Explicit Constructions in Splitting Fields of Polynomials

Mathias Lederer – Innsbruck (Austria)

Secondo Convegno Italiano di Teoria dei Numeri
Parma, 13–15 Novembre 2003

Let K be a field and $f = Z^n + a_1 Z^{n-1} + \ldots + a_n$ a monic univariate polynomial with coefficients in K, irreducible and separable over K. Let $x = (x_1, \ldots, x_n)$ be the n-tuple of the zeros of f in some field extension of K and $T = (T_1, \ldots, T_n)$ be indeterminates over K. The *relation ideal* I of f is the set of polynomials in $K[T]$ vanishing at x, thus

$$I = \{P \in K[T]; P(x) = 0\} .$$

The importance of the relation ideal lies in the fact that the quotient $K[T]/I$ is isomorphic to the splitting field of f. Thus if we had a Gröbner basis of the relation ideal, we could perform computations in the splitting field of f. In particular we would have a good tool to tackle computations in algebraic number fields.

I will talk about the construction of a Gröbner basis (for the lexicographical ordering of T) of the relation ideal. This Gröbner basis is indeed of the simplest possible shape – it is *triangular*. This means that I is generated by $\widehat{f}_i$, for $i = 1, \ldots, n$, where $\widehat{f}_i$ is a polynomial in $T_1, \ldots, T_i$, monic with regard to T_i. From this it follows that the algorithm for reducing a polynomial in $K[T]$ modulo the ideal I is nothing but the usual euclidean division by $\widehat{f}_n, \ldots, \widehat{f}_1$. The ingredients for my construction are the Galois group of f on the one hand and the zeros of f on the other hand. The formula for the Gröbner basis is a multidimensional version of Lagrange interpolation.

As for polynomials over $\mathbb{Q}$, nowadays it is possible to compute the Galois group for polynomials up to degree 15. However, the situation is not so good for the zeros of such polynomials: We do not have the zeros themselves at hand but only approximations to the zeros. I will discuss the method of p-adic approximation of the zeros. This method serves to determine the Gröbner basis not just approximatively but exactly. I will illustrate the whole process by giving some examples.

As an additional result of my work, I will give a classical theorem of E. Galois an explicit shape. The theorem of Galois is as follows:

> A rational polynomial f of degree p, where p is a prime number, is solvable by radicals if and only if each zero of f can be expressed as a polynomial (with rational coefficients) in any two other zeros.

The theorem does not tell us in which way one zero can be expressed as a polynomial in two other zeros. In fact, this can be achieved just by evaluating $P(x)$, where P is an appropriate generator of the relation ideal I.