KMB, 24/3/16

M345P11: Existence of algebraic closure of a field.

Recall that a field L is said to be *algebraically closed* if any non-constant polynomial $f(x) \in L[x]$ has a root in L, that is, there is some $\lambda \in L$ such that $f(\lambda) = 0$. It's easy to check (induction on degree of $f(x)$) that this is equivalent to saying that every non-constant polynomial factors into linear factors in $L[x]$, or equivalently that the irreducible elements of the ring $L[x]$ are the degree 1 polynomials.

Algebraically closed fields are very useful to have around. For example, algebraic geometry is a way to study systems of polynomial equations by looking at their zeros as a geometric object, and of course you're not going to get very far understanding the polynomials $x^{2n} + y^{2n} = -1$ for $n \in \mathbf{Z}_{\geq 1}$ if you just look at their rational or real solutions, because there aren't any – no square of a real number is negative. If you want to see that these polynomials really have different geometry as n varies you must look at the complex solutions. Closer to home, if you want to construct a splitting field for $f(x) \in K[x]$ cheaply (K any field) you could just hope that K is a subfield of an algebraically closed field L and then look at the extension of K generated by the roots of $f(x)$ in L. But do we have a sufficiently rich choice of algebraically closed fields? In particular, if K is any field, does there exist an algebraically closed field L containing K? The answer is yes.

Theorem 1. *If K is any field then there exists an algebraically closed field L and an injective field map $K \to L$. In particular any field K may be thought of as a subfield of an algebraically closed field.*

This theorem has some useful consequences. For example one can check that if K is any field and $K \subseteq L$ with L an algebraically closed field, then the elements of L which are algebraic over K form a subfield $\overline{K}$, which one can check is an *algebraic* extension of K which is algebraically closed. This field $\overline{K}$ is called an *algebraic closure* of K, and one can check that algebraic closures are unique up to (typically non-unique) isomorphism. In some sense $\overline{K}$ is "the smallest algebraically closed field containing K".

I stated the theorem above (existence of algebraically closed field containing a given field) in the course, but I did not prove it, because the proof involves some ring theory and also Zorn's Lemma, which is a kind of transfinite version of induction, and I felt it would take me too far from the course to go through all the details. In fact I thought that the proof of this theorem would be ideal for a hand-out, so here's the hand-out and let's go.

Proof of theorem. We begin with a lemma – this is where we need Zorn's Lemma.

Lemma 2. *If R is a non-zero commutative ring with a 1, then R has a maximal ideal.*

Let S be the set of ideals I of R such that $I \neq R$. Let's partially order S, by defining $I \leq J$ if and only if $I \subseteq J$. This is called a *partial* order because of course we might have ideals I and J with $I \not\subseteq J$ and $J \not\subseteq I$, so our ordering does not order these elements I and J – they are just "incomparable".

What we're looking for is a maximal element of S, that is, an element M of S such that if $I \in S$ and $M \leq I$ then $M = I$. Now we recall (or we look up on Wikipedia)

Zorn's Lemma: If S is any partially ordered set, with the property that any chain in S (that is any subset X of S with the property that for any $x, y \in X$ either $x \leq y$ or $y \leq x$) has an upper bound (that is, an element $b \in S$ such that $x \leq b$ for all $x \in X$), then S has at least one maximal element.

Zorn's Lemma is equivalent to the Axiom of Choice, which is one of the axioms of mathematics, so we can assume it :-)

The proof of our lemma is trivial given Zorn's Lemma – the hypotheses of the lemma are satisfied because if X is a chain in S, then X is a bunch of ideals of R, with the property that if I and J are in X then either $I \subseteq J$ or $J \subseteq I$, and now it's easy to check that the union of

the ideals in X (and also throw in $\{0\}$ if X is empty, he said pedantically) is also an ideal which is clearly an upper bound for X; moreover the union can't be all of R because if it were then it would contain 1, which would mean some ideal in X contained 1, which can't happen because S only contains proper ideals of R.

So by Zorn's Lemma S has a maximal element, which is a maximal ideal of R.

Corollary 3. *If R is a commutative ring with a 1, and $I \subset R$ is an ideal of R such that $I \neq R$, then R has a maximal ideal containing I.*

Proof. Apply the lemma to R/I and then look at the pre-image of the maximal ideal of R/I under the natural map $R \to R/I$. □

Now let's build an algebraically closed field containing a given field K.

First let's construct a polynomial ring $R = K[X_{f_1}, X_{f_2}, ...]$ in infinitely many variables X_{f_i}, where the f_i run over every polynomial in $K[X]$ of positive degree and X_{f_i} is just a variable which is labelled by f_i. Just to be clear – an element of R is a polynomial in only finitely many of the variables X_{f_i}, and with coefficients in K.

Now let I be the ideal of R generated by all the elements $f_i(X_{f_i})$ as the f_i run through all of the polynomials of positive degree. The claim is that $I \neq R$. Why is this? Well, if $I = R$ then $1 \in I$, so one can write

$$1 = \sum_{i=1}^{n} a_i f_i(X_{f_i})$$

for some polynomials $f_i \in K[X]$ of positive degree, and elements $a_i \in A$. Now let M be a splitting field over K for the product of the f_i, $1 \leq i \leq n$, and choose a root α_i for each of these f_i in M. If we now consider the map from R to M sending X_{f_i} to α_i, $1 \leq i \leq n$, and X_f to zero for the other f's, then $f_i(\alpha_i) = 0$ and the equation becomes $1 = 0$, which is nonsense. This proves that $I \neq R$, as claimed.

By the corollary there's a maximal ideal m of R with $I \subseteq m \subset R$. Define $K_1 = R/m$, and note that there's a natural injection $K \to K_1$. Furthermore every polynomial $f(X) \in K[X]$ of degree 1 or more has a root in K_1! Indeed X_f is a root of $f(X)$ in R/I, so its image in K_1 is a root of $f(X)$ in K_1.

It would be great if we were now done. Unfortunately we are not yet there. The problem is that K_1 has the property that every polynomial in $K[X]$ of degree 1 or more has a root – however there may be polynomials of degree 1 or more in the larger ring $K_1[X]$ that do not have roots. Once you realise this you wonder whether we have got anywhere at all!

However the trick is to iterate this construction. If we start with K_1 then we build a field K_2 containing K_1 such that every element of $K_1[X]$ of positive degree has a root in K_2. And so on. We continue, getting an infinite collection of fields $K \subseteq K_1 \subseteq K_2 \subseteq K_3 \subseteq \cdots$. Now, informally, we could just let L be the union of the K_i, and if this made sense (and it nearly does) then L will be algebraically closed, because any $f \in L[X]$ of degree 1 or more will have each coefficient in some K_i, so all coefficients will be in K_N for N large enough, so f has a root in K_{N+1} and hence in L.

However we can't really take a union because really we don't have $K_i \subseteq K_{i+1}$, we just have a natural injection $K_i \to K_{i+1}$, so we need to use a slightly more sophisticated language – we let L be the *colimit* of the K_i, which is something that does make sense: formally L is the disjoint union of the K_i, modulo the equivalence relation generated by saying that $\alpha \in K_i$ is equivalent to its image in K_{i+1}. In other words L is a set of equivalence classes, and a typical equivalence class looks like $\{\alpha_i, \alpha_{i+1}, \alpha_{i+2}, \ldots\}$ with $\alpha_i \in K_i$ and all the α_{i+n}'s are the image of α_i in K_{i+n}.

The field L is the extension of K that we seek. □