Affine Transformations of Algebraic Numbers

D.J. Jeffrey
Ontario Research Centre for Computer Algebra
The University of Western Ontario
London, Ontario, Canada
djeffrey@uwo.ca

Pratibha*
Department of Applied Mathematics
The University of Western Ontario
London, Ontario, Canada
pratibhag@rediffmail.com

K.B. Roach
The Symbolic Computation Group
The University of Waterloo
Waterloo, Ontario, Canada
themission@att.net

ABSTRACT

We consider algebraic numbers de¯ned by univariate polynomials over the rationals. In the syntax of Maple, such numbers are expressed using the `RootOf` function. This paper de¯nes a canonical form for `RootOf` with respect to a±ne transformations. The a±ne shifts of monic irreducible polynomials form a group, and the orbits of the polynomials can be used to de¯ne a canonical form. The canonical form of the polynomials then de¯nes a canonical form for the corresponding algebraic numbers. Reducing any `RootOf` to its canonical form has the advantage that a±ne relations between algebraic numbers are readily identi¯ed. More generally, the reduction minimizes the number of algebraic numbers appearing in a computation, and also allows the Maple indexed `RootOf` to be used more easily.

Categories and Subject Descriptors

G.1.5 [Numerical Analysis]: Roots of Nonlinear Equations | *Polynomials, methods for*

General Terms

Algorithms

Keywords

Algebraic numbers, RootOf, A±ne Transformation

1. INTRODUCTION

We consider univariate polynomials over the ¯eld $\mathbb{Q}$ of rational numbers. When Maple computes the roots of a polynomial $p(x) \in \mathbb{Q}[x]$, it uses the `RootOf` function to represent any algebraic numbers required. Mathematica uses an equivalent construction. `RootOf` has two forms: indexed and

*Present address: Information Technology Development Agency (ITDA), Government of Uttaranchal,272-B, Phase II, Vasant Vihar, DEHRADUN, INDIA 248 006

```
R(Z^5+Z^2+1,index = 1),
R(Z^5+Z^2+1,index = 2),
R(Z^5+Z^2+1,index = 3),
R(Z^5+Z^2+1,index = 4),
R(Z^5+Z^2+1,index = 5),
R(Z^5-10*Z^4+40*Z^3-79*Z^2+76*Z-27,index = 1),
R(Z^5-10*Z^4+40*Z^3-79*Z^2+76*Z-27,index = 2),
R(Z^5-10*Z^4+40*Z^3-79*Z^2+76*Z-27,index = 3),
R(Z^5-10*Z^4+40*Z^3-79*Z^2+76*Z-27,index = 4),
R(Z^5-10*Z^4+40*Z^3-79*Z^2+76*Z-27,index = 5)
```

Table 1: The roots of the polynomial $p(x)$ de¯ned in equation 1 as expressed in `RootOf` notation by Maple 9.5. The function name `RootOf` has been abbreviated to $\mathcal{R}$ to save space.

Maple's `simplify`, `evala`, `evalb` commands cannot verify this. However, ¯nding the limitations of particular Maple commands is not the point (a su±ciently expert user will be able to guide Maple to this simpli¯cation). The point is that working with algebraic numbers is more convenient if they are expressed in a canonical form. Notice that two things must be recognized in the above statement: the relation between the polynomials and the indexing of the roots.

2. AFFINE TRANSFORMATIONS OF ALGEBRAIC NUMBERS

Let $\mathbb{P} \subset \mathbb{Q}[x]$ be the set of monic irreducible polynomials over $\mathbb{Q}$. Further, let $\mathbb{P}_n$ be the set of monic irreducible polynomials of degree n. We consider the algebraic numbers de¯ned by the roots of the elements of $\mathbb{P}$. From the point of view of Maple, this corresponds to using the output of the `factors` command, rather than the `solve` command.

