I.D. Algebraic closures

Recall that any polynomial \( f \in \mathbb{Q}[x] \) splits over \( \mathbb{C} \). Since the roots are algebraic over \( \mathbb{Q} \), they belong to \( \mathbb{Q} \) (cf. I.A.18), hence \( f \) actually splits in \( \overline{\mathbb{Q}}[x] \).

We have shown that every \( f \in K[x] \), for any \( K \), has a splitting field. But is there a field that does for \( K \) what \( \overline{\mathbb{Q}} \) does for \( \mathbb{Q} \) — an algebraic extension that splits every polynomial at once? Indeed there is, and we will construct it.

I.D.1. Definition. (i) \( L \) is algebraically closed if any \( f \in L[x] \) splits over \( L \).
(ii) \( L/K \) is an algebraic closure if \( L/K \) is algebraic and \( L \) is algebraically closed.

I.D.2. Example. \( \mathbb{C}/\mathbb{R} \) is an algebraic closure, but \( \mathbb{C}/\mathbb{Q} \) is not: there are only countably many polynomials over \( \mathbb{Q} \), hence countably many roots of such equations in \( \mathbb{C} \); but \( \mathbb{C} \) is uncountable, and the remaining elements must therefore be transcendental over \( \mathbb{Q} \). Of course, the point is that \( \overline{\mathbb{Q}}/\mathbb{Q} \) is an algebraic closure, and this argument shows that \( \overline{\mathbb{Q}} \subset \mathbb{C} \) is a proper subfield.

I.D.3. Proposition. The following are equivalent:
(i) \( L/K \) is an algebraic closure.
(ii) \( L/K \) is algebraic; and any irreducible \( f \in K[x] \) splits over \( L \).
(iii) \( L/K \) is algebraic; and \( L'/L \) algebraic \( \implies \) \( L' = L \).

Proof. (i) \( \implies \) (ii): clear from the definition.
(ii) \( \implies \) (iii): Given \( L'/L \) algebraic, \( L'/K \) is algebraic. Take \( \alpha' \in L' \) and its (irreducible) minimal polynomial \( m_{\alpha'} \in K[x] \). By (ii), \( m_{\alpha'} = \prod_i(x - \lambda_i) \) splits over \( L \), and so \( \alpha' = \lambda_j \) for some \( j \). That is, \( \alpha' \in L \); conclude that \( L = L' \).
(iii) \( \implies \) (i): Given \( f \in L[x] \), there exists a splitting field extension \( L'/L \). Since this is necessarily algebraic, we have \( L = L' \) by assumption, and \( f \) splits over \( L \). So \( L \) is algebraically closed. \( \square \)
In particular, there are no nontrivial algebraic extensions of fields like \( \mathbb{C} \) and \( \bar{\mathbb{Q}} \):

I.D.4. **Corollary.** If \( L \) is algebraically closed and \( L'/L \) is an algebraic extension, then \( L' = L \).

**Proof.** Take \( K = L \) in I.D.3(i), and conclude (iii). \( \square \)

If you had any lingering doubts about \( \bar{\mathbb{Q}} \) being an algebraic closure of \( \mathbb{Q} \), just take \( L = \mathbb{C} \) and \( K = \mathbb{Q} \) in the following:

I.D.5. **Corollary.** Given an extension \( L/K \), with \( L \) algebraically closed and \( L_0 := L_{\text{alg}}/K \subset L \) the subfield of elements algebraic over \( K \) (as in I.A.17). Then \( L_0 \) is an algebraic closure of \( K \).

**Proof.** Replace “\( L/K \)” in I.D.3(ii) by \( L_0/K \), and conclude (i). \( \square \)

We now formulate the main existence result:

I.D.6. **Theorem.** Any field \( K \) has an algebraic closure \( \bar{K} \).

**Doomed Proof (V. 1.0).** Let

\[
\mathcal{E} := \{ M \text{ field} \mid M \supset K, M/K \text{ algebraic} \},
\]

partially ordered by inclusion. Given a chain \( \mathcal{C} \), consider the set \( \mathcal{M}_C := \bigcup_{M \in \mathcal{C}} M \). If \( \alpha, \beta \in \mathcal{M}_C \), there exists \( M \in \mathcal{C} \) with \( \alpha, \beta \in M \) so that \( \alpha \beta, \alpha^{-1}, \alpha + \beta \in M \); hence \( \mathcal{M}_C \) is a field. Moreover, \( \mathcal{M}_C/K \) is algebraic since any \( \alpha \in \mathcal{M}_C \) is contained in some \( M \) algebraic over \( K \) (\( \alpha \) algebraic). Conclude that \( \mathcal{M}_C \in \mathcal{E} \) gives an upper bound for \( \mathcal{C} \); by Zorn, it follows that \( \mathcal{E} \) has a maximal element \( E \). By “(iii) \( \implies \) (i)” in I.D.3, \( E/K \) is an algebraic closure. \( \square \)

The problem is at the very beginning of the proof: what is meant by “ordered by inclusion”? That would work if all these \( M \)’s are subfields of a larger field — like an algebraic closure. Hmm. Some nice circular reasoning there.

