Abstractly building extension fields.

Kevin Buzzard

November 4, 2013

Here's the idea. If $p(x) \in \mathbf{Q}[x]$ is an irreducible polynomial, it would be nice to have a field K containing a root of $p(x)$; but we have such a field, namely the complex numbers $\mathbf{C}$. In fact $\mathbf{C}$ is rather large, but if $\alpha \in \mathbf{C}$ is a root of $p(x)$ then we could instead use the field $K := \mathbf{Q}(\alpha) \subset \mathbf{C}$.

Proposition 2.4 tells us what K looks like: if $p(x)$ has degree d then $[K : \mathbf{Q}] = d$ and a $\mathbf{Q}$-basis for K is $\{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\}$ (the $\mathbf{Q}$-vector space V spanned by this set has dimension d because $p(x)$ is irreducible and hence is the minimum polynomial for α over $\mathbf{Q}$, and in particular V is finite-dimensional, so by the rank-nullity trick it is a field).

Furthermore, we know how to multiply elements of K together: a general element of K is of the form $\sum_{i=0}^{d-1} \lambda_i \alpha^i$ with $\lambda_i \in \mathbf{Q}$, and if $f(x) \in \mathbf{Q}[x]$ and $g(x) \in \mathbf{Q}[x]$ are polynomials of degree at most $d-1$ then $f(\alpha)g(\alpha)$ can be computed thus: write $f(x)g(x) = q(x)p(x) + r(x)$ with $r(x)$ of degree less than $\deg(p) = d$, and then $f(\alpha)g(\alpha) = r(\alpha)$ because $p(\alpha) = 0$.

The point is this. If now we have a random field E, not contained within the complex numbers, and $p(x) \in E[x]$ irreducible of degree d, then even though we can't choose a root α and form the field $E(\alpha)$, we can still perform the polynomial construction: we quotient out the abelian group $E[t]$ by the subgroup I of polynomials which are multiples of $p(t)$, and this quotient group is naturally a field, it contains a copy of E, and it is an E-vector space of dimension d with basis $1 + I, t + I, \ldots, t^{d-1} + I$. Let's call it F. Furthermore, F contains $t + I$ which is easily checked to be a root of $p(X)$ in F. If you are not sure why any of this is true, you should try and check it yourself because it is all simple algebra. In the language of ring theory, what is happening is that $p(t) \in E[t]$ is irreducible, so the ideal $I = (p(t))$ is prime, so $F := E[t]/I$ is an integral domain, but it's finite-dimensional over a field so it's a field by the rank-nullity trick.

Iterating this procedure, we can even construct abstract splitting fields: the construction above gives us an extension field containing a root of any irreducible polynomial, and you just apply it repeatedly, factoring $p(x)$ in each new field you construct and continuing until all the irreducible factors of $p(x)$ have degree 1.