First, some definitions I haven’t actually mentioned yet, but which I think you’ve probably already gleaned:

**Definition 0.1.** Let $A$ be a ring. By the center of $A$ we mean the set of elements $a \in A$ such that $ab = ba$ for all $b \in B$.

**Definition 0.2.** Let $R$ be a commutative ring. By an $R$-algebra we mean a ring $A$ equipped with a ring homomorphism $\rho : R \rightarrow A$ whose image is contained in the center of $A$. We often write $r \cdot a$ for $\rho(r)a$, thinking of $\rho$ as providing $A$ with a “scalar” action of $R$.

By a morphism of $R$-algebras $A \rightarrow B$ we mean a ring homomorphism $f : A \rightarrow B$ such that $f(r \cdot a) = r \cdot f(a)$ for all $r \in R$.

By a commutative $R$-algebra we mean an $R$-algebra whose underlying ring is commutative.

**Proposition 0.3.** Let $R$ be a commutative ring. Then a commutative $R$-algebra is the same thing as a commutative ring $S$ together with a ring map $R \rightarrow S$.

**Proof.** The center of a commutative ring is the ring itself. \hfill $\Box$

1. **Algebraic closures.**

Here is a definition you have seen before:

**Definition 1.1.** Let $k$ be a field. We say that $k$ is algebraically closed if every nonconstant polynomial $f(x) \in k[x]$ has a root in $k$.

This has several (easy) equivalent formulations:

**Proposition 1.2.** Let $k$ be a field. The following conditions on $k$ are equivalent:

- $k$ is algebraically closed.
- Each nonconstant polynomial $f(x) \in k[x]$ factors as a product $f(x) = \alpha(x - r_1) \cdots (x - r_n)$ for some nonnegative integer $n$ and some $\alpha, r_1, \ldots, r_n \in k$.
- The irreducible elements in $k[x]$ are exactly the elements of the form $\alpha x + r$ for some $\alpha, r \in k$.

**Proof.** If every nonconstant polynomial $f(x) \in k[x]$ factors completely into linear factors, then clearly every nonconstant polynomial in $f(x)$ has a root in $k$ (just choose $r_i$ from any of the linear factors $x - r_i$). Conversely, if every nonconstant polynomial $f(x) \in k[x]$ has a root $r \in k$, then $x - r$ divides $k[x]$, and the long division algorithm in $k[x]$ (which we can carry out, since $k[x]$ is a principal ideal domain!) then tells us how to write $f(x)$ as $(x - r)f_1(x)$ for some $f_1(x) \in k[x]$. Now either $f_1(x)$ is a constant polynomial, or it has a root itself, and we repeat the process; by downward induction on the degree of $f(x)$, we factor $f(x)$ as the product of linear factors $x - r_i \in k[x]$ and a constant $\alpha \in k$. \hfill $\Box$

*Date: February 2016.*
Definition 1.3. Let $k$ be a field. By an algebraic closure of $k$ we mean any algebraic field extension $K/k$ such that $K$ is algebraically closed.

Theorem 1.4. (Existence of algebraic closures.) Every field has an algebraic closure.

Proof. Let $k$ be a field. Form the polynomial ring

$$k \left[ X_f : f \in k[x], \text{deg } f > 0 \right],$$

a polynomial ring over $k$ with one generator $X_f$ for each nonconstant polynomial $f \in k[x]$. Let $I \subseteq k \left[ X_f : f \in k[x], \text{deg } f > 0 \right]$ be the ideal generated by all the polynomials of the form $f(X_f)$. I claim that $1 \notin I$. Here is a proof by contradiction: suppose that $1 \in I$. Then, by the definition of $I$, there exists a set of elements $f_1, \ldots, f_n \in k[X_f : f \in k[x], \text{deg } f > 0]$ such that

$$g_1 \cdot f_1(X_{f_1}) + \cdots + g_n \cdot f_n(X_{f_n}) = 1.$$

Choose a root $r_i$ of $f_i$ for each $i$, and let $h : k \left[ X_f : f \in k[x], \text{deg } f > 0 \right] \to k$ be the $k$-algebra homomorphism sending $X_{f_i}$ to $r_i$ and sending all the other $X_f$ generators to zero. Then

$$h(g_1 \cdot f_1(X_{f_1}) + \cdots + g_n \cdot f_n(X_{f_n})) = 0 = h(1) = 1,$$

a contradiction.