De¯nition 1. For $x \in \mathbb{C}$ and ®;¯ $\in \mathbb{Q}$, an a±ne transformation T

Theorem 3 shows that algebraic numbers are affinely related if their defining polynomials are related by corresponding affine shifts. Consequently it seems that all affine relations can be deduced by considering the orbits of the defining polynomials. There is a difficulty, however. It is possible for affine relations to exist within a `RootOf` set. This corresponds to an affine polynomial shift mapping a polynomial nontrivially onto itself. It is therefore important to decide when this can occur.

T9]T9TD[T/F88.96Tf27.1587TD[90[(Two)-2(a)-34=(38.96Tf175.88089[(¡)]TJ/F118.96Tf7.170TD[(r)]TJ/F58.96Tf6.46

Theorem 4. *Two different roots $r \in \mathbb{Q}$ and $s \in \mathbb{Q}$ of an irreducible polynomial cannot be linearly related over $\mathbb{Q}$ unless $r = T(-1;\beta)s$ for some $\beta \in \mathbb{Q}$.*

Proof. Assume r and s are different roots of an irreducible polynomial $p(x)$ such that $s = T(\alpha;\beta)r$, $\alpha \in \mathbb{Q}$, and $\beta \in \mathbb{Q}$. Let

$$r_n = \alpha^n + \beta \sum_{i=0}^{n-1} \alpha^i$$

for $n \in \mathbb{N}$. Then $r_0 = r$ is a root of p. By lemma 1, if r_n is a root of p, then $r_{n+1} = \alpha r_n + \beta$ is a root of p. So, by induction, r_n is a root of p for all $n \in \mathbb{N}$. Consider the cases $\alpha = 1$ and $\alpha \neq 1$ separately.

Two and s = 138.96Tf175.880TD[(p)]TJ/F580TD[7TD[

If $\alpha = 1$, then $r_n = r + n\beta$ is a root of p for all $n \in \mathbb{N}$. The Fundamental Theorem of Algebra requires $\{r_n \mid n \in N\}$ be a finite set. Since $\alpha \in \mathbb{Q}$, $\alpha \neq 0$, and $\alpha \neq 1$, this implies $\beta = 0$ and $s = r$, a contradiction.

If $\alpha \neq 1$, then

$$r_n = \alpha^n \left(r + \frac{\beta}{\alpha - 1} \right) - \frac{\beta}{\alpha - 1}$$

is a root of p for all $n \in \mathbb{N}$. The Fundamental Theorem of Algebra requires $\{r_n | n \in N\}$ be a finite set. This implies $\alpha = -1$ and $s = -r + \beta$. □

has1,8(ots)-485(118.96Tf-123.0395TD[6TD[(®)/F58.96Tf6.970T8[(=)-284(1,)-29)57-J/F118.3Tf25.60TTD[7TD[

Example. 8.650TD[(9618.6520TD[(¡)]TJ/F118.9-11898Tf5.750TD[3311.)]TJ/F118.3Tf5.220TD[-3311.

and

$$
\begin{aligned}
a_1^n a_2 (b_1^n b_2)^{n-1} &= a_1^n b_1^{n(n-1)} k_2^n c_2 \\
&= a_1 b_1^{n-1} k_2 \;\; ^n c_2
\end{aligned}
$$

implying

$$
[\text{½}_1^n \, \text{½}_2]_n = \frac{|\, a_1 \,|\, b_1^{n-1} k_2}{b_1^n b_2} = \frac{|\, a_1 \,|\, k_2}{b_1 b_2} = |\, \text{½}_1 \,|\, [\text{½}_2]_n \; :
$$

$\square$

(d) $r_{¾+} = r_{¾\times} = r_{¾¾} = r_{¾}$

(e)

Since $\operatorname{csgn}(\sqrt{s_i}) = 1$ for the principal branch of the square

6. CONCLUDING REMARKS

There remain a number of implementation questions. It should be recalled that Maple allows any polynomial to be