Algebraic closure

Definition. A field K is called *algebraically closed* if every nonconstant polynomial $f(x) \in K[x]$ has a root in K. Put differently, K is algebraically closed if and only if every polynomial in $K[x]$ factors completely into linear polynomials, that is, if and only if K has no proper algebraic extensions.

Definition. A field extension $\overline{F}$ of F is called an *algebraic closure* if $\overline{F}$ is an algebraic extension of F and $\overline{F}$ is algebraically closed.

Theorem. *Every field F has an algebraic closure $\overline{F}$.*

PROOF. The idea of the proof is simple: consider all fields $(E, +, \cdot)$ which are algebraic extensions of F, find a maximal one among them by Zorn's Lemma, and show that it is algebraically closed by virtue of having no further algebraic extensions.

There are two technical complications. First of all, we have to make sure that all our field extensions E stay within one fixed set Ω. This set Ω will have to be chosen large enough to accommodate at least one copy of every conceivable algebraic extension of F. Secondly, because the same set E of elements can form very different fields $(E, +, \cdot)$ for different binary structures "+" and " $\cdot$ ", we have to make sure that we include all possibilities when considering all algebraic extensions of F.

As far as picking the right size for the set Ω, we start with the set

$$S = \{(k, a_0, a_1, a_2, \cdots, a_n, 0, 0, \cdots) \in \mathbb{N} \times F \times F \times \cdots \mid a_i \in F,\ 1 \leqslant k \leqslant n\}.$$

Any algebraic field extension E of F can have at most as many elements as the set S. (Every $\alpha \in E$ is a root of some polynomial $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \in F[x]$, which has at most n different roots in E.) In order to get even more elements, we take the powerset $\mathscr{P}(S)$ of S and recall that its cardinality satisfies $|\mathscr{P}(S)| > |S|$. Since the function $f : F \to \mathscr{P}(S)$ given by $f(a) = \{(1, a, -1, 0, 0, \cdots)\}$ is injective, we may remove its image $f[F]$ from the set $\mathscr{P}(S)$ and replace it by F itself, so as to form a new set Ω such that $F \subseteq \Omega$ and $|\Omega| > |S|$.

Now, for a given field $(E, +, \cdot)$ with $E \subseteq \Omega$, addition is a function $+ : E \times E \to E$, which is a subset of $(E \times E) \times E \subseteq (\Omega \times \Omega) \times \Omega = \Omega^3$. The same can be said for multiplication. So, we can form the set $\mathscr{E}$ of all algebraic field extensions E of F with $E \subseteq \Omega$ by defining

$$\mathscr{E} = \{(E, +, \cdot) \in \mathscr{P}(\Omega) \times \mathscr{P}(\Omega^3) \times \mathscr{P}(\Omega^3) \mid (E, +, \cdot) \text{ is an algebraic field extension of } F\}.$$

Observe that $\mathscr{E}$ is not empty, because it contains the field F.

We partially order the set $\mathscr{E}$ by declaring $E_1 \preccurlyeq E_2$ if and only if E_2 is a field extension of E_1. Then every chain $\mathscr{C}$ in $\mathscr{E}$ has an upper bound K in $\mathscr{E}$. Indeed, if $\mathscr{C}$ is a nonempty chain in $\mathscr{E}$, we can take $K = \bigcup_{E \in \mathscr{C}} E$ along with binary operations defined as follows. If $\alpha, \beta \in K$, then $\alpha \in E_1$ and $\beta \in E_2$ for some E_1 and E_2 in $\mathscr{C}$. Since $\mathscr{C}$ is a chain, either E_1 is a subfield of E_2 or E_2 is a subfield of E_1. Either way, there is an E in $\mathscr{C}$ with $\alpha, \beta \in E \subseteq K$ and we can define $\alpha + \beta$ and $\alpha \cdot \beta$ as the result of the corresponding operation in the field E. These definitions are independent of the choice of E, for if E' is another element of the chain $\mathscr{C}$ with $\alpha, \beta \in E'$, then either E is a subfield of E' or vice versa. Therefore, $\alpha + \beta$ is the same element in E as it is in E' and hence a well-defined element of K. The same holds for $\alpha \cdot \beta$. Since every calculation in K actually occurs in some field E of $\mathscr{C}$, it follows that these operations turn K itself into a field. In fact, K is an algebraic extension of F, because every element $\alpha \in K$ lies in some algebraic extension $E \in \mathscr{C}$ of F and is therefore algebraic over F. We conclude that $(K, +, \cdot\,) \in \mathscr{E}$ and that $E \preccurlyeq K$ for all E in $\mathscr{C}$.

Zorn's Lemma now guarantees the existence of a maximal element $\overline{F}$ of $\mathscr{E}$. By definition of $\mathscr{E}$, $\overline{F}$ is an algebraic field extension of F and $\overline{F} \subseteq \Omega$. It remains to be shown that $\overline{F}$ is algebraically closed. To this end, let $f(x) \in \overline{F}[x]$ be any nonconstant polynomial and suppose, to the contrary, that $f(x)$ has no root in $\overline{F}$. By Kronecker's Theorem, there is a finite field extension E of $\overline{F}$ and an element $\alpha \in E$ such that $f(\alpha) = 0$. Since E is a finite field extension of $\overline{F}$, E is an algebraic extension of $\overline{F}$. Since $\overline{F}$, in turn, is an algebraic extension of F, E is an algebraic extension of F.

