7

Autour des nombres et fonctions algébriques en Maple

Marc Rybowicz
Université de Limoges

[résumé par François Morain]

La simplification d'expressions algébriques contenant des radicaux est une tâche assez ardue, encore mal algorithmisée. Par exemple, en MAPLE, il est facile de trouver les racines d'un polynôme du troisième degré en utilisant les formules de Cardan :

```
    |\^/|      MAPLE V
._|\|   |/|_.  Copyright (c) 1981-1990 by the University of Waterloo.
 \  MAPLE  /   All rights reserved.  MAPLE is a registered trademark of
 <____ ____>   Waterloo Maple Software.
      |        Type ? for help.
> p:=x^3+x+1;
                                   3
                            p := x  + x + 1

> solve(");
                                                    1/2
          %2 + %1, - 1/2 %2 - 1/2 %1 + 1/2 3    (%2 - %1) I,

                                        1/2
              - 1/2 %2 - 1/2 %1 - 1/2 3    (%2 - %1) I

                                      1/2  1/2 1/3
%1 :=                 (- 1/2 - 1/18 31    3   )

                                      1/2  1/2 1/3
%2 :=                 (- 1/2 + 1/18 31    3   )
```

Par contre, si l'on veut vérifier que ce sont vraiment les racines de `p`, il faut substituer ces valeurs dans `p` et simplifier les expressions obtenues. Dans l'état actuel (MAPLE V), il est impossible de montrer que les expressions obtenues sont nulles, d'une façon algébrique. Bien sûr, une évaluation flottante est possible et confirme la validité des formules.
Cet exposé se propose de passer en revue quelques méthodes de simplification de radicaux et de préciser l'implantation de celles-ci dans la procédure `radnormal` de MAPLE, réalisée par l'auteur.

1 Présentation du problème

Soit k un corps de nombres et α_1, α_2, ..., α_n des éléments de k, r_1, r_2, ..., r_n des entiers naturels. On pose

$$K = k(\alpha_1^{1/r_1}, \alpha_2^{1/r_2}, \ldots, \alpha_n^{1/r_n}).$$

Le problème qui se pose est de déterminer le degré de l'extension $[K : k]$ et/ou de calculer une base de K/k.
Les premiers à aborder ce problème ont été Caviness et Fateman [2], puis Zippel [3]. Borodin *et al.* ont étudié la simplification d'expressions faisant intervenir des racines carrées [1].

2 Quelques méthodes de résolution

2.1 Une méthode brutale

Cette méthode consiste à factoriser $X_1^{r_1} - \alpha_1$, à choisir un facteur P_1, puis à factoriser $X_2^{r_2} - \alpha_2$ sur $k[X_1]/(P_1)$, etc. A la fin du processus, on a construit

$$K \simeq k[X_1, X_2, \ldots, X_n]/(P_1 P_2 \ldots P_n) = \{X_1^{e_1} X_2^{e_2} \ldots X_n^{e_n}, 0 \leq e_i < \deg(P_i)\}$$

Considérons par exemple le cas :

$$k = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{-5}),$$
$$\alpha_1 = 1 + \sqrt{-5}, \quad \alpha_2 = 1 - \sqrt{-5},$$
$$\beta_1 = \sqrt{\alpha_1}, \quad \beta_2 = \sqrt{\alpha_2},$$
$$K = k(\beta_1, \beta_2).$$

