ZORN'S LEMMA AND SOME APPLICATIONS, II

KEITH CONRAD

We will describe some applications of Zorn's lemma to field extensions.

An *algebraic closure* of a field K is an algebraic extension L/K such that L is algebraically closed. In [1, p. 544] there is a proof that every field admits an algebraic closure. The proof uses an iterative procedure starting with a polynomial ring in a very large number of variables and a maximal ideal of this ring which contains a certain proper ideal. Such a maximal ideal exists by Zorn's lemma. A modification of this argument is given in the course handout on algebraic closures. For a different proof of the existence of algebraic closures, using Zorn's lemma in a more direct fashion, see [2, pp. 259–260].

Now that we have the existence of algebraic closures, we will use Zorn's lemma to prove any two algebraic closures of a field are isomorphic fields. The first step in the proof, which is where Zorn's lemma is used, concerns the extension of a field homomorphism to a larger field.

Theorem 1. *Let L/K be an algebraic extension and let C be an algebraically closed field. Any ring homomorphism $\varphi\colon K \to C$ can be extended to a homomorphism $L \to C$.*

Proof. Let S be the set of pairs (F, f) where F is an intermediate field between K and L and $f|_K = \varphi$. For instance $(K, \varphi) \in S$, so $S \neq \emptyset$.

Partially order S by declaring $(F, f) \leq (F', f')$ if $F \subset F'$ and $f'|_F = f$. For a totally ordered subset $\{(F_\alpha, f_\alpha)\}_{\alpha \in A}$ in S, an upper bound can be produced as follows. Let $F = \cup_{\alpha \in A} F_\alpha$. Since the F_α's are totally ordered, it's easy to check that F is a field. Define $f\colon F \to C$ by $f(x) = f_\alpha(x)$ when $x \in F_\alpha$. If x is also in F_β, we should check $f_\alpha(x) = f_\beta(x)$ so we know the definition of $f(x)$ is independent of the choice of F_α containing x. Since our subset of S is totally ordered, either $(F_\alpha, f_\alpha) \leq (F_\beta, f_\beta)$ or $(F_\beta, f_\beta) \leq (F_\alpha, f_\alpha)$. In the first case, f_β restricts to f_α on F_α, so $f_\beta(x) = f_\alpha(x)$. The argument in the second case is the same. For $x \in K$, we can view x in any F_α and then $f(x) = f_\alpha(x) = \varphi(x)$ since $f_\alpha|_K = \varphi$, so $f|_K = \varphi$. To prove f is a ring homomorphism, view any two elements of F in a common F_α (total ordering) and use the properties of f_α. Since $f|_{F_\alpha} = f_\alpha$, (F, f) is an upper bound on all the (F_α, f_α)'s.

Now we can apply Zorn's lemma: S has a maximal element (F, σ). That is, F is a field between K and L with a homomorphism $\sigma\colon F \to C$ such that $\sigma|_K = \varphi$ and there is no extension of σ to a homomorphism from a larger intermediate field to C. We will prove $F = L$, which means φ extends up to L.

If $F \neq L$ then there is some $x \in L$ with $x \notin F$. Then $F(x)/F$ is a finite extension of degree greater than 1. We're going to extend σ to a homomorphism $F(x) \to C$. Let $g(X)$ be the minimal polynomial for x in $F[X]$, so there is an F-isomorphism $F(x) \cong F[X]/(g(X))$. Applying σ to the coefficients of $g(X)$ gives a polynomial $g^\sigma(X) \in C[X]$. Since C is algebraically closed, $g^\sigma(X)$ has a root in C, say r. Let $F[X] \to C$ by acting as σ on F and sending X to r. This is a ring homomorphism which sends $g(X)$ to $g^\sigma(r) = 0$, so we get an induced homomorphism $F[X]/(g(X)) \to C$ acting as σ on F and sending $\overline{X}$ to r. Composing this with the isomorphism $F(x) \cong F[X]/(g(X))$ from before gives us a

homomorphism $\tau\colon F(x) \to C$ acting as σ on F. Thus $(F,\sigma) \leq (F(x),\tau)$. This is impossible by maximality of (F,σ), so $F = L$. □

The extension of φ to L is very far from unique.

Corollary 2. *Let K be a field and $i\colon K \to L$ be a ring homomorphism to another field L such that $L/i(K)$ is an algebraic extension. For any ring homomorphism $\varphi\colon K \to C$ into an algebraically closed field there is a ring homomorphism $\sigma\colon L \to C$ such that $\sigma \circ i = \varphi$.*

Proof. Since i is a map of fields it is injective: K and $i(K)$ are isomorphic fields using i. Run through the above proof with the following change: S is the pairs (F, f) where F is a field between $i(K)$ and L and $f \circ i = \varphi$ (rather than $f|_K = \varphi$ as we used before). Define the partial ordering as before: $(F, f) \leq (F', f')$ when $F \subset F'$ and $f'|_F = f$. It is left to the reader to check that S satisfies the assumptions of Zorn's lemma and that a maximal element of S provides a solution to our problem. □

Now we can establish the desired result about two algebraic closures.