Since $|\overline{F}| \leqslant |E| \leqslant |S| < |\Omega|$, we have $|\Omega| = |\Omega \setminus \overline{F}|$ by the lemma bellow (when applied to the sets $A = \Omega$, $B = \overline{F}$ and $C = \Omega \setminus \overline{F}$). Thus, we have $|E \setminus \overline{F}| \leqslant |E| < |\Omega| = |\Omega \setminus \overline{F}|$, so that there is an injective function $g : E \to \Omega$, which extends the inclusion function $i : \overline{F} \to \Omega$. Transcribing the addition and multiplication tables for the field E to its image $g[E]$ in Ω, while keeping the operations on F as they are, we may assume that $E \subseteq \Omega$ and $E \in \mathscr{E}$, in the first place. Since $f(x)$ has no root in $\overline{F}$, we have that $\alpha \notin \overline{F}$ so that $\overline{F} \subsetneqq E$, contradicting the maximality of $\overline{F}$. □

Lemma. *Let A be an $\underline{\text{infinite}}$ set expressed as $A = B \cup C$ with $B \cap C = \emptyset$. Then*

(1) *either $|B| \leqslant |C|$ or $|C| \leqslant |B|$;*

(2) *if $|B| \leqslant |C|$, then $|B \cup C| = |C|$;*

(3) *if $|C| \leqslant |B|$, then $|B \cup C| = |B|$.*

PROOF. (1) Clearly, we may assume that neither B nor C is empty. Consider the set $\mathscr{D}$ of all pairs (D, f) such that $D \subseteq B$ and $f : D \to C$ is an injective function. Then $\mathscr{D} \neq \emptyset$, since we can always take D to be a one-point subset of B and $f : D \to C$ any function. Partially order $\mathscr{D}$ by declaring $(D_1, f_1) \preccurlyeq (D_2, f_2)$ if and only $D_1 \subseteq D_2$ and $f_2|_{D_1} = f_1$, that is, if f_2 and f_1 agree on D_1. Then every chain $\mathscr{C}$ in $\mathscr{D}$, has an upper bound $(\tilde{D}, \tilde{f})$ for $\mathscr{C}$ in $\mathscr{D}$. We leave it as a straightforward exercise to verify that for a nonempty chain $\mathscr{C}$ in $\mathscr{D}$, one can take $\tilde{D}$ to be the union of all sets D with $(D, f) \in \mathscr{C}$, while defining $\tilde{f} : \tilde{D} \to C$ by $\tilde{f}(x) = f(x)$ when $x \in D$ and $(D, f) \in \mathscr{C}$. By Zorn's Lemma, $\mathscr{D}$ has a maximal element (D, f). Then either $D = B$ or $f[D] = C$, for otherwise we could pick elements $b \in B \setminus D$ and $c \in C \setminus f[D]$ and extend $f : D \to C$ to an injective function $g : D \cup \{b\} \to C$ by defining $g(b) = c$, contradicting the maximality of (D, f). If $D = B$, then $f : B \to C$ is injective so that $|B| \leqslant |C|$. If $f[D] = C$, then the inverse $h : C \to D \subseteq B$ of the bijection $f : D \to C$ is injective so that $|C| \leqslant |B|$.

(2) Suppose $|B| \leqslant |C|$. It will suffice to show that $|C \times \{0, 1\}| = |C|$, because then we have $|C| \leqslant |B \cup C| \leqslant |C \times \{0, 1\}| = |C|$. To this end, form the set $\mathscr{D}$ of all pairs (D, f) such that $D \subseteq C$ and $f : D \times \{0, 1\} \to D$ is a bijective function. Since C must be infinite, we can select a countably infinite subset $D' = \{c_0, c_1, c_2, \cdots\} \subseteq C$. Defining $f' : D' \times \{0, 1\} \to D'$ by the formula $f'(c_n, i) = c_{2n+i}$, we see that $(D', f') \in \mathscr{D}$ so that $\mathscr{D} \neq \emptyset$. As is the proof of (1), we partially order $\mathscr{D}$ by set-containment and function extension, so as to obtain a maximal element (D, f) by Zorn's Lemma. Then $f : D \times \{0, 1\} \to D$ is a bijection and therefore $|D \times \{0, 1\}| = |D|$. We claim that $|D| = |C|$, which will complete the proof. Since C is infinite and since $D \subseteq C$, it suffices to argue that $C \setminus D$ is finite. Suppose, to the contrary, that $C \setminus D$ is infinite and select a countably infinite set $\tilde{D} = \{c_0, c_1, c_3, \cdots\} \subseteq C \setminus D$. As above, there is a bijection $\tilde{f} : \tilde{D} \times \{0, 1\} \to \tilde{D}$ which we combine with the bijection $f : D \times \{0, 1\} \to D$ to a bijection $g : \left(D \cup \tilde{D}\right) \times \{0, 1\} \to \left(D \cup \tilde{D}\right)$. But this contradicts the maximality of (D, f) in $\mathscr{D}$. □