ZORN'S LEMMA AND SOME APPLICATIONS, II

KEITH CONRAD

We will describe some applications of Zorn's lemma to field extensions, mostly involving algebraically closed and real closed fields.

1. Zorn's lemma and algebraic closures

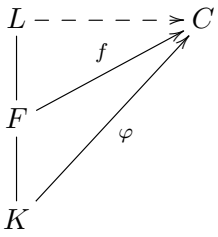
An *algebraic closure* of a field K is an algebraic extension of K that is algebraically closed. That every field has an algebraic closure is proved in [1, p. 544] by an iterative procedure starting with a polynomial ring in a very large number of variables and a suitably chosen maximal ideal of this ring. Such a maximal ideal exists by Zorn's lemma.[1] A proof of the existence of algebraic closures that uses Zorn's lemma in a more direct fashion is in [2, pp. 259–260].

We will use Zorn's lemma here to prove all algebraic closures of a field are isomorphic to each other. The first step in the proof, which is where Zorn's lemma is used, is to extend a field homomorphism to a larger field.

Theorem 1.1. *Let L/K be an algebraic extension. Every field homomorphism $\varphi\colon K \to C$, where C is an algebraically closed field, can be extended to a homomorphism $L \to C$.*

We are *not* saying C is an algebraic closure of K: it could be much larger. For example, K could be $\mathbf{Q}(\sqrt[4]{2})$ and C could be $\mathbf{C}$. Also, the extension of $\varphi\colon K \to C$ to a homomorphism $L \to C$ is very far from being unique.

Proof. Let S be the set of pairs (F, f) where F is an intermediate field between K and L and $f\colon F \to C$ is a field homomorphism such that $f|_K = \varphi$. Since $(K, \varphi) \in S$, $S \neq \emptyset$.



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 $F = \bigcup_{\alpha \in A} F_\alpha$. 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 some F_α and then $f(x) = f_\alpha(x) = \varphi(x)$ since $f_\alpha|_K = \varphi$,

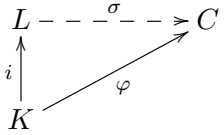
[1] A modification of this proof is in https://kconrad.math.uconn.edu/blurbs/galoistheory/algclosureshorter.pdf.

so $f|_K = \varphi$. To prove f is a field homomorphism, view two elements of F in a common F_α (total ordering) and use the fact that f_α is a field homomorphism. 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 that 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 $F = L$. □

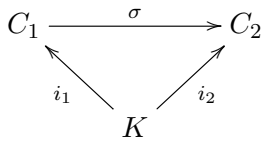
Corollary 1.2. *Let K be a field and $i\colon K \to L$ be a homomorphism to a field L such that $L/i(K)$ is an algebraic extension. For each field homomorphism $\varphi\colon K \to C$ to an algebraically closed field C, there is a field homomorphism $\sigma\colon L \to C$ such that $\sigma \circ i = \varphi$.*



Proof. Since i is a field homomorphism it is injective: K and $i(K)$ are isomorphic fields using i. Run through the above proof with the following change: S is the set of 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 comparing two algebraic closures of a field.

Corollary 1.3. *All algebraic closures of a field are isomorphic. More precisely, if C_1 and C_2 are algebraic closures of a field K with embeddings $i_1\colon K \to C_1$ and $i_2\colon K \to C_2$, there is a field isomorphism σ that makes the following diagram commute.*



Proof. Since C_2 is algebraically closed and C_1 is an algebraic extension of $i_1(K)$, Corollary 1.2 implies there is a field 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 that 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 $\sigma\colon C_1 \to C_2$ is a field isomorphism and $\sigma \circ i_1 = i_2$. □

There is a huge number of isomorphisms between two algebraically closed fields, so the construction in Corollary 1.3 is not at all canonical.