On cherche à déterminer le degré de $[K : k]$. MAPLE met 10 secondes pour trouver que $X^2 - \alpha_1$ est irréductible sur k. On doit maintenant essayer de factoriser $X^2 - \alpha_2$ sur $k(\beta_1)$. Après 880 secondes, MAPLE retourne deux facteurs linéaires. On en déduit que $[K : k] = 2$.

```
# definition de k
> k:={RootOf(_Z^2-2), RootOf(_Z^2-3), RootOf(_Z^2+5)}:
> alpha1:=1+RootOf(_Z^2+5):
> alpha2:=1-RootOf(_Z^2+5):
# factorisation de X^2-alpha1
> evala(Factor(X^2-alpha1, k));
                              2                 2
                             X  - 1 - RootOf(_Z  + 5)
# kbeta1:=(beta1)
> kbeta1:=k union {RootOf(_Z^2-alpha1)}:
# factorisation de X^2-alpha2
> evala(Factor(X^2-alpha2, kbeta1));
   (X - 1/6 %3 %4 %2 %1 + 1/6 %4 %2 %1) (X + 1/6 %3 %4 %2 %1 - 1/6 %4 %2 %1)

                                        2
%1:=                           RootOf(_Z  - 2)

                                        2
%2:=                           RootOf(_Z  - 3)

                                        2
%3:=                           RootOf(_Z  + 5)

                                      2
%4:=                        RootOf(_Z  - 1 - %3)
```

2.2 L'algorithme de Zippel

Cet algorithme suppose deux choses [3] : la première que les entiers r_i sont tous égaux à r, et deuxièmement que le corps k contient les racines r-ièmes de l'unité.
On pose

$$\Delta = \{\alpha_1^{e_1}\alpha_2^{e_2}\dots\alpha_n^{e_n}, 0 \le e_i < r\},$$
$$k^{*r} = \{a^r, a \in k^*\},$$

et

$$\Delta k^{*r} = \{a^r b, a \in k^*, b \in \Delta\}.$$

Alors, on a le résultat suivant :

Théorème. (Kummer; Artin et Tate, 1968) Le groupe de Galois $\mathrm{Gal}(K/k)$ est isomorphe à $\Delta k^{*r}/k^{*r}$, et par suite $[K : k] = (\Delta k^{*r} : k^{*r})$.

Nous renvoyons le lecteur à [3] pour l'algorithme de calcul de $\Delta k^{*r}/k^{*r}$. On ne sait pas à l'heure actuelle comment se passer de la deuxième hypothèse de Zippel.
Reprenons l'exemple précédent. On part de

$$\Delta_1 = \{1, \alpha_1, \alpha_2, \alpha_1\alpha_2\}.$$

MAPLE a besoin de 10 secondes pour montrer que $X^2 - \alpha_1$ et $X^2 - \alpha_2$ sont irréductibles sur k, c'est-à-dire que ni α_1, ni α_2 ne sont des carrés parfaits dans k. Par contre, $X^2 - \alpha_1\alpha_2 = X^2 - 6$ a deux facteurs linéaires sur k (après 22 secondes de calcul) et donc $\alpha_1\alpha_2$ est un carré dans k. On traduit cela par les relations $\alpha_1\alpha_2 \simeq 1 \bmod k^{*2}$, $\alpha_2^2 \simeq 1$ et par suite, $\alpha_1 \simeq \alpha_2$. On en déduit que

$$\Delta k^{*2}/k^{*2} = \{1, \alpha_1\}.$$

Et par suite, $[K : k] = 2$.

2.3 Implantation en MAPLE

L'auteur a implanté l'algorithme de Zippel; la fonction de simplification s'appelle `radnormal`. Remarquons au passage que l'on est amené à faire des choix de stratégie dans l'élaboration des tours de corps (cas de plusieurs extensions imbriquées). Il semble qu'en pratique, il vaut mieux faire un "grand" nombre de factorisations dans un "petit" corps, qu'une seule factorisation dans un "grand" corps.
Si l'on revient à l'exemple cité dans l'introduction, MAPLE, via la procédure `radnormal`, met maintenant 3 secondes à vérifier que les expressions obtenues par les formules de Cardan sont bien des racines de `p`.

Références

[1] A. Borodin, R. Fagin, J. E. Hopcroft, and M. Tompa. Decreasing the nesting depth of expressions involving square roots. *Journal of Symbolic Computation*, 1:169–188, 1985.

[2] B. F. Caviness and R. J. Fateman. Simplification of radical expressions. In *Proceedings of the 1976 ACM Symposium on Symbolic and Algebraic Computation*, pages 329–338, 1976.

[3] R. Zippel. Simplification of expressions involving radicals. *Journal of Symbolic Computation*, 1:189–210, 1985.