] une description de ces derniers et une comparaison de leur efficacité en fonction des différents paramètres du problème.

L'algorithme de factorisation sur  $\mathbb{Q}$  que nous décrirons est de nature « modulaire » : on factorise  $\bar{P}$  sur  $\mathbb{F}_p$  et l'on reconstruit les facteurs de  $P$  dans  $\mathbb{Z}[x]$  à partir des facteurs de  $\bar{P}$ . C'est possible grâce à une borne a priori  $M$  des coefficients des diviseurs de  $P$  (borne de Mignotte); on prend alors  $p > 2M$ . Nous nous limiterons au cas d'un seul grand nombre premier. Il existe d'autres variantes : par exemple, prendre un petit premier  $p$  et un entier  $n$  tel  $p^n > 2M$ . On relève alors la factorisation dans  $\mathbb{F}_p$  en une décomposition dans  $\mathbb{Z}/p^n\mathbb{Z}$  grâce au « lemme de Hensel ». Le lecteur intéressé trouvera dans [G-G] chapitre 15 une description de cette seconde méthode modulaire, ainsi qu'une discussion de la pertinence des deux méthodes en fonction des paramètres du problème.

## 9 TP.IX.B. LES QUATERNIONS DE HAMILTON

Ce TP propose une construction géométrique du corps (non commutatif)  $\mathcal{H}$  des quaternions de Hamilton. On y étudie la structure algébrique de  $\mathcal{H}$ , puis l'on interprète géométriquement

quement l'action de  $\mathcal{H}^\times$  par automorphisme intérieur sur  $\mathcal{H}$ . Il en résulte un isomorphisme entre  $\text{SO}_3(\mathbb{R})$  et le quotient  $\mathcal{H}^\times/\mathbb{R}^\times$ . Cela permet d'interpréter algébriquement la composition de deux rotations de l'espace, de manière similaire au cas de la dimension 2, où il est bien connu que la composition de rotations correspond au produit de nombres complexes de norme 1. Telle était d'ailleurs l'une des motivations à l'introduction des quaternions par Hamilton.

Ce TP reprend et complète une partie des notions rencontrées au cours du TR.IX.B : on regarde les coordonnées cartésiennes comme des variables formelles et donne des preuves analytiques formelles de certains résultats démontrés au papier-crayon dans le thème de réflexion (notamment l'associativité du produit des quaternions et la description des automorphismes intérieurs comme rotations de l'espace  $E$ ). Une telle méthode, sans l'aide de l'ordinateur pour effectuer les calculs, serait fastidieuse. Cependant, MAPLE travaillant dans des corps de fractions rationnelles, il s'agit d'être rigoureux lorsque l'on évalue en des réels donnés.

## 10 TP.XI. NOMBRES ALGÈBRIQUES ET POLYNÔME MINIMAL

On se propose de manipuler, avec MAPLE, les nombres algébriques (c'est-à-dire les nombres complexes définis comme zéros  $a$  de polynômes  $P$  de  $\mathbb{Q}[x]$ , ou, de façon équivalente, de  $\mathbb{Z}[x]$ ). On travaille donc dans des corps de nombres  $\mathbb{Q}(a) \simeq \mathbb{Q}[x]/(P)$  (on suppose  $P$  irréductible). On va voir comment définir en MAPLE de telles extensions et calculer dans  $\mathbb{Q}(a)$ .

L'un des problèmes est de trouver le polynôme minimal de  $b \in \mathbb{Q}(a)$ . L'ingrédient essentiel est le résultant, qui permet de calculer la *norme* d'un polynôme de  $\mathbb{Q}(a)[x]$  (voir plus loin). En effet, la norme de  $x - b$  est liée au « polynôme caractéristique » de  $b$ , donc au polynôme minimal. Nous étudierons en détail le résultant puis la norme, qui est cruciale également dans l'algorithme de factorisation d'un polynôme sur un corps de nombres. Ainsi MAPLE est-il capable de factoriser un polynôme  $Q$  de  $\mathbb{Q}[x]$  sur  $\mathbb{Q}(a)$ . Bien entendu, on utilise la factorisation sur  $\mathbb{Q}$  (algorithme décrit au TP.IX.A). Nous donnons pour finir quelques applications.

## 11 TP.XII. CALCULS DANS LES CORPS DE NOMBRES

Ce TP fait suite au TP.XI et poursuit l'étude des corps de nombres, c'est-à-dire des extensions finies de  $\mathbb{Q}$ . On commence par illustrer la notion de corps de rupture et de corps de décomposition, puis on s'intéresse à des extensions  $\mathbb{Q}(a, b)$ . Par exemple, comment trouver le polynôme minimal de  $b + \lambda a$ ,  $\lambda \in \mathbb{Q}$ , à partir des polynômes minimaux de  $a$  et  $b$ ? On y répond en utilisant la norme, dont il a été question au sein du TP.XI. Cela permet de donner un algorithme de détermination d'un élément primitif de l'extension  $\mathbb{Q}(a, b)/\mathbb{Q}$ . Pour finir, on démontre certaines identités algébriques remarquables dues à Ramanujan, en calculant dans des corps de nombres.

## 12 TP.XIV. AUTOUR DE LA CORRESPONDANCE DE GALOIS

Le but de ce TP est de calculer les sous-corps d'une extension  $\mathbb{Q}(a)/\mathbb{Q}$  définie comme corps de rupture d'un polynôme irréductible  $P$ . Lorsque ce dernier est normal, c'est-à-dire lorsque  $\mathbb{Q}(a)$  est corps de décomposition de  $P$  et l'extension  $\mathbb{Q}(a)/\mathbb{Q}$  galoisienne, il est facile de calculer

le groupe de Galois  $G = Gal(P) = Gal(\mathbb{Q}(a)/\mathbb{Q})$  comme groupe de permutations des racines qui sont des polynômes en  $a$ . On utilise alors la correspondance de Galois pour déterminer les sous-corps maximaux de  $\mathbb{Q}(a)$  : il suffit de calculer les invariants sous un élément de  $G$  en résolvant un système linéaire.