So $1 \notin I$, so there exists (by Zorn’s Lemma) some maximal ideal $m$ of $k \left[ X_f : f \in k[x], \text{deg } f > 0 \right]$ containing $I$. Write $E_1$ for the quotient ring $k \left[ X_f : f \in k[x], \text{deg } f > 0 \right]/m$. Then $E_1$ is a field since $m$ is a maximal ideal, and we have a ring map $k \to E_1$ by construction, and by construction, every nonconstant polynomial in $k[x]$ has a root in $E_1$. We don’t know that every nonconstant polynomial over $E_1$ has a root in $E_1$, however, only that every nonconstant polynomial in $k$ has a root in $E_1$. So iterate this construction, with $E_1$ in place of $k$, to get a tower of field extensions

$$k = E_0 \subseteq E_1 \subseteq E_2 \subseteq E_3 \subseteq \ldots$$

such that every nonconstant polynomial in $E_n[x]$ has a root in $E_{n+1}$. It is an easy exercise (we have done it in class already) that the union of a tower of field extensions is itself a field, so $E = \cup_{n} E_n$ is a field extension of $k$, and each given element of $E$ is contained in some $E_n$ and hence has a root in $E_{n+1} \subseteq E$. So $E$ is an algebraically closed field extension of $k$.

We still need to know that $k$ has an algebraically closed algebraic field extension, but this part is easier: let $E' \subseteq E$ be the union of all the subfields $F$ of $E$ containing $k$ such that the extension $F/k$ is algebraic. In other words, $E'$ is the collection of all the elements of $E$ which are algebraic over $k$. I claim that $E'$ is a field. The argument is as follows: if $\alpha, \beta \in E$ are algebraic elements, $k(\alpha)$ is a finite extension of $k$, and $k(\alpha, \beta) = k(\alpha)[x]/(\text{Irr}(\beta, k(\alpha), x))$ is a finite extension of $k(x)$ (since it has degree dividing the degree of $\text{Irr}(\beta, k, x)$). So $k(\alpha, \beta)$ is a finite extension of $k$, hence $k(\alpha, \beta)$ is an algebraic extension of $k$, hence every element in $k(\alpha, \beta)$ is the root of some polynomial in $k[x]$. In particular, $\alpha + \beta$ and $\alpha \beta$ and $-\alpha$ and $1/\alpha$ are all roots of polynomials in $k[x]$. So the set of elements of $E$ which are algebraic over $k$ is closed under addition, multiplication, subtraction, and division; so $E'$ is a subfield of $E$.

Now every element of $E'$ is, by construction, algebraic over $k$. So $E'$ is an algebraic field extension of $k$. If $f(x) \in E'[x]$, then $f(x)$ has a root $r \in E$, and that root is clearly algebraic over $E'$; each of the coefficients of $f(x)$ lives in some algebraic extension of $k$, and there
are only finitely many nonzero coefficients of \( f(x) \), so \( f(x) \in F(x) \) for some algebraic field extension \( F/k \), with \( F \subseteq E \). So \( r \) is algebraic over \( F \), and \( F \) is an algebraic extension of \( k \). So \( r \) is algebraic over \( k \), so \( r \in E' \). So every polynomial \( f(x) \in E'[x] \) has a root in \( E' \).

Hence \( E' \) is an algebraic closure of \( k \). \( \square \)

Another important property of algebraic closures: if \( k \) is a field with algebraic closure \( E' \), and \( K \) is an algebraic extension of \( k \), then there is a ring homomorphism from \( K \) to \( E' \) which sends \( k \subseteq K \) to \( k \subseteq E' \) by the identity map. In the case where \( K \) is another algebraic closure of \( k \), this implies that any two algebraic closures of a field are isomorphic.

Consequently we can speak of the algebraic closure of a field \( k \), and this is well-defined up to isomorphism. People often write \( \overline{k} \) for the algebraic closure of a field \( k \).

The fact that algebraic closures exist and have this uniqueness-up-to-isomorphism property is very useful. For example, suppose \( k \) is a field, and we want to speak of \( k(\sqrt{2}) \), without already knowing of some field extension of \( k \) that has a square root of \( 2 \). This is fine, since we know that (unless \( k \) has a square root of \( 2 \) already) the irreducible polynomial of \( \sqrt{2} \) needs to be \( x^2 - 2 \), so we can just form \( k[x]/(x^2 - 2) \), and this is clearly a minimal field extension of \( k \) containing a square root of \( 2 \). But we might find ourselves in situations where this kind of reasoning becomes more and more awkward: for example, suppose we need to study how certain invariants of the field \( k(\zeta_{p^n}) \) change as \( n \) increases. (This idea—studying how fundamental invariants of number fields change in infinite towers of extensions—is basically the idea behind Iwasawa theory, a part of algebraic number theory.) We can iteratively construct \( k(\zeta_{p^{n+1}}) \) as an extension of \( k(\zeta_{p^n}) \), but it is much more convenient to simply have a big (but still algebraic) extension of \( k \) in which all possible roots of unity exist, and then all the extensions \( k(\zeta_{p^n}) \) naturally sit inside this big extension. This is what the algebraic closure \( \overline{k} \) is for!