Corollary 1.4. *Let K_1 and K_2 be isomorphic fields with respective algebraic closures C_1 and C_2. Each 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 every field homomorphism $f\colon K \to C$ such that $C/f(K)$ is algebraic extends to a field automorphism of C.*

There is nothing canonical about the extension: an isomorphism $K_1 \to K_2$ will generally have many extensions to an isomorphism $C_1 \to C_2$.

Proof. Let $f\colon K_1 \to K_2$ be a field isomorphism and $i_1\colon K_1 \to C_1$ and $i_2\colon K_2 \to C_2$ be embeddings into algebraic closures. Composing f with the embedding $i_2\colon K_2 \to C_2$ gives us a field homomorphism $i_2 \circ f\colon K_1 \to C_2$. In Corollary 1.2 use $L = C_1$ 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

$$\begin{array}{ccc} C_1 & \xrightarrow{\sigma} & C_2 \\ {\scriptstyle i_1}\uparrow & \nearrow_{\varphi} & \uparrow{\scriptstyle i_2} \\ K_1 & \xrightarrow{f} & K_2 \end{array}$$

that shows $\sigma(C_1)$ is a subfield of C_2 containing $\sigma(i_1(K_1)) = i_2(f(K_1)) = i_2(K_2) = K_2$. Since C_2 is an algebraic closure of K_2, $K_2 \subset \sigma(C_1) \subset C_2$, and $\sigma(C_1)$ is algebraically closed, we must have $\sigma(C_1) = C_2$, so σ is an isomorphism.

If the field K has algebraic closure C and $f\colon K \to C$ is a field homomorphism, then $f\colon K \to \sigma(K)$ is a field isomorphism (a homomorphism, surjective, and injective since all field homomorphisms are injective). When C is algebraic over $f(K)$, C is an algebraic closure of $f(K)$, so $f\colon K \to f(K)$ extends to an isomorphism $C \to C$ by using $K_1 = K$, $K_2 = f(K)$, $C_1 = C_2 = C$, and $i_1\colon K \to C$ and $i_2\colon f(K) \to C$ are inclusions.

$$\begin{array}{ccc} C & \xrightarrow{\sigma} & C \\ {\scriptstyle i_1}\uparrow & & \uparrow{\scriptstyle i_2} \\ K & \xrightarrow{f} & f(K) \end{array}$$

□

2. Zorn's lemma and real closed fields

Every field has an algebraic closure. 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. For instance, $\mathbf{R}$ is a real field. A subfield of a real field is also real. More generally, a field that can be embedded into a real field is real. For example, the abstract field $\mathbf{Q}(\theta)$ where $\theta^4 = 2$ is a real field since it is isomorphic to $\mathbf{Q}(\sqrt[4]{2})$, which is real because it is a subfield of $\mathbf{R}$. The fields $\mathbf{C}$ and $\mathbf{Q}(i)$ are not real since -1 is a square in these fields. The field $\mathbf{Q}(\sqrt{-2})$ is not real since -1 is a sum of two squares in this field: $-1 = (\sqrt{-2}/2)^2 + (\sqrt{-2}/2)^2$.

The concept of a real field is closely connected with the concept of an ordered field (a field in which there is a reasonable notion of positive and negative): a field has some ordering – not necessarily just one – precisely when it is a real field. That is, the orderable fields are the real fields. For example, $\mathbf{Q}(\theta)$ where $\theta^4 = 2$ has two orderings, based on the two embeddings into $\mathbf{R}$ ($\theta \mapsto \sqrt[4]{2}$ and $\theta \mapsto -\sqrt[4]{2}$). For more information about real fields, see [4, Chap. XI].

A *real closure* of a field K is an extension field L that is algebraic over K, real, and admits no proper real algebraic extension. A real closure is essentially a maximal algebraic extension in which -1 is not a sum of squares. For example, the field of real algebraic numbers is a real closure of $\mathbf{Q}$. Real closures are not algebraically closed since $X^2 + 1$ has no root in real fields.

Since a real closure is a real field and subfields of real fields are real, K can only have a real closure if K is real. And indeed they all do, as we now prove.

