10. Algebraic closure

Definition 10.1. *Let K be a field. The* ***algebraic closure*** *of K, denoted $\bar{K}$, is an algebraic field extension L/K such that every polynomial in $K[x]$ splits in L.*

We say that K is ***algebraically closed*** *if $K = \bar{K}$.*

Lemma 10.2. *Let L/K be an extension of fields.*

TFAE

(1) L/K is algebraic and L is algebraically closed.
(2) $L = \bar{K}$ is an algebraic closure of K.
(3) L/K is algebraic and for every finite extension N/L, $N = L$.

Proof. (1) clearly implies (2).

Suppose that (2) holds. Let N/L be a finite extension. Passing to a normal closure, we may as well assume that N/L is a splitting field for $f(x) \in L[x]$. Let $L/M/K$ be the intermediary field generated by the coefficients of $f(x)$. Then $f(x) \in M[x]$.

As $f(x)$ splits in N, we may find an intermediary field $N/N'/M$ which is a splitting field for $f(x)$ over M. As $M \subset L$ and L/K is algebraic, M/K is algebraic. As it is also finitely generated, M/K is finite. Similarly for N'/M. By the tower law N'/K is finite. Pick $\alpha \in N'$. Then α is algebraic over K. Let $m(x) \in K[x]$ be the minimum polynomial of α. By assumption $m(x)$ splits in L. As α is a root of $m(x)$, and $m(x)$ splits in L, it follows that $\alpha \in L$. But then $N' \subset L$. But then $N = L$, as we have shown that $f(x)$ splits in L. Hence (3).

Now suppose that (3) holds. Let $f(x) \in L[x]$. We have to show that $f(x)$ splits in L. Let N/L be a splitting field for $f(x)$. Then N/L is finite. But then $N = L$, and $f(x)$ splits in L. □

We now turn to the proof of existence and uniqueness. Unfortunately to prove either of these, we need to confront a highly non-trivial logical issue.

Axiom 10.3 (Axiom of Choice)**.** *For every set x, which does not contain the empty set, we may find a set y and a function $f\colon x \longrightarrow y$ such that*

$$f(z) \in z,$$

for every $z \in x$.

In other words, the axiom of choice states that given a collection of sets x (for example $x = \{A_i \mid i \in I\}$) for every element z of x, we may pick an element $f(z)$ of z (for the example in brackets, we would have $a_i \in A_i$). Note that if the set x is finite, there is no issue here at all. The problem is when x is a very big set (equivalently the indexing

set I is very big), since in this case we are supposed to be making infinitely many choices. In fact there could be a problem, even when every element of x has only finitely many elements.

There are many axioms in set theory, all of which are equivalent to the axiom of choice.

Definition 10.4. *Let $(x, <)$ be a total order. We say that x is **well-ordered** if every subset of x has a smallest element.*

A classic example of a well-ordered set is the set of natural numbers, under the natural ordering.

Axiom 10.5 (Well-Ordering Principle)**.** *For every set x, we may find a total ordering of the elements of x such that the resulting order is a well-ordering.*

For example, the well-ordering principle states that the real numbers can be well-ordered. Clearly the usual ordering is not a well-ordering.

One of the most useful equivalent ways to state the axiom of choice is the following:

Axiom 10.6 (Zorn's Lemma)**.** *Let $(P, <)$ be a partially ordered set.*

Suppose that for every totally ordered subset Q of P we may find an element b of P such that $a \leq b$, for all $a \in Q$.

Then P has an element m which is not smaller than any other element.

The element m is sometimes called a maximal element. Note that m does not have the property that it is bigger than every other element of P, just that if we can compare m with another element n, then $n \leq m$.

Here are some other equivalent formulations of the axiom of choice.

Axiom 10.7 (Tychonov's Theorem)**.** *The product of compact topological spaces is compact.*

The issue with Tychonov's Theorem, as with the axiom of choice, is that no restriction on the number of factors in the product is given.

Axiom 10.8. *Every vector space has a basis.*

Axiom 10.9. *Every ring has a maximal ideal.*

Axiom 10.10. *Every field has an algebraic closure.*

Let us practice using Zorn's Lemma, with some baby applications.

Lemma 10.11. *Let R be a ring and let I be an ideal, $I \neq R$.*

Zorn's Lemma implies that R contains a maximal ideal which contains I.

Proof. Let P be the partically ordered set of all ideals, not equal to R, that contain I, with the order given by inclusion. We want to apply Zorn's Lemma.

Let Q be a totally ordered subset of P. Let J be the union of all the elements of Q. I claim that J is an ideal of R, which contains I. Clearly J contains I and so it is definitely non-empty. We have to prove that J is closed under addition and scalar multiplication.

Pick a and $b \in J$. Then there are K and L in Q with $a \in K$ and $b \in L$. As Q is totally ordered, possibly switching K and L, $K \subset L$ and so we may assume that a and $b \in L$. In this case $a + b \in L$ and so $a + b \in J$. Similarly $ra \in L$, for all $r \in R$, so that $ra \in J$. On the other hand, note that $1 \notin J$. Thus $J \in P$ and J dominates every element of Q.

