ALGEBRAIC EXTENSIONS AND ALGEBRAIC CLOSURE 
IN SCRATCHPAD II

C. Dicrescenzo
TIM3, 46 av. F.-Viallet, F-38031 Grenoble Cedex
D. Duval
Institut Fourier, BP74, F-38402 St-Martin-d’Hères Cedex

Introduction. — Many problems in computer algebra, as well as in high-school exercises, are such that their statement only involves integers but their solution involves complex numbers. For example, the complex numbers \( \sqrt{2} \) and \(-\sqrt{2}\) appear in the solutions of elementary problems in various domains:

- In integration:
  \[
  \int \frac{dx}{x^2 - 2} = \frac{\log(x - \sqrt{2})}{2\sqrt{2}} + \frac{\log(x - (-\sqrt{2}))}{2(-\sqrt{2})}.
  \]

- In linear algebra: the eigenvalues of the matrix \[
  \begin{pmatrix}
    1 & 1 \\
    1 & -1
  \end{pmatrix}
\]
  are \( \sqrt{2} \) and \(-\sqrt{2}\).

- In geometry: the line \( y = x \) intersects the circle \( y^2 + x^2 = 1 \) at the points \( (\sqrt{2}, \sqrt{2}) \) and \((-\sqrt{2}, -\sqrt{2})\).

Of course, more “complicated” complex numbers appear in more complicated examples. But two facts have to be emphasized:

- In general, if a problem is stated over the integers (or over the field \( \mathbb{Q} \) of rational numbers), the complex numbers that appear are algebraic complex numbers, which means that they are roots of some polynomial with rational coefficients, like \( \sqrt{2} \) and \(-\sqrt{2}\) are roots of \( T^2 - 2 \).

- Similar problems appear with base fields different from \( \mathbb{Q} \). For example finite fields, or fields of rational functions over \( \mathbb{Q} \) or over a finite field. The general situation is that a given problem is stated over some “small” field \( \mathbb{K} \), and its solution is expressed in an algebraic closure \( \overline{\mathbb{K}} \) of \( \mathbb{K} \), which means that this solution involves numbers which are roots of polynomials with coefficients in \( \mathbb{K} \).

The aim of this paper is to describe an implementation of an algebraic closure domain constructor in the language Scratchpad II [Je], simply called Scratchpad below. In the first part we analyze the problem, and in the second part we describe a solution based on the D5 system.

This implementation is still in progress. It has been initiated during a stay at I.B.M. Thomas J. Watson Research Center, and we would like to thank everyone in the Scratchpad group for their kind help.
1. Simple algebraic extensions and algebraic closure:

Analysis. —  The preceding examples were too simple to be typical of the way algebraic numbers appear during a given computation. A better example is the computation of the Puiseux expansions of a curve at its singular points:

Let $\Gamma$ be an algebraic plane curve of equation $F(x, y) = 0$ for some bivariate polynomial $F(X, Y)$ with coefficients in $\mathbb{Q}$. Assume that we want to determine all the singular points of $\Gamma$ over the field $\mathbb{C}$ of complex numbers, and all the Puiseux expansions of $\Gamma$ at these points. We shall not define precisely these notions here (see [Wa] for classical definitions, and [Du] for rationality questions). Here, we only have to know that the singular points of $\Gamma$ are in finite number, and that they cancel the derivative $F'_Y$ of $F$ with respect to $Y$. The Puiseux expansions of $\Gamma$ at a point $M_0 = (x_0, y_0)$ of $\Gamma$ are the local parametrizations of the branches of $\Gamma$ at $M_0$ of the form

$$x = x_0 + t^\epsilon, \quad y = y_0 + \sum_{i \geq 1} y_i t^i.$$

Let $D(X)$ denote the discriminant of $F(X, Y)$ with respect to $Y$, so that $D(X)$ is a polynomial in $X$ with coefficients in $\mathbb{Q}$. Then every singular point $M_0 = (x_0, y_0)$ of $\Gamma$ is such that $D(x_0) = 0$, and of course $F(x_0, y_0) = 0$. It follows that $x_0$ is algebraic over $\mathbb{Q}$. Let $\mathbb{Q}(x_0)$ denote the subfield of $\mathbb{C}$ generated by $x_0$ over $\mathbb{Q}$, i.e. the smallest subfield of $\mathbb{C}$ that contains $\mathbb{Q}$ and $x_0$. Then the equality $F(x_0, y_0) = 0$ means that $y_0$ is a root of the univariate polynomial $F(x_0, Y)$ in $Y$ with coefficients in $\mathbb{Q}(x_0)$. It follows that $y_0$ is algebraic over $\mathbb{Q}(x_0)$, and by a classical result of number theory, that $y_0$ is algebraic over $\mathbb{Q}$. The smallest subfield of $\mathbb{C}$ that contains both $x_0$ and $y_0$ is denoted $\mathbb{Q}(x_0, y_0)$. Let $\mathbb{Q}$ denoted the subset of $\mathbb{C}$ made of the complex numbers which are algebraic over $\mathbb{Q}$. Then $\mathbb{Q}$ is a subfield of $\mathbb{C}$, which contains $\mathbb{Q}(x_0, y_0)$.

Now, let us consider a Puiseux expansion of $\Gamma$ at $M_0$, say $x = x_0 + t^\epsilon, \quad y = y_0 + \sum_{i \geq 1} y_i t^i$. It has been proved by I. Newton that there exists an integer $N$ and polynomials $\varphi_i(X, Y, Y_1, \ldots, Y_i)$ for $i = 1$ to $N$, with positive degree in $Y_i$, such that

$$\varphi_i(x_0, y_0, y_1, \ldots, y_i) = 0.$$

This means that each coefficient $y_i$ is algebraic over the field $\mathbb{Q}(x_0, y_0, y_1, \ldots, y_{i-1})$, and thus algebraic over $\mathbb{Q}$. For $i > n$, the $y_i$'s are in the field $\mathbb{Q}(x_0, y_0, y_1, \ldots, y_N)$, so that the tower of fields

$$\mathbb{Q} \subset \mathbb{Q}(x_0) \subset \mathbb{Q}(x_0, y_0) \subset \ldots \subset \mathbb{Q}(x_0, y_0, y_1, \ldots, y_i) \subset \ldots$$

actually is finite.

More generally, let us now consider the following situation: a given computable field $K_0$ is given, and an algebraic closure $\overline{K}$ of $K_0$ is fixed. A tower

$$K_0 \subset K_1 \subset \ldots \subset K_n$$

of subfields of $\overline{K}$ is constructed, such that each $K_i$ (for $1 \leq 1 \leq n$) is a simple algebraic extension of $K_{i-1}$ by a root $\alpha_i$ of a univariate polynomial $P_i$ with coefficients in $K_{i-1}$. It means that $K_i$ is the smallest subfield of $\overline{K}$ which contains $K_{i-1}$ and $\alpha_i$, and is usually denoted $K_i = K_{i-1}(\alpha_i)$. This is the general way algebraic extensions appear in computer algebra.