Theorem 2.1. *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, if it exists, is a particular kind of algebraic extension of K, so we will work inside a fixed algebraic closure $C \supset K$.

Since a real closure should be a maximal real algebraic extension of K, 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 $F = \bigcup_{\alpha \in A} F_\alpha$ is a field (by the usual proof) that is inside of C and it contains each F_α. To see that F is real, assume otherwise: $-1 = \sum_{i=1}^n c_i^2$ 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 $-1 = \sum_{i=1}^n c_i^2$ violates the property of F_α being real. So -1 is not a sum of squares in F, which means F is real and thus F 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. To show R is a real closure of K we need to show R has no proper real algebraic extension. There is no such extension of R in C because R is maximal with respect to inclusion among real algebraic extensions of K in C. If there is a field extension $R \hookrightarrow R'$ outside of C where R' is real and algebraic over R, then by Theorem 1.1 we can embed R' into C by a map fixing R. (The field C is an algebraic closure of R since it is an algebraic closure of K and R/K is algebraic.) 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 all real closures of a real field are isomorphic to each other [4, p. 455]. The proof requires some preliminary work on "real roots" of polynomials that would be a bit of a diversion for us to review here.

In a real field, none of the polynomials $\sum_{i=1}^n X_i^2 + 1$ have solutions. If we only avoid fields with solutions to the single polynomial $X^2 + 1$, such maximal extensions need not be isomorphic. That is, Zorn's lemma implies that a field not containing a square root of -1 has a maximal algebraic extension not containing 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 so each of these fields has 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.

3. Zorn's lemma and transcendence bases

So far we have focused on applications of Zorn's lemma to algebraic field 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 over K. The central notion here is a transcendence basis for a field extension L/K, which is a nonlinear generalization of a basis for L/K.

Definition 3.1. In a field extension L/K, a finite subset $\{s_1, \ldots, s_n\}$ of L is called *algebraically dependent over* K if $f(s_1, \ldots, s_n) = 0$ for some nonzero polynomial $f(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]$. A finite subset of L that is not algebraically dependent over K is called *algebraically independent* over K. An arbitrary subset of L is called algebraically dependent over K if some finite subset is algebraically dependent over K and it is called algebraically independent over K when every finite subset is algebraically independent over K (that is, no finite subset is algebraically dependent over K).

If we only use linear polynomials $f(X_1, \ldots, X_n) = a_1X_1 + \cdots + a_nX_n$ in this definition then we get the concepts of linear dependence and linear independence over K. That is why algebraic dependence and independence over K is a higher-degree generalization of linear dependence and independence over K. We consider $\emptyset$ in L to be algebraically independent over K, just as $\emptyset$ in L is linearly independent over K.

Example 3.2. In $\mathbf{R}$, $\{\pi, \pi + \sqrt{2}\}$ is linearly independent over $\mathbf{Q}$ (since $\sqrt{2}$ is algebraic and π is transcendental), but is algebraically dependent over $\mathbf{Q}$ since $f(\pi, \pi + \sqrt{2}) = 0$ where $f(X, Y) = (X - Y)^2 - 2$.

Example 3.3. In $\mathbf{R}$, $\{\pi^2 - 2, 3\pi + \sqrt{2}\}$ is algebraically dependent over $\mathbf{Q}$: $f(\pi^2 - 2, 3\pi + \sqrt{2}) = 0$ where $f(X, Y) = (X + 2 - (Y - \sqrt{2})^2/9)(X + 2 - (Y + \sqrt{2})^2/9) = X^2 + (32/9)X + Y^4/81 - (2/9)XY^2 - (40/81)Y^2 + 256/81$.

Example 3.4. A one-element subset $\{s\}$ of L is algebraically independent over K if and only if it s is transcendental over K.

Example 3.5. The extension L/K is algebraic if and only if the only subset of L that is algebraically independent over K is $\emptyset$.

Example 3.6. It is expected that π and e are algebraically independent over $\mathbf{Q}$, but this is still an open problem. It would follow from Schanuel's conjecture [5, Theorem 21.3].