Corollary 3. *Any two algebraic closures of a field are isomorphic.*

Proof. Let C_1 and C_2 be algebraic closures of the field K. There are inclusion maps $i_1\colon K \to C_1$ and $i_2\colon K \to C_2$. Since C_2 is algebraically closed and C_1 is an algebraic extension of $i_1(K)$, Corollary 2 tells us there is a ring homomorphism $\sigma\colon C_1 \to C_2$ such that $\sigma \circ i_1 = i_2$.The image $\sigma(C_1)$ is an algebraically closed field which contains $\sigma(i_1(K)) = i_2(K)$. Since C_2 is an algebraic extension of $i_2(K)$, $C_2/\sigma(C_1)$ is an algebraic extension of algebraically closed fields, so the extension has to be trivial: $\sigma(C_1) = C_2$. Thus σ is an isomorphism of C_1 and C_2. □

There is a huge number of isomorphisms between two algebraically closed fields, so the construction in Corollary 3 is not at all canonical.

Corollary 4. *Let K_1 and K_2 be isomorphic fields with respective algebraic closures C_1 and C_2. Any isomorphism $K_1 \to K_2$ extends to an isomorphism $C_1 \to C_2$. In particular, if K is a field with algebraic closure C then any field automorphism of K extends to a field automorphism of C.*

Proof. Let $f\colon K_1 \to K_2$ be a field isomorphism. Composing this with the inclusion $i_2\colon K_2 \to C_2$ gives us a homomorphism $i_2 \circ f\colon K_1 \to C_2$. Apply Corollary 2 using $L = C_1$ and $\varphi = i_2 \circ f$ to see there is a field homomorphism $\sigma\colon C_1 \to C_2$ such that $\sigma \circ i_1 = \varphi = i_2 \circ f$, so we have a commutative diagram

$$\begin{array}{ccc} C_1 & \stackrel{\sigma}{\longrightarrow} & C_2 \\ \uparrow{\scriptstyle i_1} & & \uparrow{\scriptstyle i_2} \\ K_1 & \stackrel{f}{\longrightarrow} & K_2 \end{array}$$

which shows $\sigma(C_1)$ is an algebraically closed subfield of C_2 that contains $\sigma(i_1(K_1)) = i_2(f(K_1)) = i_2(K_2) = K_2$. As C_2 is an algebraic closure of K_2 we must have $\sigma(C_1) = C_2$, so σ is an isomorphism. □

There is nothing canonical about the choice of σ: the isomorphism f will generally have many extensions to an isomorphism of C_1 with C_2.

In addition to algebraic closures, certain fields have another, smaller, kind of closure called a *real closure*. Before we define a real closure, we have to define a real field. A field is called *real* (some use the label *formally real*) if -1 is not a sum of squares in the field.

Obviously $\mathbf{R}$ is an example of a real field. Any subfield of a real field is also real. More generally, any field that can be embedded in a real field is real. For example, the abstract field $\mathbf{Q}(\theta)$ where $\theta^3 = 2$ is a real field since it is isomorphic to $\mathbf{Q}(\sqrt[3]{2})$, which is real because it is a subfield of $\mathbf{R}$. The fields $\mathbf{C}$ and $\mathbf{Q}(i)$ are obviously not real since -1 is a square in these fields. Less obviously, $\mathbf{Q}(\sqrt{-2})$ is not real; although -1 is not a square in $\mathbf{Q}(\sqrt{-2})$ it is a sum of two squares: $-1 = (\sqrt{-2}/2)^2 + (\sqrt{-2}/2)^2$.

The concept of a real field is closely connected with the concept of an ordered field (a field on which one has a reasonable notion of positive and negative): the fields which admit an ordering – not necessarily just one – turn out to be precisely the real fields. For more information about real fields, see [3, Chap. XI].

A *real closure* of a field K is an extension field L that is algebraic, real, and admits no proper real algebraic extensions. In other words, it basically behaves for real fields like algebraic closures do for all fields (but a real closure is not algebraically closed, *e.g.*, X^2+1 has no root in real fields). Since a real closure is a real field, and subfields of real fields are real, only real fields could have real closures. And indeed they all do, as we now prove.

Theorem 5. *Every real field admits a real closure.*

Proof. Let K be a real field. That is, -1 is not a sum of squares in K. A real closure of K would be a particular kind of algebraic extension, so we will work in a fixed algebraic closure $C \supset K$. Since a real closure should arise as a maximal real algebraic extension, the way to use Zorn's lemma should be obvious: take for S the set of all real algebraic extensions of K *inside of* C. We know $S \neq \emptyset$ since $K \in S$. Define a partial ordering on S by inclusion: $F \leq F'$ if $F \subset F'$. If $\{F_\alpha\}_{\alpha \in A}$ is a totally ordered subset of S then the union $F = \cup_{\alpha \in A} F_\alpha$ is a field (by the usual proof) which is inside of C and it contains each F_α. To see that F is real, assume otherwise: $-1 = \sum_{k=1}^n c_i^2$ where $c_i \in F$. These finitely many c_i's are in some common F_α (since the F_α's are totally ordered), but then the equation violates the property of that F_α being real. So in fact -1 is not a sum of squares in F, which means F is real and thus is an upper bound on $\{F_\alpha\}_{\alpha \in A}$ in S.

