Abstract Algebra B (Math 521B)
Michael E. O'Sullivan

Notes of field extension
Thursday, April 30, 2009

Let's start with a very fundamental result about polynomial rings.

Theorem 1. *Let $\phi : R \longrightarrow S$ be a homomorphism of rings and let $s \in S$. There is a unique homomorphism of rings $\tilde{\phi} : R[x] \longrightarrow S$ which extends ϕ and takes x to s. The homomorphism is defined by*

$$\tilde{\phi}(\sum_i r_i x^i) = \sum_i \phi(r_i) s^i$$

I won't prove this here, but notice the following: (1) the constants in $R[x]$ form a subring which is isomorphic to R. When we say $\tilde{\phi}$ extends ϕ we just mean that $\tilde{\phi}(r) = \phi(r)$ for r a constant polynomial. (2) Since $\tilde{\phi}$ is a homomorphism, and we want $\tilde{\phi}(x) = s$ the only possibility for the definition of $\tilde{\phi}$ is the one given above. (3) The proof of the theorem just boils down to justifying that this definition does indeed give a homomorphism.

We are interested in the case where R is a field, which we call F, and S is a bigger field containing F. That is, we have F a subfield of K and $\alpha \in K$. We let $F(\alpha)$ be the smallest field containing F and α (this plays the role of S). The theorem above says that there is a homomorphism $\tilde{\phi} : F[x] \longrightarrow F(\alpha)$ that is the identity on F and takes x to α.

$$\tilde{\phi}(\sum_i f_i x^i) = \sum_i f_i \alpha^i$$

In particular the image of $\tilde{\phi}$ is $\tilde{\phi}(F[x]) \subseteq F(\alpha)$. Now apply The First Isomorphism Theorem, Theorem 6.13: $\tilde{\phi}$ is a surjective homomorphism onto its image $\tilde{\phi}(F[x])$, so

$$F[x] \Big/ p(x) \cong \tilde{\phi}(F[x])$$

where $p(x)$ is the minimal polynomial of α. We've shown that $p(x)$ is irreducible, so $F[x]/p(x)$ is a field. Thus $\tilde{\phi}(F[x])$ is also a field contained in $F(\alpha)$. But, by definition, $F(\alpha)$ is the smallest field containing F and α. Thus $F(\alpha) = \tilde{\phi}(F[x])$ and this is isomorphic to $F[x]/p(x)$. Thus we have the theorem.

Theorem 2. *Let F be a subfield of K. Let $\alpha \in K$ be algebraic over F with minimal polynomial $p(x)$. Then $F(\alpha) \cong F[x]/p(x)$.*

This has some consequences that are not obvious. Let $\omega = \frac{-1+\sqrt{3}i}{2}$ and note that ω is a cube root of 1. We see that $\sqrt[3]{2}$ and $\sqrt[3]{2}\omega$ are both cube roots of 2, so they have the same minimal polynomial, $x^3 - 2$. Therefore the fields $Q(\sqrt[3]{2})$ and $Q(\sqrt[3]{2}\omega)$ are isomorphic. Both are isomorphic to $Q[x]/\langle x^3 - 2\rangle$. This is a bit surprising, since $Q(\sqrt[3]{2})$ is contained in the Real numbers and $Q(\sqrt[3]{2}\omega)$ is not.

The assignment also includes a problem on splitting fields.

Given an irreducible polynomial, $p(x) \in F[x]$ we can create a new field $F(\alpha)$, which has a root of $p(x)$. We make the extension field $F[x]/p(x)$ and we denote the class of x by α. As we discussed in class, there is some abuse of notation. We continue to think about x as an indeterminate in the polynomial ring $F(\alpha)[x]$. Then $p(x)$ now has a root, namely α. Let us continue this process with an irreducible factor of $p(x)$. Make a new field in which this factor has a root. Continue this process until $p(x)$ factors completely. The field you arrive at is called a splitting field for $p(x)$. We are going to skip over the technical theory, but the main result is easy to understand. For any $p(x) \in F[x]$, there is an extension field of F in which $p(x)$ factors into linear factors. Any two fields in which this happens (and which are as small as possible) are isomorphic. This field is called the splitting field of $p(x)$ over F.

As an example, consider $x^3 - 2$. We can form $Q(\sqrt[3]{2})$ and factor

$$x^3 - 2 = (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + \sqrt[3]{4})$$

The roots of the quadratic are $\sqrt[3]{2}\omega$ and $\sqrt[3]{2}\omega^2$. So we have to do another extension to factor $x^3 - 2$ completely. In $Q(\sqrt[3]{2}, \sqrt[3]{2}\omega)$ we have

$$x^3 - 2 = (x - \sqrt[3]{2})(x - \sqrt[3]{2}\omega)(x - \sqrt[3]{2}\omega^2)$$

It is also worth noting that $Q(\sqrt[3]{2}, \sqrt[3]{2}\omega) = Q(\omega, \sqrt[3]{2})$. To show this prove that each contains the other! Notice that we can think about $Q(\omega, \sqrt[3]{2})$ as adjoining a root of $x^3 - 2$ to the field $Q(\omega)$. The field $Q(\omega)$ is built from Q by adjoining a cube root of unity and is isomorphic to $Q[x]/\langle x^2 + x + 1\rangle$.