Example 3.7. In the rational function field in n variables, $K(u_1, \ldots, u_n)$, $\{u_1, \ldots, u_n\}$ is algebraically independent over K.

Definition 3.8. In a field extension L/K, a subset S of L is called a *transcendence basis* over K if S is algebraically independent over K and S is not strictly contained in any other algebraically independent subset over K.

Example 3.9. For a field K, each nonconstant rational function $a(u)/b(u) \in K(u)$ is a transcendence basis: $a(u)/b(u)$ is transcendental over K because $K(u)/K(a/b)$ is algebraic (u is a root of $a(X) - (a(u)/b(u))b(X) \in K(a/b)[X]$, which is not 0) and $K(u)/K$ is not

algebraic. No subset of $K(u)$ strictly containing $\{a(u)/b(u)\}$ is algebraically independent since $K(u)/K(a/b)$ is algebraic.

Example 3.10. In the rational function field $K(u_1, \ldots, u_n)$, the subset $\{u_1, \ldots, u_n\}$ is a transcendence basis: it is algebraically independent over K, and for a rational function $r = a(u_1, \ldots, u_n)/b(u_1, \ldots, u_n)$, the polynomial

$$f(X_1, \ldots, X_n, X_{n+1}) = b(X_1, \ldots, X_n)X_{n+1} - a(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n, X_{n+1}]$$

is nonzero (why?) and $f(u_1, \ldots, u_n, r) = 0$. Therefore $\mathrm{tr.deg}(K(u_1, \ldots, u_n)/K) = n$.

Theorem 3.11. *Every field extension L/K has a transcendence basis and every subset of L that is algebraically independent over K can be extended to a transcendence basis of L/K.*

Proof. To show L/K has a transcendence basis, consider the collection of all subsets of L that are algebraically independent over K, partially ordered by containment. This is not an empty collection since $\emptyset$ is algebraically independent over K by definition. For every totally ordered subset $\{S_\alpha\}_{\alpha \in A}$ of algebraically independent subsets over K, the union $S = \bigcup_\alpha S_\alpha$ is an algebraically independent subset over K because every finite set of elements of S is in some S_α and S_α is an algebraically independent subset over K. Therefore by Zorn's lemma there is a subset of L that is (i) algebraically independent over K and (ii) not strictly contained in a subset of L that is algebraically independent over K. Properties (i) and (ii) describe a transcendence basis of L/K.

To show every subset S_0 of L that is algebraically independent over K can be extended to a transcendence basis of L/K, run through the previous argument using algebraically independent subsets of L that contain S_0. □

Theorem 3.12. *All transcendence bases of L/K have the same cardinality.*

Proof. See [2, Chap. VI, Theorems 1.8, 1.9]. □

The common cardinality of all transcendence bases for L/K is called the *transcendence degree* of L/K and is denoted $\mathrm{tr.deg}(L/K)$. This cardinal number is well-defined by Theorem 3.12.

Example 3.13. We have $\mathrm{tr.deg}(L/K) = 0$ if and only if L/K is algebraic.

Example 3.14. We have $\mathrm{tr.deg}(K(u_1, \ldots, u_n)/K) = n$.

Example 3.15. The field $K(x, y)$ where x is transcendental over K and $y^2 = x^3 - 1$ has transcendence degree 1 over K, with transcendence basis $\{x\}$.

See [4, Chap. VIII] or [7, pp. 357–373] for a detailed discussion of transcendence bases and [1, Sect. 14.9] for a survey on transcendence bases without proofs.

When L/K has a transcendence basis S, the intermediate field $K(S)$ is purely transcendental over K, in the sense that it is generated over K by elements that are algebraically independent over K. The extension $L/K(S)$ is algebraic: if some $\alpha \in L$ were transcendental over $K(S)$ then $S \cup \{\alpha\}$ would be algebraically independent over K (why?), which contradicts the maximality of a transcendence basis. Therefore every field extension L/K can be broken up into a tower $L/K(S)/K$ where $K(S)/K$ is purely transcendental and $L/K(S)$ is algebraic. In particular, if L is algebraically closed then L is an algebraic closure of the field $K(S)$ that is purely transcendental over K.

