CONSTRUCTING ALGEBRAIC CLOSURES

KEITH CONRAD

Let K be a field. We want to construct an algebraic closure of K, *i.e.*, an algebraic extension of K which is algebraically closed. It will be built out of the quotient of a polynomial ring in a very large number of variables.

Let P be the set of all nonconstant monic polynomials in $K[X]$ and let $A = K[t_f]_{f \in P}$ be the polynomial ring over K generated by a set of indeterminates indexed by P. This is a *huge* ring. For each $f \in K[X]$ and $a \in A$, $f(a)$ is an element of A. Let I be the ideal in A generated by the elements $f(t_f)$ as f runs over P.

Lemma 1. *The ideal I is proper: $1 \notin I$.*

Proof. Every element of I has the form $\sum_{i=1}^n a_i f_i(t_{f_i})$ for a finite set of $f_1, \ldots, f_n$ in P and $a_1, \ldots, a_n$ in A. We want to show 1 can't be expressed as such a sum. Construct a finite extension L/K in which $f_1, \ldots, f_n$ all have roots. There is a substitution homomorphism $A = K[t_f]_{f \in P} \to L$ sending each polynomial in A to its value when t_{f_i} is replaced by a root of f_i in L for $i = 1, \ldots, n$ and t_f is replaced by 0 for those $f \in P$ not equal to an f_i. Under this substitution homomorphism, the sum $\sum_{i=1}^n a_i f_i(t_{f_i})$ goes to 0 in L so this sum could not have been 1. $\square$

Since I is a proper ideal, Zorn's lemma guarantees that I is contained in some maximal ideal $\mathfrak{m}$ in A. The quotient ring $A/\mathfrak{m}$ is a field and the natural composite homomorphism $K \to A \to A/\mathfrak{m}$ of rings let us view the field $A/\mathfrak{m}$ as an extension of K (ring homomorphisms out of fields are always injective). Every nonconstant monic polynomial $f \in K[X]$ has a root in $A/\mathfrak{m}$: the coset $\overline{t}_f = t_f \bmod \mathfrak{m}$ is a root, since $f(\overline{t}_f) = \overline{f(t_f)} = \overline{0}$. Since each $\overline{t}_f$ is algebraic over K and $A/\mathfrak{m}$ is generated over K as a ring by the $\overline{t}_f$'s, $A/\mathfrak{m}$ is an algebraic extension of K in which every monic polynomial in $K[X]$ has a root.

If K is not algebraically closed, the field $K' := A/\mathfrak{m}$ is a larger field than K because every polynomial in $K[X]$ has a root in K'. If K' is algebraically closed then we are done. If it is not then our construction can be iterated (producing a larger field $K'' \supset K'$ whose relation to K' is the same as that of K' to K) over and over and a union of all iterations is taken. The union is an algebraic extension of the initial field K since it is at the top of a tower of algebraic extensions. It can be proved [1, p. 544] that this union is itself algebraically closed and thus constitutes an algebraic closure of K.

The interesting point is that there is no need to iterate the construction: $K' = A/\mathfrak{m}$ is already algebraically closed. This requires some effort to prove, but it is a nice illustration of various techniques (in particular, the use of perfect fields in characteristic p). The result follows from the next theorem and was inspired by [2].

Theorem 2. *Let L/K be an algebraic extension such that every nonconstant polynomial in $K[X]$ has a root in L. Then every nonconstant polynomial in $L[X]$ has a root in L, so L is an algebraic closure of K.*

Proof. It suffices to show every irreducible in $L[X]$ has a root in L.

First we will describe an incomplete attempt at a proof, just to make it clear where the difficulty in the proof lies. Pick an irreducible $\widetilde{\pi}(X)$ in $L[X]$. We want to show it has a root in L, but all we know to begin with is that any irreducible in $K[X]$ has a root in L. So let's first show $\widetilde{\pi}(X)$ divides some irreducible in $L[X]$. Any root of $\widetilde{\pi}(X)$ (in some extension of L) is algebraic over L, and thus is algebraic over K, so it has a minimal polynomial $m(X)$ in $K[X]$. Then $\widetilde{\pi}(X)|m(X)$ in $L[X]$ since $\widetilde{\pi}(X)$ divides any polynomial in $L[X]$ having a root in common with $\widetilde{\pi}(X)$. Since $m(X) \in K[X]$, by hypothesis $m(X)$ has a root in L. But this does not imply $\widetilde{\pi}(X)$ has a root in L since we don't know if the root of $m(X)$ in L is a root of its factor $\widetilde{\pi}(X)$ or is a root of some other irreducible factor of $m(X)$ in $L[X]$. So we are stuck. It would have been much simpler if our hypothesis was that every irreducible polynomial in $K[X]$ splits completely in $L[X]$, since then $m(X)$ would split completely in $L[X]$ so its factor $\widetilde{\pi}(X)$ would split completely in $L[X]$ too: if a polynomial splits completely over a field then so does any factor, but if a polynomial has a root in some field then not every factor of it has to have a root in that field. Thus, the difficulty with proving this theorem is working with the weaker hypothesis that polynomials in $K[X]$ pick up a root in L rather than a full set of roots in L.