There is a way to fix it by embedding all extensions inside the power set of \( K[x] \times \mathbb{N} \), but I’d rather not; instead, we take a different tack.
PROOF (V. 2.0). Let

\[ S := \{(f, j) \mid f \in K[x] \text{ monic nonconstant}, 1 \leq j \leq \deg(f)\}, \]

and define a corresponding set \( X_S := \{x_j(f) \mid (f, j) \in S\} \) of formal indeterminates. For each monic nonconstant \( f = x^n - a_1(x)x^{n-1} + \cdots + (-1)^n a_n(f) \) (with \( a_i(f) \in K \)), we write formally

\[ \prod_{j=1}^{n}(x - x_j(f)) = x^n - \sigma_1(x)x^{n-1} + \cdots + (-1)^n \sigma_n(x) \in K[X_S][x], \]

where \( \sigma_i(x) := \sum_{j_1 < \cdots < j_i} x_{j_1}(f) \cdots x_{j_i}(f) \) are elementary symmetric polynomials in the indeterminates, and put \( t_i(f) := \sigma_i(f) - a_i(f) \). I claim that the ideal \( I := \langle \{t_i(f)\}_{f,i} \rangle \subset K[X_S] \) is proper.

Suppose (on the contrary) that \( 1 \in I \), i.e. that exist \( r_{\ell} \in K[X_S] \) and \( t_{i_{\ell}}(f_{\ell}) \) such that \( r_{1}t_{i_{1}}(f_{1}) + \cdots + r_{N}t_{i_{N}}(f_{N}) = 1 \). Let \( L/K \) be a splitting field extension for \( f_1 \cdots f_N \), and write (in \( L[x] \))

\[ f_{\ell} = \prod_{j=1}^{d_{\ell}}(x - \alpha_{\ell j}) = x^{d_{\ell}} - a_1(f_{\ell})x^{d_{\ell}-1} + \cdots + (-1)^{d_{\ell}}a_n(f_{\ell}), \]

where the \( a_i(f) \)'s are clearly elementary symmetric polynomials in the \( \alpha_{\ell j} \)'s for each \( \ell \). Consider the evaluation map

\[ \text{ev} : K[X_S] \rightarrow L \]

\[ k \mapsto t(k) \]

\[ x_j(f_{\ell}) \mapsto \alpha_{\ell j} \]

\[ \{\text{other indeterminates in } X_S\} \mapsto 0. \]

We have \( \text{ev}(\sigma_i(f_{\ell})) = a_i(f_{\ell}) \) hence \( \text{ev}(t_i(f_{\ell})) = 0 \) (\( 1 \leq \ell \leq N, 1 \leq i \leq n_{\ell} \)), which gives

\[ 1 = \text{ev}(1) = \text{ev}(r_{1})\text{ev}(t_{i_{1}}(f_{1})) + \cdots + \text{ev}(r_{N})\text{ev}(t_{i_{N}}(f_{N})) = 0, \]

which is absurd. So \( 1 \not\in I \), and \( I \) is proper as claimed.

Recall from [Algebra I] that by Zorn’s Lemma, there exists a maximal proper ideal \( J \) such that \( I \subseteq J \subseteq K[X_S] \). This gives a field \( M := K[X_S]/J \), a quotient map \( q : K[X_S] \rightarrow M \), and (by composing \( q \) with \( K \hookrightarrow K[X_S] \)) an embedding \( j : K \hookrightarrow M \). Notice that
\[ j(a_i(f)) = q(a_i(f)) = q(\sigma_i(f)) \] since \( I \subset J \). I claim that \( M / K \) is an algebraic closure of \( K \). Equivalently, we can show that I.D.3(ii) holds: \( M / K \) is algebraic and splits all of our polynomials \( f \).