Example 3.16. If C is an algebraically closed field of characteristic 0 and S is a transcendence basis of $C/\mathbf{Q}$ then $C = \overline{\mathbf{Q}(S)}$.

Example 3.17. If C is an algebraically closed field of characteristic p and S is a transcendence basis of $C/\mathbf{F}_p$ then $C = \overline{\mathbf{F}_p(S)}$.

Remark 3.18. A transcendence basis S for L/K such that the algebraic extension $L/K(S)$ is separable is called a *separating transcendence basis*. When K is perfect, every finitely generated extension field of K has a separating transcendence basis over K. We will not use this concept here.

Theorem 3.19. *If C is an algebraically closed field and K is a subfield then every automorphism of K can be extended to an automorphism of C.*

This is not Corollary 1.4, but is more general, since here C is not necessarily the algebraic closure of K. It could be bigger. We will use Corollary 1.4 in the proof of Theorem 3.19.

Proof. Let S be a transcendence basis of C/K, so $C = \overline{K(S)}$. Each field automorphism σ of K extends in a unique way to an automorphism of the polynomial ring $K[S]$ by behaving like σ on K and fixing all the elements of S. (We can think of $K[S]$ as a polynomial ring in S because elements of S are algebraically independent over K.) This automorphism of $K[S]$ extends in a unique way to an automorphism of its fraction field $K(S)$. Since C is an algebraic closure of $K(S)$, by Corollary 1.4 every automorphism of $K(S)$ extends to an automorphism of C. Thus σ extends (usually in many ways) to an automorphism of C. □

Example 3.20. On the field $\mathbf{Q}(\sqrt[4]{2})$ there is a unique automorphism sending $\sqrt[4]{2}$ to $-\sqrt[4]{2}$. Theorem 3.19 tells us there is an automorphism of $\mathbf{C}$ sending $\sqrt[4]{2}$ to $-\sqrt[4]{2}$. In particular, this automorphism of $\mathbf{C}$ is not the identity or complex conjugation since they both fix all real numbers. Similarly, every automorphism of a finite extension of $\mathbf{Q}$ extends (in many ways) to an automorphism of $\mathbf{C}$. It is basically hopeless to expect we can write down formulas on all of $\mathbf{C}$ for automorphisms other than the identity or complex conjugation. The existence of such automorphisms is entirely due to Zorn's lemma.

Our next application of transcendence bases is a surprising result about uncountable algebraically closed fields.

Theorem 3.21. *Two uncountable algebraically closed fields are isomorphic if and only if they have the same characteristic and cardinality.*

For instance, every 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 3.21 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 $\mathbf{Q}$.

To prove Theorem 3.21 we will use the following two lemmas about transcendence bases.

Lemma 3.22. *Let C and C' be algebraically closed fields. Then C is isomorphic to C' if and only if the fields have the same characteristic and the same transcendence degree over their prime subfield ($\mathbf{Q}$ or $\mathbf{F}_p$).*

Proof. Suppose C and C' are isomorphic fields and $f\colon C \to C'$ is an isomorphism. Certainly the characteristics of C and C' are the same. Let F be the common prime subfield of C and C' (either $\mathbf{Q}$ or $\mathbf{F}_p$). Then f is the identity map on F. For a transcendence

basis S of C/F, check that its image $f(S)$ is a transcendence basis for C'/F. Therefore $\mathrm{tr.deg}(C/F) = \mathrm{card}\, S = \mathrm{tr.deg}(C'/F)$.