It turns out that the stronger hypothesis we would rather work with is actually a consequence of the weaker hypothesis we are provided: if every irreducible polynomial in $K[X]$ has a root in L then every irreducible polynomial in $K[X]$ splits completely in $L[X]$. Once we prove this, the idea in the previous paragraph does show every irreducible in $L[X]$ splits completely in $L[X]$ and thus L is algebraically closed.

First we will deal with the case when K has characteristic 0. We want to show that every irreducible polynomial in $K[X]$ splits completely in $L[X]$. Let $\pi(X) \in K[X]$ be irreducible. Let K_π denote a splitting field of π over K. Since K has characteristic 0, it is perfect field so by the primitive element theorem we can write $K_\pi = K(\alpha)$ for some α. There is no reason to expect α is a root of $\pi(X)$ (usually the splitting field of $\pi(X)$ over K is obtained by doing more than adjoining just one root of $\pi(X)$ to K), but α does have some minimal polynomial over K. Denote it by $m(X)$, so $m(X)$ is an irreducible polynomial in $K[X]$. By hypothesis $m(X)$ has a root in L, say β. Then the fields $K_\pi = K(\alpha)$ and $K(\beta)$ are both obtained by adjoining to K a root of the irreducible polynomial $m(X) \in K[X]$, so these fields are K-isomorphic. Since $\pi(X)$ splits completely in $K_\pi[X] = K(\alpha)[X]$ by the definition of a splitting field, $\pi(X)$ splits completely in $K(\beta)[X] \subset L[X]$.

Thus when K has characteristic 0, every irreducible in $K[X]$ splits completely in $L[X]$, which means the argument at the start of the proof shows L is algebraically closed.

If K has characteristic $p > 0$, is the above argument still valid? The essential construction was a primitive element for the splitting field K_π/K for any irreducible π in $K[X]$. There is a primitive element for every finite extension of K provided K is perfect. In characteristic 0 this is no constraint at all. When K has characteristic p, it is perfect if and only if $K^p = K$. It may not be true for our K that $K^p = K$. We will find a way to reduce ourselves to the case of a perfect base field in characteristic p by replacing K with a larger base field.

Let $F = \{x \in L : x^{p^n} \in K \text{ for some } n \geq 1\}$. If $x^{p^n} \in K$ and $y^{p^{n'}} \in K$ then let $s = \max(n, n')$ and note $(x \pm y)^{p^s} = x^{p^s} \pm y^{p^s} \in K$. So F is an additive subgroup of L and contains K. It is easy to see F is closed under multiplication and inversion of nonzero elements, so F is a field between K and L. This field is perfect: $F^p = F$. To see this, choose $x \in F$. For some $n \geq 1$, $x^{p^n} \in K$. Let $a = x^{p^n}$. The polynomial $X^{p^{n+1}} - a$ is in $K[X]$, so by the basic hypothesis of the theorem this polynomial has a root r in L. Since

$r^{p^{n+1}} = a$ is in K, $r \in F$. Since
$$x^{p^n} = a = (r^p)^{p^n},$$
$x = r^p$ because the pth power map is injective for fields of characteristic p. Therefore every $x \in F$ is the pth power of an element of F, so $F^p = F$:

Since L/F is algebraic, any irreducible polynomial in $L[X]$ divides some irreducible polynomial in $F[X]$ and the latter polynomial is separable (F is perfect), so every irreducible polynomial in $L[X]$ is separable. Thus L is perfect, so $L^p = L$.

If we can show that every polynomial in $F[X]$ has a root in L then our proof in characteristic 0 can be applied to the extension L/F, so we will be able to conclude that L is algebraically closed.

Let $g(X) \in F[X]$, say $g(X) = \sum c_i X^i$. We want to show $g(X)$ has a root in L. For some n, $c_i^{p^n} \in K$ for all i. The polynomial $\sum c_i^{p^n} X^i$ is in $K[X]$, so it has a root $r \in L$ by hypothesis. Since $L = L^p$, also $L = L^{p^n}$, so $r = z^{p^n}$ for some $z \in L$. Then
$$0 = \sum_i c_i^{p^n} r^i = \sum_i (c_i z^i)^{p^n} = \left(\sum_i c_i z^i\right)^{p^n} = g(z)^{p^n},$$
so $g(X)$ has a root z in L. □

For a generalization of this theorem, see [3].

References

[1] D. Dummit, R. Foote, "Abstract Algebra," 3rd ed., Wiley, New York, 2004.

[2] R. Gilmer, *A Note on the Algebraic Closure of a Field*, Amer. Mathematical Monthly **75**, 1968, 1101-1102.

[3] I. M. Isaacs, *Roots of Polynomials in Algebraic Extensions of Fields*, Amer. Mathematical Monthly **87**, 1980, 543-544.