Par contre, lorsque  $P$  n'est pas normal, il est beaucoup plus difficile de calculer le groupe de Galois (voir TP XVI) et l'extension  $\mathbb{Q}(a)/\mathbb{Q}$  n'est plus galoisienne. On va déterminer les sous-corps sans calculer  $Gal(P)$ , la correspondance de Galois étant cependant toujours en filigrane, quitte à passer à la clôture galoisienne. On a besoin pour cela de savoir décrire une intersection  $\mathbb{Q}(a) \cap \mathbb{Q}(b)$  de deux corps de nombres. En résolvant algorithmiquement ce problème, on parvient à décrire les sous-corps maximaux, donc tous les corps intermédiaires, quitte à réitérer le processus.

### 13 TP.XV. RACINES DE L'UNITÉ DANS UN CORPS FINI ET CODES BCH

On se propose, dans ce TP, de passer en revue la théorie des polynômes cyclotomiques sur un corps fini  $\mathbb{F}_q$ . Comme application, on génère des codes *BCH* construits, par définition, à partir des polynômes minimaux de puissances de racines primitives de l'unité sur  $\mathbb{F}_q$ . Puis l'on offre une initiation à la théorie des codes correcteurs d'erreurs : on expose comment coder et décoder un message dans le cas des codes *BCH*, (ne pas confondre avec la cryptographie dont le propos est d'envoyer un message secret que seul le destinataire puisse décoder) et l'on teste expérimentalement la capacité de correction du code et la puissance de l'algorithme de décodage (une variante de l'algorithme d'Euclide étendu, due à Berlekamp et Massey). Ces méthodes sont fondamentales dans les technologies de transmission de l'information, d'où de multiples applications dans l'industrie.

### 14 TP.XVI. THÉORIE DE GALOIS CONSTRUCTIVE

Le but de ce TP est d'aborder des aspects effectifs de la théorie de Galois des corps de nombres tout en manipulant et en illustrant la théorie. En effet, puisque MAPLE parvient à calculer les groupes de Galois des polynômes  $P \in \mathbb{Z}[x]$  de petits degrés, quels sont les algorithmes que cachent la commande `galois` ?

Nous allons voir que les ingrédients sont de deux types : d'une part, on réduit  $P$  modulo différents nombres premiers  $p$  et l'on exploite l'information dont on dispose sur  $Gal(\bar{P})$ . MAPLE prédit alors de quel groupe il s'agit : il utilise pour cela un théorème remarquable de Chebotarev qui constitue une méthode « probabiliste » de calcul du groupe de Galois. D'autre part, on calcule des « résolvantes », ces dernières remontant aux travaux de Lagrange (voir également le TR.XVI.A). Nous formaliserons la théorie générale des résolvantes, ce qui nous amènera entre autres, lors de l'implémentation, à écrire un programme exprimant un polynôme en  $n$  indéterminées invariant sous l'action de  $S_n$  comme polynôme en les fonctions symétriques élémentaires.

Pour finir, mentionnons que nos calculs fournissent des réponses partielles au problème de galois inverse, c'est-à-dire celui de savoir si tout groupe fini est (isomorphe au) groupe de Galois d'un polynôme à coefficients rationnels. En se restreignant aux polynômes irréductibles, cela revient à se demander si tout sous-groupe transitif (voir ci-dessous) du groupe symétrique  $S_n$  est groupe de Galois d'un polynôme de degré  $n$ . C'est vrai jusqu'à  $n = 7$  d'après nos calculs.

A la connaissance des auteurs, la réponse est encore positive jusqu'à  $n = 18$ , la vérification nécessitant l'élaboration d'algorithmes plus sophistiqués que les nôtres. Nous nous heurtons en effet très tôt aux limitations liées à la puissance de calcul des machines, ce qui nous oblige déjà à recourir, par exemple pour le calcul des résolvantes, à des méthodes numériques d'approximation des racines complexes de  $P$ .

## Références

- [Art] **M. ARTIN**, Algebra, Prentice-Hall, 1991.
- [CCS] **A.M.COHEN, H.CUYPERS, H.STERK**, Some Tapas of Computer Algebra. Algorithms and Computation in Mathematics, vol. 4. Springer, 1999.
- [Co] **H. COHEN**, A course in Computational Algebraic Number Theory. GTM, vol. 138. Springer, 1993.
- [G-G] **J. von zur GATHEN, J. GERHARD**, Modern Computer Algebra. Second edition. Cambridge, 2003.
- [Ko] **N. KOBLITZ**, Introduction to Elliptic Curves and modular Forms. GTM 97. Springer, 1984.
- [KS] **D.L. KREHER, D. STINSON**, Combinatorial algorithms : generation, enumeration and search. Discrete Mathematics and Its Applications, vol. 11. CRC Press, 1998.
- [L-S] **H. W. LENSTRA, P. STEVENHAGEN**, Chebotarev and his density theorem. The Math. Intelligencer, vol. 18 (1996), 26-36.
- [M] **M. MIGNOTTE**, Mathématiques pour le calcul formel. PUF, 1989.
- [PR] **B. PERRIN-RIOU**, Algèbre, Arithmétique et MAPLE. Cassini, 2000.
- [Sa] **P. SAMUEL**, Théorie algébrique des nombres. Hermann, 1997.
- [S-T] **J. H. SILVERMAN, J. TATE**, Rational Points on Elliptic Curves. UTM. Springer, 1992.