Conversely, suppose C and C' have the same characteristic and the same transcendence degree over their common prime subfield F. Let S be a transcendence basis for C/F and S' be a transcendence basis for C'/F, so by hypothesis S and S' have the same cardinality: there is a bijection $S \to S'$. This bijection extends uniquely to a ring isomorphism $F[S] \to F[S']$ (fixing the elements of F), which extends uniquely to a field isomorphism of fraction fields $F(S) \to F(S')$. By Corollary 1.4, the field isomorphism $F(S) \to F(S')$ extends (by Zorn's lemma, so in many ways) to a field isomorphism of the algebraic closures, which are C and C'. □

This lemma tells us that an algebraically closed field is determined up to isomorphism by its characteristic and its transcendence degree over its prime subfield. Computing the transcendence degree of a field extension might seem formidable: what are $\mathrm{tr.deg}(\mathbf{R}/\mathbf{Q})$ or $\mathrm{tr.deg}(\mathbf{C}/\mathbf{Q})$?

Lemma 3.23. *Let F be a field that is finite or countably infinite and $\{X_i\}_{i\in I}$ be an infinite set of algebraically independent indeterminates over F. The cardinality of $F(\{X_i\}_{i\in I})$ equals* $\mathrm{card}\, I$.

Proof. We will prove the polynomial ring $R := F[\{X_i\}_{i\in I}]$ has cardinality $\mathrm{card}\, I$. That suffices, since every infinite integral domain has the same cardinality as its fraction field.

In R, the set of powers $X_i^{m_i}$ with $m_i \geq 1$ is in bijection with $\mathbf{Z}^+ \times I$, which is in bijection with I since I is infinite. The set of pure monomials $X_{i_1}^{m_1} \cdots X_{i_k}^{m_k}$ (coefficient is 1, exponents are ≥ 1) is in bijection with the set $\mathcal{F}$ of finite subsets of $\mathbf{Z}^+ \times I$ by sending each finite subset to the product of the corresponding powers (send $\emptyset$ to 1). The set of finite subsets of an infinite set $\mathcal{S}$ has the same cardinality as $\mathcal{S}$, so $\mathrm{card}\, \mathcal{F} = \mathrm{card}(\mathbf{Z}^+ \times I) = \mathrm{card}\, I$. The set $\mathcal{M}$ of all monomials in R (allowing arbitrary coefficients from F) is in bijection with $F \times \mathcal{F}$, so $\mathrm{card}\, \mathcal{M} = \mathrm{card}(F \times \mathcal{F}) = \mathrm{card}(F \times I)$.

Let E_n be the set of elements of R that are a sum of *at most* n monomials, so $E_n \subset E_{n+1}$ and $R = \bigcup_{n\geq 1} E_n$. Addition of polynomials gives us a surjection $\mathcal{M}^n \to E_n$, so $\mathrm{card}(E_n) \leq \mathrm{card}(\mathcal{M}^n)$. Since $\mathcal{M}$ is infinite, $\mathrm{card}(\mathcal{M}^n) = \mathrm{card}\, \mathcal{M} = \mathrm{card}(F \times I)$. Therefore R is a countable union of sets E_n that each have cardinality $\leq \mathrm{card}(F \times I)$, so $\mathrm{card}\, R \leq \mathrm{card}(F \times I)$.

Up to now we have not used the fact that F is finite or countably infinite. Now we use that: it tells us $\mathrm{card}(F \times I) = \mathrm{card}\, I$. Therefore $\mathrm{card}\, R \leq \mathrm{card}\, I$. Since R contains $\{X_i\}_{i\in I}$, $\mathrm{card}\, R \geq \mathrm{card}\, I$, so the Schroeder–Bernstein theorem tells us $\mathrm{card}\, R = \mathrm{card}\, I$. □

Now we can prove Theorem 3.21.

Proof. Let C be an algebraically closed field. By Lemma 3.22, C is determined up to isomorphism by its characteristic and its transcendence degree over its prime subfield F. We will show when C is uncountable that $\mathrm{tr.deg}(C/F) = \mathrm{card}\, C$, so C is determined up to isomorphism by its characteristic and cardinality.

