Constructing Algebraic Closures

April 16, 2022

Constructing Algebraic Closures

Let K be a field. The purpose of this note is to construct an algebraic closure of K. Let us first introduce some notation. For each $k, n \in \mathbb{N}$ the **kth elementary symmetric polynomial in n variables** $X_1, \ldots, X_n$, denoted $e_k(X_1, \ldots, X_n)$, is defined by

$$e_k(X_1, \ldots, X_n) = \begin{cases} 1 & \text{if } k = 0 \\ \sum_{1 \le i_1 < \cdots < i_k \le n} X_{i_1} \cdots X_{i_k} & \text{if } k \le n \\ 0 & \text{if } k > n \end{cases}$$

For each nonconstant monic polynomial $f(X)$ in $K[X]$, write

$$f(X) = X^{n_f} + c_{f,1}X^{n_f - 1} + \cdots + c_{f,k}X^{n_f - k} + \cdots + c_{f,n_f}$$

where n_f is the degree of f and $c_{f,k} \in K$ for all $1 \le k \le n_f$, and let $t_{f,1}, \ldots, t_{f,n_f}$ be independent variables. Throughout this section, whenever we write "$t_{f,k}$", it is understood that f is a nonconstant monic polynomial in $K[X]$ and that $1 \le k \le n_f$. For each nonconstant monic polynomial f in $K[X]$, choose a splitting field of f over K and let $\alpha_{f,1}, \ldots, \alpha_{f,n_f}$ be the roots of f in this splitting field. Let $A = K[\{t_{f,k}\}]$ be the polynomial ring generated over K by indepedent variables doubly indexed by every nonconstant monic $f \in K[X]$ and $1 \le k \le n_f$, and let $\mathfrak{a}$ be the ideal in A generated by the coefficients of all the difference polynomials

$$f(X) - \prod_{i=1}^{n_f}(X - t_{f,k}) \in A[X].$$

In other words, $\mathfrak{a} = \langle \{u_{f,k}\} \rangle$ where

$$u_{f,k} := c_{f,k} - (-1)^k e_k(t_{f,1}, \ldots, t_{f,n_f})$$

for each nonconstant monic polynomial f and for each $1 \le k \le n_f$. Observe that

$$u_{f,k}(\alpha_{f,1}, \ldots, \alpha_{f,n_f}) = 0$$

for all nonconstant monic polynomials f in $K[X]$. Indeed, we can factor f over $K(\alpha_{f,1} \ldots, \alpha_{f,n_f})$ as

$$(X - \alpha_{f,1}) \cdots (X - \alpha_{f,n_f}) = f(X) = X^{n_f} + c_{f,1}X^{n_f - 1} + \cdots + c_{f,n_f}. \quad (1)$$

Expanding the left-hand side of (1) and comparing coefficients gives us the desired result.

Lemma 0.1. *The ideal $\mathfrak{a}$ is proper.*

Proof. Assume for a contradiction that $\mathfrak{a}$ is not proper, so $1 \in \mathfrak{a}$. Then we can write 1 as a finite sum

$$1 = \sum_{i=1}^{m} v_i u_{f_i,k_i} \quad (2)$$

where $v_i \in A$ for all $1 \le i \le m$. Evaluating $t_{f_i,k_i} = \alpha_{f_i,k_i}$ for each $1 \le i \le m$ to both sides of (2) gives us $1 = 0$. This is a contradiction. $\square$

Since $\mathfrak{a}$ is a proper ideal, Zorn's Lemma guarantees that $\mathfrak{a}$ is contained in some maximal ideal $\mathfrak{m}$ of A. The quotient ring $A/\mathfrak{m}$ is a field and the natural composite homomorphism $K \to A \to A/\mathfrak{m}$ of rings lets us view the field $A/\mathfrak{m}$ as an extension of K since ring homomorphisms out of fields are always injective.

Theorem 0.2. *The field $A/\mathfrak{m}$ is an algebraic closure of K.*

Proof. For each indeterminate $t_{f,k}$, let $\bar{t}_{f,k}$ denote its coset in $A/\mathfrak{m}$. Observe that for each nonconstant monic polynomial f in $K[X]$, we have

$$\begin{aligned} f(X) &= X^{n_f} + \sum_{k=1}^{n_f} c_{f,k} X^{n_f - k} \\ &\equiv X^{n_f} + \sum_{k=1}^{n_f} (-1)^k e_k(t_{f,,1}, \dots, t_{f,n_f}) X^{n_f-k} \quad \bmod \mathfrak{m} \\ &= \prod_{k=1}^{n_f} (X - \bar{t}_{f,k}). \end{aligned}$$

since $u_{f,1}, \dots, u_{f,n_f} \in \mathfrak{m}$. Thus $f(X)$ splits completely in $(A/\mathfrak{m})[X]$, and since $\bar{t}_{f,k}$ is a root of f, we see that each $\bar{t}_{f,k}$ is algebraic over K. It follows that $A/\mathfrak{m}$ is an algebraic extension field of K since $A/\mathfrak{m}$ is generated by the $\bar{t}_{f,k}$'s (as A is generated by the $t_{f,k}$'s) and that every nonconstant monic in $K[X]$ splits completely in $A/\mathfrak{m}$.

