Math 461 F — Spring 2011
Quadratic Field Extensions — Drew Armstrong

Let F be a field and let $c \in F$ be an element such that $\sqrt{c} \notin F$. (This notation means that the equation $x^2 - c = 0$ has no solution in F.) In this case we can define a new, bigger number system

$$F[\sqrt{c}] := \{a + b\sqrt{c} : a, b \in F\},$$

which we call "F adjoin $\sqrt{c}$". We have already seen an important example of this. The complex numbers are just the same as $\mathbb{R}$ adjoin $\sqrt{-1}$:

$$\mathbb{C} = \mathbb{R}[\sqrt{-1}] = \left\{a + b\sqrt{-1} : a, b \in \mathbb{R}\right\}.$$

You will agree by now that the complex numbers have remarkable and beautiful properties. So perhaps the same is true of $F[\sqrt{c}]$? Yes.

First note that we can **divide** in $F[\sqrt{c}]$. Given $a + b\sqrt{c} \in F[\sqrt{c}]$ we have

$$\begin{aligned}
\frac{1}{a + b\sqrt{c}} &= \frac{1}{a + b\sqrt{c}} \cdot \frac{a - b\sqrt{c}}{a - b\sqrt{c}} \\
&= \frac{a - b\sqrt{c}}{a^2 - cb^2} \\
&= \left(\frac{a}{a^2 - cb^2}\right) + \left(\frac{-b}{a^2 - cb^2}\right)\sqrt{c},
\end{aligned}$$

which is again in $F[\sqrt{c}]$. We can multiply, add, and subtract elements of $F[\sqrt{c}]$ in the obvious way. Hence $F[\sqrt{c}]$ is itself a field. We will call the pair $F \subseteq F[\sqrt{c}]$ a quadratic field extension.

In the above proof we used the high-school technique of "rationalizing the denominator". More formally, we define a conjugation map $F[\sqrt{c}] \to F[\sqrt{c}]$ by

$$\overline{a + b\sqrt{c}} := a - b\sqrt{c}.$$

Just like complex conjugation, the map $v \mapsto \bar{v}$ preserves addition and multiplication. Please check that for all $u, v \in F[\sqrt{c}]$ we have

- $\overline{u + v} = \bar{u} + \bar{v}$, and
- $\overline{uv} = \bar{u}\bar{v}$.

(We say that $v \mapsto \bar{v}$ is an automorphism of the field $F[\sqrt{c}]$.)

Finally, we note that $F[\sqrt{c}]$ is (just like the complex numbers) really a two-dimensional vector space. Suppose that $a + b\sqrt{c}$ and $a' + b'\sqrt{c}$ are in $F[\sqrt{c}]$ with $a + b\sqrt{c} = a' + b'\sqrt{c}$. Then we have

$$a - a' = (b' - b)\sqrt{c}.$$

If $b \neq b'$ then we can divide both sides by $b' - b$ to get

$$\sqrt{c} = \frac{a - a'}{b' - b} \in F,$$

which is a contradiction because we assumed that $\sqrt{c}$ is **not** in F. Hence $b = b'$ and consequently $a = a'$. That is, the element $a + b\sqrt{c}$ acts very much like a vector (a, b) with two coordinates. We could say that $F[\sqrt{c}]$ is isomorphic to the "F-plane" F^2.

Why did I bring this up now? Because quadratic extensions give us the correct way to discuss constructibility.

Fact. The real number α is constructible with straightedge and compass if and only if there exists a chain of quadratic extensions

$$\mathbb{Q} = F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_r \subseteq \cdots \subseteq \mathbb{R}$$

such that $\alpha \in F_r$. Let's say that $F_{k+1} = \{a + b\sqrt{c_k} : a, b \in F_k\}$, where $c_k \in F_k$ is some element such that $\sqrt{c_k} \notin F_k$. (We will assume that $c_k > 0$ so that we always stay in $\mathbb{R}$.) In general, the elements of F_k have more "nested" square root brackets as k gets larger.

This interpretation immediately allows us to prove that $\sqrt[3]{2}$ is **not** constructible with straightedge and compass. Hence the ancient problem of "doubling the cube" is impossible. This result was (apparently) first proved by Descartes.

Theorem. The real cube root of 2 is not constructible.

Proof. Suppose (for contradiction) that $\sqrt[3]{2}$ is constructible. Then there exists a chain of quadratic extensions

$$\mathbb{Q} = F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq \mathbb{R}$$

such that $\sqrt[3]{2}$ is in F_i for some i. Let F_{k+1} be the **minimum** F_i which contains $\sqrt[3]{2}$. (You will show on the homework that $k + 1 \geq 1$.) Thus $\sqrt[3]{2}$ is in $F_{k+1} = F_k[\sqrt{c_k}]$, but **not** in F_k, and we can write $\sqrt[3]{2} = a + b\sqrt{c_k}$ for some $a, b \in F_k$ with $b \neq 0$ (why?). Observe that

$$(a + b\sqrt{c_k})^3 - 2 = 0.$$

Now consider the conjugation map for the quadratic extension $F_k \subseteq F_{k+1}$ and apply this to both sides of the equation to get

$$\begin{aligned} \overline{(a + b\sqrt{c_k})^3 - 2} &= \overline{0} \\ \left(\overline{a + b\sqrt{c_k}}\right)^3 - \overline{2} &= \overline{0} \\ (a - b\sqrt{c_k})^3 - 2 &= 0. \end{aligned}$$

In other words, $a - b\sqrt{c_k}$ is also a real cube root of 2. Since there is only one real cube root of 2 (why?), we must have $a + b\sqrt{c_k} = a - b\sqrt{c_k}$, which implies that $b = -b$, or $b = 0$. This is a contradiction. $\square$