Let S be a transcendence basis of C/F, so $C = \overline{F(S)}$. Since C is uncountable, S has to be infinite: if S were finite then, since F is finite or countable, an algebraic closure of $F(S)$ would be countable. By definition, $\mathrm{tr.deg}(C/F) = \mathrm{card}\, S$. Lemma 3.23 tells us $\mathrm{card}\, S = \mathrm{card}(F(S))$. Since $F(S)$ is infinite and $C/F(S)$ is algebraic, $\mathrm{card}\, C = \mathrm{card}\, F(S)$. Thus $\mathrm{card}\, C = \mathrm{card}\, S = \mathrm{tr.deg}(C/F)$. □

The proof of Theorem 3.21 used the fact that C is algebraically closed in its appeal to Lemma 3.22 and nowhere else. Therefore the reasoning in the proof shows that if L is an arbitrary uncountable field with prime subfield F, $\mathrm{tr.deg}(L/F) = \mathrm{card}\, L$.

Example 3.24. The extensions $\mathbf{C}/\mathbf{Q}$ and $\mathbf{R}/\mathbf{Q}$ have transcendence degree equal the cardinality of the continuum.

4. More extension problems using Zorn's lemma

Zorn's lemma is the standard method used to extend functions to a field when starting with a function on a subset of the field. This has been done so far with field homomorphisms. Here we describe two other kinds of functions that occur in field theory: derivations and absolute values. Motivation for interest in these concepts comes from commutative algebra, algebraic geometry, and number theory.

Example 4.1. For a field extension L/K, a *derivation* $d\colon K \to L$ is a mapping such that (i) $d(x+y) = d(x) + d(y)$ and (ii) $d(xy) = xd(y) + yd(x)$. This can be regarded as an abstract version of differentiation. For instance, differentiation with respect to u on the rational function field $F(u)$ is a derivation $F(u) \to F(u)$. The zero function on a field is also a derivation (it's the only derivation on $\mathbf{Q}$).

If L/K is a separable algebraic field extension, possibly of infinite degree, then every derivation $K \to L$ extends uniquely to a derivation $L \to L$. The proof of this reduces, by Zorn's lemma, to the case when $L = K(\alpha)$ is a finite separable extension [3, Cor. 2.4, Chap. 4].

Example 4.2. An *absolute value* on a field F is a function $|\cdot|\colon F \to \mathbf{R}$ such that (i) $|x| \geq 0$ for all $x \in F$, with equality if and only if $x = 0$, (ii) $|xy| = |x||y|$, and (iii) $|x+y| \leq |x| + |y|$. When (iii) is replaced by the more restrictive condition $|x+y| \leq \max(|x|, |y|)$, the absolute value $|\cdot|$ is called non-Archimedean. (The terminology "non-Archimedean" come from the condition $|x| < |y|$ not implying there is an integer n such that $|nx| > |y|$, which is the Archimedean property of the real numbers.)

Krull's theorem about the extension of absolute values says that for every field extension L/K, a non-archimedean absolute value on a field K can be extended (generally not uniquely) to a non-archimedean absolute value on L. By Zorn's lemma, the proof of this reduces to the case of a simple extension $L = K(t)$, and then the cases when t is algebraic over K or transcendental over K are treated separately [8, pp. 36–39]. For an alternate proof of Krull's theorem using Zorn's lemma, see [6, 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] G. Karpilovsky, "Topics in Field Theory," North-Holland, 1989.
[4] S. Lang, "Algebra," 3rd revised ed., Springer-Verlag, New York, 2002.
[5] M. R. Murty and P. Rath, "Transdencental Numbers," Springer-Verlag, New York, 2014.
[6] P. Ribenboim, "The Theory of Classical Valuations," Springer-Verlag, New York, 1999.
[7] J. Rotman, "Advanced Modern Algebra," Prentice-Hall, Upper Saddle River, NJ, 2002.
[8] W. Schikhof, "Ultrametric calculus: an introduction to p-adic analysis," Cambridge Univ. Press, Cambridge, 1984.