Computer Algebra
Michael Sagraloff

Summer 2011
To be handed in on May, 24th.
Discussion on May, 25th.

Exercise 6

6.1 Algebraic numbers form a field

An *algebraic number* is a (possibly complex) root of a univariate polynomial with arbitrary integer coefficients. We denote by $\overline{\mathbb{Q}} := \{\alpha \in \mathbb{C} : \text{there is an } f \in \mathbb{Z}[z] \text{ such that } f(\alpha) = 0\}$ the set of all algebraic numbers. For $\alpha \in \overline{\mathbb{Q}}$, a primitive polynomial μ_α in $\mathbb{Z}[z]$ is called a *minimal polynomial* of α if $\mu_\alpha(\alpha) = 0$ and $n = \deg \mu_\alpha$ is minimal for all polynomials with this property. In this situation, n is called the *degree* of α over $\mathbb{Q}$.
In this exercise, we aim to show that $\overline{\mathbb{Q}}$ is a subfield of $\mathbb{C}$ with the usual operations.
In the following considerations, let α, $\beta \in \overline{\mathbb{Q}}$ be two algebraic numbers with defining minimal polynomials μ_α, $\mu_\beta \in \mathbb{Z}[x]$.

1. Determine a minimal polynomial for $\alpha \in \mathbb{Q}$.
2. For $\alpha \in \overline{\mathbb{Q}} \setminus \{0\}$, show that $1/\alpha$ is algebraic as well.
3. For α, $\beta \in \overline{\mathbb{Q}}$, show how to compute the minimal polynomial of $\alpha \pm \beta$ in terms of μ_α and μ_β.
   Hint: Use bivariate polynomials F and G such that $(\alpha \pm \beta, \beta)$ is a simultaneous solution of $F = G = 0$.
4. Determine defining polynomials of $\alpha \cdot \beta$ and α^q for $q \in \mathbb{Q}$.
5. Conclude that the set of algebraic numbers is actually a field with countably infinitely many elements and, thus, a proper subset of $\mathbb{C}$.
6. To compare arbitrary (complex) elements of $\overline{\mathbb{Q}}$ in lexicographical order, it remains to show that both $\operatorname{Re}\alpha$ and $\operatorname{Im}\alpha$ are algebraic. Explain how to compute the corresponding minimal polynomials in terms of μ_α and μ_β.

6.2 An algorithm for computing minimal polynomials

Implement an algorithm to compute the minimal polynomials of

$$\alpha = \left(\frac{\sqrt{3}+\sqrt{2}}{\sqrt{2}+1}\right)^2 + 1 \qquad \text{and} \qquad \beta = \left(\frac{\sqrt[5]{7+\sqrt{3}}}{\sqrt{2}+\sqrt{3}} - 5\right)^3 + (\sqrt{11}-3)(\sqrt[4]{2}+2).$$

What are the degrees of α and β?

6.3 The algebraic closure of rational numbers

Now we aim to prove that $\overline{\mathbb{Q}}$ as defined in exercise 6.1 is actually the *algebraic closure* of $\mathbb{Q}$, that is the "smallest" field extension of $\mathbb{Q}$ which is closed under algebraic operations. By *algebraic operations*, we mean the set of the usual field operations $\{+, -, \cdot, /\}$ and, in addition, root extraction of arbitrary polynomials over $\overline{\mathbb{Q}}$. In particular, this implies that $\sqrt[n]{\alpha} \in \overline{\mathbb{Q}}$ for arbitrary $\alpha \in \overline{\mathbb{Q}}$ and $n \in \mathbb{N}$.
Given a set of $n+1$ algebraic numbers $\alpha_0, \alpha_1, \dots \alpha_n \in \overline{\mathbb{Q}}$ with corresponding minimal polynomials μ_i, show that the roots of the polynomial equation

$$0 = f(\alpha) = \alpha_n z^n + \alpha_{n-1} z^{n-1} + \cdots + \alpha_1 z + \alpha_0$$

are again algebraic.
Hint: Consider f as an $n+2$-variate polynomial in $\mathbb{Z}[x, \alpha_0, \dots, \alpha_n]$.

6.4 Shearing to generic position

A (square-free) polynomial $f \in \mathbb{Z}[x, y]$ defines an algebraic plane curve by its vanishing set $\mathcal{V}_f := \{(x, y) \in \mathbb{C}^2 : f(x, y) = 0\}$. We call a point $p \in \mathcal{V}_f$ on f *singular* if $f(p) = f_x(p) = f_y(p) = 0$, where $f_x = \frac{\partial}{\partial x} f$ and $f_y = \frac{\partial}{\partial y} f$ denote the partial derivatives with respect to x and y.

1. Prove: If $\mathrm{Res}^{(y)}(f, f_x)$ and $\mathrm{Res}^{(y)}(f, f_y)$ do not share a common root, then V_f has no singularity.

   Does the converse hold as well? Explain in geometrical terms!

2. A point $p = (p_x, p_y)$ on $\mathcal{V}_f$ is called *x-critical* if $f(p_x, p_y) = f_y(p_x, p_y) = 0$. Accordingly, a *fiber* $\mathcal{V}_f \cap (\{x_0\} \times \mathbb{C})$ of $\mathcal{V}_f$ at x_0 is called *x-critical* if it contains an x-critical point of f.

   Geometrically interpret the notion of an x-critical point, and explain the shape of the curve between two consecutive x-critical fibers.

3. A *shear* of f with the shear factor $s \in \mathbb{Z}$ is the polynomial

   $$\mathrm{Sh}_s\, f := f(x + s\, y, y).$$

   Geometrically explain the relation between $\mathcal{V}_f$ and $\mathcal{V}_{\mathrm{Sh}\, f}$.

4. Covertical x-critical points impose problems for several algorithms computing the topology of an algebraic curve. By shearing, we can always ensure to remedy this situation. However, what is the flaw of the following simple "proof:"

   > Due to *Bézout's theorem* (or, alternatively, the finite degree of the resultants in x- and y-direction), the number of x-critical points on $\mathcal{V}_f$ is bounded in the degree of f. Thus, only finitely many combinations of x-coordinates of the x-critical values are possible, and, hence, only finitely many shear factors leave fibers with covertical x-critical points.

Have fun with the solution!