We will now show $A/\mathfrak{m}$ is algebraically closed, and thus it is an algebraic closure of K. Set $L = A/\mathfrak{m}$. It suffices to show every monic irreducible π in $L[X]$ has a root in L. We have already seen that any nonconstant monic polynomial in $L[X]$ splits completely in $L[X]$, so let's show π is a factor of some monic polynomial in $L[X]$. There is a root α of π in some extension of L. Since α is algebraic over L and L is algebraic over K, it follows that α is algebraic over K. This implies some monic f in $K[X]$ has α as a root. The polynomial π is the minimal polynomial of α in $L[X]$, so $\pi \mid f$ in $L[X]$. Since f splits completely in $L[X]$, we have $\alpha \in L$. $\square$

Counting the Number of Maximal Ideals

In this section, let $f(X)$ to be a monic separable irreducible polynomial over a field K of degree n and express it as

$$f = X^n + \sum_{i=1}^{n} c_i X^{n-i}$$

where $c_i \in K$ for all $1 \leq i \leq n$. Let L be a splitting field of f over K and let $\alpha_1, \dots, \alpha_n$ be the roots of f in L, so $L = K(\alpha_1, \dots, \alpha_n)$. Let $T_1, \dots, T_n$ be indeterminates, and let $R = K[T_1, \dots, T_n]/\langle u_1, \dots, u_n \rangle$ where

$$u_i = c_i - (-1)^i e_i(T_1, \dots, T_n)$$

for each $1 \leq i \leq n$. We denote by t_i to be the image of T_i under the quotient map $K[T_1, \dots, T_n] \to R$ for each $1 \leq i \leq n$.

Theorem 0.3. *The number of maximal ideals of R is given by*

$$\frac{n!}{|\mathrm{Gal}(L/K)|}$$

Proof. We first note that the maximal ideals of R are all of the form $\ker \psi$ where $\psi\colon R \to L$ is a nonzero K-algebra homomorphism. Indeed, let $\mathfrak{m}$ be a maximal ideal of R and let $\bar{t}_i$ be the image of t_i under the quotient map $\rho\colon R \to R/\mathfrak{m}$ for each $1 \leq i \leq n$. Note that f splits over R as

$$\begin{aligned} f(X) &= X^n + \sum_{i=1}^{n} c_i X^{n-i} \\ &= X^n + \sum_{i=1}^{n_i} (-1)^i e_i(t_1, \dots, t_n) X^{n-i} \\ &= \prod_{i=1}^{n} (X - t_i). \end{aligned}$$

In particular $f(t_i) = 0$ for all $1 \leq i \leq n$. This implies $f(\bar{t}_i) = 0$ for each $1 \leq i \leq n$. Therefore $R/\mathfrak{m} = K(\bar{t}_1, \dots, \bar{t}_n)$ is a splitting field of f over K. It follows that there exists a K-algebra isomorphism $\iota\colon R/\mathfrak{m} \to L$. Thus $\mathfrak{m}$ is the kernel of the K-algebra homomorphism $\iota\rho\colon R \to L$.

Thus in order to describe the maximal ideals of R, it suffices to describe the nonzero K-algebra homomorphisms $R \to L$. There is an obvious nonzero K-algebra homomorphism $\varphi\colon R \to L$ given by $\varphi(t_i) = \alpha_i$ for all $1 \leq i \leq n$. Furthermore, if $\pi \in S_n$, then we obtain another nonzero K-algebra homomorphism $\varphi\pi\colon R \to L$ given by $\varphi\pi(t_i) = \alpha_{\pi(i)}$ for all $1 \leq i \leq n$. We claim that this is all of them. Indeed, since $f(t_i) = 0$, we see that any K-algebra homomorphism $R \to L$ must send t_i to some root of f in L, say $\alpha_{\pi(i)}$, for each $1 \leq i \leq n$. Moreover, the $\alpha'_{\pi(i)}s$ must satisfy

$$f(X) = \prod_{i=1}^{n} (X - \alpha_{\pi(i)}).$$

Thus π must be a permutation of $\{1, \dots, n\}$. It follows that every K-algebra has the form $\varphi\pi$ for some $\pi \in S_n$.

Finally, suppose $\psi_1\colon R \to L$ and $\psi_2\colon R \to L$ are two K-algebra homomorphisms. We claim that $\ker \psi_1 = \ker \psi_2$ if and only if there exists a $\sigma \in \mathrm{Gal}(L/K)$ such that $\psi_1\sigma = \psi_2$ (where we view $\mathrm{Gal}(L/K)$ as a subgroup of S_n in the natural way). Indeed, one direction is clear. For the other direction, let $\rho\colon R \to R/\ker \psi_1$ be the quotient map and let $\overline{\psi}_1\colon R/\ker \psi_1 \to L$ and $\overline{\psi}_2 = R/\ker \psi_1 \to L$ be the K-algebra isomorhpisms induced by ψ_1 and ψ_2 respectively (so $\overline{\psi}_1\varrho = \psi_1$ and $\overline{\psi}_2\pi = \psi_2$). If we define $\sigma = \overline{\psi}_2\overline{\psi}_1^{-1}$, then it is easy to check that $\psi_1\sigma = \psi_2$. □