

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 defined by univariate polynomials over the rationals. In the syntax of Maple, such numbers are expressed using the `RootOf` function. This paper defines a canonical form for `RootOf` with respect to affine transformations. The affine shifts of monic irreducible polynomials form a group, and the orbits of the polynomials can be used to define a canonical form. The canonical form of the polynomials then defines a canonical form for the corresponding algebraic numbers. Reducing any `RootOf` to its canonical form has the advantage that affine relations between algebraic numbers are readily identified. 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`, Affine Transformation

1. INTRODUCTION

We consider univariate polynomials over the field \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

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to

$R(Z^5+Z^2+1, \text{index} = 1),$
 $R(Z^5+Z^2+1, \text{index} = 2),$
 $R(Z^5+Z^2+1, \text{index} = 3),$
 $R(Z^5+Z^2+1, \text{index} = 4),$
 $R(Z^5+Z^2+1, \text{index} = 5),$
 $R(Z^5-10*Z^4+40*Z^3-79*Z^2+76*Z-27, \text{index} = 1),$
 $R(Z^5-10*Z^4+40*Z^3-79*Z^2+76*Z-27, \text{index} = 2),$
 $R(Z^5-10*Z^4+40*Z^3-79*Z^2+76*Z-27, \text{index} = 3),$
 $R(Z^5-10*Z^4+40*Z^3-79*Z^2+76*Z-27, \text{index} = 4),$
 $R(Z^5-10*Z^4+40*Z^3-79*Z^2+76*Z-27, \text{index} = 5)$

Table 1: The roots of the polynomial $p(x)$ defined 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, finding the limitations of particular Maple commands is not the point (a sufficiently expert user will be able to guide Maple to this simplification). 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 defined 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.

Definition 1. For $x \in \mathbb{C}$ and $\alpha; \beta \in \mathbb{Q}$, an affine transformation T

Theorem 3 shows that algebraic numbers are closely 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.

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 $r = T(-1; \tau)s$ for some $\tau \in \mathbb{Q}$.*

Proof. Assume r and s are different roots of an irreducible polynomial $p(x)$ such that $s = T(\tau; \tau)r$, $\tau \in \mathbb{Q}$, and $\tau \neq 0$. Let

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

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 $r_{n+1} = \tau r_n + 1$ is also a root of p . By induction, r_n is a root of p for all $n \in \mathbb{N}$. Consider the cases $\tau = 1$ and $\tau \neq 1$ separately.

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

If $\tau \neq 1$, then

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

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

Example. $\sqrt{2}$ and $\sqrt{2} + 1$ are roots of the same irreducible polynomial over \mathbb{Q} .

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

$$[k_1^n k_2]_n = \frac{|a_1| b_1^{n-1} k_2}{b_1^n b_2} = \frac{|a_1| k_2}{b_1 b_2} = |k_1| [k_2]_n :$$

□

(d) $r_{\frac{3}{4}+} = r_{\frac{3}{4}\times} = r_{\frac{3}{4}\frac{3}{4}} = r_{\frac{3}{4}}$

(e)

Since $\text{csgn}(\sqrt{s_i}) = 1$ 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