For each \((f, j) \in S\), set \( \beta_j(f) := q(x_j(f)) \in M \). We have
\[
\begin{align*}
f &= x^n - a_1(f)x^{n-1} + \cdots + (-1)^n a_n(f) \in K[x] \setminus K \\
\Rightarrow j(f) &= x^n - j(a_1(f))x^{n-1} + \cdots + (-1)^n j(a_n(f)) \in M[x] \\
&= x^n - q(\sigma_1(f))x^{n-1} + \cdots + (-1)^n q(\sigma_n(f)) \\
&= q \left( x^n - \sigma_1(f)x^{n-1} + \cdots + (-1)^n \sigma_n(f) \right) \\
&= q \left( \prod_{j=1}^n (x - \beta_j(f)) \right),
\end{align*}
\]
so \( f \) splits over \( M \). Moreover, since \( K[X_S] \) is generated over \( K \) by the \( x_j(f) \), \( M \) is generated over \( K \) by their images \( \beta_j(f) \); being roots of \( f \) (for various \( f \)'s), these are algebraic over \( j(K) \). By I.A.21, \( M / K \) is algebraic.

\[ \square \]

Turning to the uniqueness of algebraic closures, we first need a

I.D.7. Lemma. Let \( L / K \) be an algebraic extension, and \( K' \) an algebraically closed field. Then any embedding \( i: K \hookrightarrow K' \) extends to \( j: L \hookrightarrow K' \).

Proof. Define a partial order on
\[
S := \left\{ (M, \theta) \mid M \subset L \text{ a subfield containing } K, \text{ and } \theta: M \hookrightarrow K' \text{ an embedding with } \theta|_K = i \right\}
\]
by \((M, \theta) \leq (M', \theta') \iff M \subset M' \text{ and } \theta'|_M = \theta\).

Let \( C \subset S \) be any chain, and put \( N := \bigcup_{(M, \theta) \in C} M \). Each \( n \in N \) belongs to \( M \) for some \((M, \theta) \in C\), and we define a function \( \phi: N \hookrightarrow K' \) by \( \phi(n) := \theta(n) \). This is well-defined (use \( \theta'|_M = \theta \)), injective (otherwise injectivity would fail on some \( M \)), and has an upper bound (namely, \((N, \phi)\)). So Zorn hands us a maximal element \((M, \Theta)\) for \( S \).
Suppose $M \subset L$, and let $\alpha \in L \setminus M$. Clearly $\alpha$ is algebraic over $M$, with minimal polynomial $m_\alpha$; and so $\Theta(m_\alpha) = 0$. Then I.C.14 produces an embedding $\Theta': M(\alpha) \rightarrow K'$ (sending $\alpha \mapsto \beta$) which extends $\Theta$ (hence $i$). This contradicts maximality of $(M, \Theta)$, and we conclude that $M = L$. □

I.D.8. THEOREM. Given $i: K \rightarrow L$ and $i': K \rightarrow L'$ two algebraic closures for $K$. Then there exists an isomorphism $j: L \rightarrow L'$ over $K$ (i.e. such that $j \circ i = i'$).

PROOF. By the Lemma, there exists $j: L \rightarrow L'$ with $j \circ i = i'$. We must show $j$ is onto.

Suppose $f \in K[x]$ is irreducible. Then $i(f)$ splits (over $L$) and so $i'(f) = j(i(f))$ splits (over $j(L)$). Hence $i': K \rightarrow j(L)$ is an algebraic closure for $K$.

Finally, since $L'/K$ is algebraic, so is $L'/j(L)$. By (i) $\implies$ (iii) in I.D.3, $L' = j(L)$ as desired. □

I.D.9. DEFINITION. In view of the uniqueness theorem I.D.8, we shall write $\bar{K}$ for the algebraic closure of $K$.

Note that, as a general rule, $\bar{K}$ has no nontrivial algebraic extensions.

A glance ahead. Here are two key conditions on an algebraic extension $L/K$ which we will take up next.

First, $L/K$ will be called normal if the condition

$f \in K[x]$ irreducible $\implies$ $f$ splits over $L$ or has no roots in $L$

holds. Equivalently, for each $\alpha \in L$ its minimal polynomial $m_\alpha \in K[x]$ splits over $L$. This will link up nicely with our earlier use of “normal”, for groups.

Second, an irreducible polynomial $f \in K[x]$ is separable if it has $\deg(f)$ distinct roots in a splitting field. Accordingly, we call the extension $L/K$ separable if the minimal polynomial $m_\alpha \in K[x]$ of each $\alpha \in L$ is separable. This is not an issue in characteristic zero: everything is separable.
To link with the material we have just covered, there is a notion of *separable algebraic closure*: instead of taking the full \( \bar{K} \), you take only the elements which have separable minimal polynomials. By the previous remark on characteristic zero, this does not affect \( \bar{Q} \).