By Zorn's lemma, S contains a maximal element. Denote one as R. Then R is a real algebraic extension field of K. Could R admit a proper real algebraic extension? Certainly not in C, because R is maximal for inclusion among real algebraic extensions of K in C. If there was some extension $R \hookrightarrow R'$ outside of C where R' is real and algebraic over R, then by Theorem 1 we can embed R' into C by a map fixing R. (C is an algebraic closure of R.) In particular, the image of an embedding $R' \hookrightarrow C$ fixing R pointwise will be a (necessarily) real field in C of degree greater than 1 over R, but that contradicts maximality of R in S. So R fits the definition of being a real closure of K. □

As with algebraic closures, Zorn's lemma can be used to prove any two real closures of a real field are isomorphic [3, p. 455], but the proof requires some preliminary work on "real roots" of polynomials that would be a bit of a diversion for us to review here. To appreciate the special role of real fields, where none of the polynomials $\sum_{j=1}^n X_i^2 + 1$ have zeros, observe that Zorn's lemma implies that a field which does not contain a square root of -1 admits a maximal algebraic extension which does not contain a square root of -1, but two such maximal extensions *need not* be isomorphic. For example, the fields $\mathbf{Q}(\sqrt{2})$ and $\mathbf{Q}(\sqrt{-2})$ don't contain a square root of -1 and therefore each admits a maximal algebraic extension $F/\mathbf{Q}(\sqrt{2})$ and $F'/\mathbf{Q}(\sqrt{-2})$ not containing $\sqrt{-1}$. Both F and F' are also maximal algebraic extensions of $\mathbf{Q}$ not containing $\sqrt{-1}$, but $F \ncong F'$ since $X^2 - 2$ has a root in F but not in

F' (if F' has a square root of 2 then its ratio with $\sqrt{-2} \in F'$ is a square root of -1 in F', and that's impossible).

We have focused our applications of Zorn's lemma for fields to the case of algebraic extensions (specifically, algebraic closures and real closures). Zorn's lemma is just as important in dealing with non-algebraic field extensions (such as $K(X, Y)$ where X and Y are indeterminantes). The central notion here is a transcendence basis, which is basically a maximal set of algebraically independent elements. It is a non-linear generalization of a vector space basis, and its existence in general uses Zorn's lemma. See [3, Chap. VIII] or [5, pp. 357–373] for a detailed discussion of transcendence bases and [1, Sect. 14.9] for a survey on transcendence bases without proofs. As motivation for caring about transcendence bases, a careful study of them yields the following interesting result about algebraically closed fields.

Theorem 6. *Two uncountable algebraically closed fields are isomorphic if and only if they have the same characteristic and cardinality.*

For instance, any algebraically closed field of characteristic 0 whose cardinality is the same as that of $\mathbf{C}$ is isomorphic to $\mathbf{C}$ as an abstract field. (Examples of this situation really do occur, *e.g.*, the algebraic closure of the p-adic numbers.)

Theorem 6 is false for countable algebraically closed fields. For instance, the algebraic closures of $\mathbf{Q}$ and $\mathbf{Q}(X)$ are both countable of characteristic 0, but they are not isomorphic fields since we can't embed $\mathbf{Q}(X)$ inside an algebraic closure of $\mathbf{Q}$: the element X is not algebraic over $\mathbf{Q}$.

Zorn's lemma has another important use in field theory, connected with the extension of absolute values: if L/K is an arbitrary field extension, any non-archimedean absolute value on K admits an extension (generally not unique) to a non-archimedean absolute value on L. This is a theorem of Krull. Much as the proof of Theorem 1 is reduced to the case of a simple field extension (that is, a single generator) using Zorn's lemma, the proof of Krull's theorem is reduced by Zorn's lemma to the case of a simple extension, and one can then treat the cases when t is algebraic over K or transcendental over K. These are handled by separate methods, as illustrated in [6, pp. 36–39]. For an alternate proof of the extension of non-archimedean absolute values using Zorn's Lemma, see [4, pp. 107–108].

References

[1] D. Dummit and R. Foote, "Abstract Algebra," 3rd ed., Wiley, New York, 2004.
[2] T. W. Hungerford, "Algebra," Springer-Verlag, New York, 1974.
[3] S. Lang, "Algebra," 3rd revised ed., Springer-Verlag, New York, 2002.
[4] P. Ribenboim, "The Theory of Classical Valuations," Springer-Verlag, New York, 1999.
[5] J. Rotman, "Advanced Modern Algebra," Prentice-Hall, Upper Saddle River, NJ, 2002.
[6] W. Schikhof, "Ultrametric calculus: an introduction to p-adic analysis," Cambridge Univ. Press, Cambridge, 1984.