By Zorn's Lemma P contains a maximal element, call it M. Then M is a maximal ideal which contains I. □

Lemma 10.12. *Zorn's Lemma implies that every vector space has a basis.*

Proof. Let V be a vector space over a field F. Let P denote the subset of the power set of V, consisting of all independent subsets of V. The relation on V is the natural one given by inclusion.

To apply Zorn's Lemma, we need to check that every totally ordered subset Q of P is dominated by an element of P. Given a totally ordered subset Q of P, set

$$B = \bigcup_{C \in Q} C.$$

Clearly $C \subset B$, for every $C \in Q$. Suppose that we may find $v_1, v_2, \ldots, v_n \in B$ and $a_1, a_2, \ldots, a_n \in F$, such that

$$\sum a_i v_i = 0.$$

For every i, there is a $C_i \in Q$, such that $v_i \in B_{k_i}$. As Q is well-ordered the maximum C of the C_i exists. Then $v_i \in C$. As C is a collection of independent vectors, we have $a_i = 0$, for all i. But then B is a collection of independent vectors, that is, $B \in P$.

As every totally ordered subset in P is dominated by an element of P, by Zorn's Lemma, it follows that there is an element B of P such that B is not smaller than any other element of P.

I claim that B is a basis of V. As $B \in P$, B is an independent set. Suppose that $v \in V$. The set $A = B \cup \{v\}$ strictly contains B. As B is maximal in P, A must be a dependent set, so that v must be a linear combination of the elements of B. Thus B spans V, and B is a basis of V. □

We now show that the axiom of choice, Zorn's Lemma and the well-ordering principle are equivalent.

Theorem 10.13. *TFAE*

(1) Well-ordering principle.
(2) Axiom of Choice.
(3) Zorn's Lemma.

Proof. Suppose that the well-ordering principle holds. Let x be a set and let y be the disjoint union of the elements of x. Well-order the elements of y. Then every element z of x is a subset of y and we define a function

$$f\colon x \longrightarrow y$$

by the simple prescription, $f(z)$ is the smallest element of z. Thus (1) implies (2).

Suppose that (2) holds. Let $(P, <)$ be a partially ordered set, in which every totally-ordered subset is dominated by an element of P. Suppose there is no maximal element of P, so that given $p \in P$ the set

$$\{\, q \in P \,|\, p < q \,\}$$

is non-empty. By the axiom of choice, there is a function

$$f\colon P \longrightarrow P \qquad \text{such that} \qquad p < f(p).$$

Now let $\mathfrak{C}$ be the set of all chains of subsets of P. By the axiom of choice there is a function

$$g\colon \mathfrak{C} \longrightarrow P$$

such that $g(C)$ is at least as big as every element of the chain $C \in \mathfrak{C}$.

Define a function h from the class of ordinals to P recursively as follows. We send 0, the empty-set, to any element p of P. If $\beta = \alpha^+$ is a successor ordinal then we define

$$h(\beta) = f(h(\alpha)).$$

If λ is a limit ordinal then

$$C = \{\, h(\alpha) \,|\, \alpha \in \lambda \,\}$$

is a chain. We define

$$h(\lambda) = f(g(C)).$$

By construction h is injective, which is a contradiction as the class of ordinals is not a set and P is a set. Thus (2) implies (3).

Finally suppose that Zorn's Lemma holds. Let x be any set. Let P be the set of all well-orderings induced on a subset y of x (note that P is a subset of the power set of x Cartesian product the power set of the Cartesian product of x with itself). Define a relation $<$ on P, if given

two elements $a_1 = (y_1, r_1)$, $a_2 = (y_2, r_2)$, we say that $a_1 < a_2$ if y_1 is a subset of y_2, the well-ordering r_2 extends r_1 and under this ordering, every element of y_1 is less than every element of y_2.

Let Q be a totally ordered subset of P. Define an element $b = (y, r) \in P$ as follows. Let y be the union of all the subsets y', where for some r', $(y', r') \in Q$.

Given l_1 and $l_2 \in y$, there exists y_1 and y_2 in Q such that $l_i \in y_i$. As Q is well-ordered, we may suppose that $y_1 \subset y_2$. Thus we may put l_1 and l_2 in the same order in y, as they are in y_2. It is easy to check that r is a well-ordering of y and that if $(y_1, r_1) \in Q$ then $(y_1, r_1) < (b, r)$. Thus b dominates Q.

By Zorn's Lemma, P contains a maximal element $(y, <)$. Suppose $y \neq x$. Let $l \in x - y$. Define an ordering on $y \cup \{l\}$ by decreeing that l is bigger than every element of y. It is clear that this ordering is a well-ordering. In this way we get an element b of P that is bigger than y, a contradiction. Thus (3) implies (1). □

In practice we assume the Axiom of Choice holds, so that we are free to apply Zorn's Lemma.

We now return to the and existence and uniqueness of an algebraic closure. First uniqueness.

Lemma 10.14. *The algebraic closure of a field is unique.*

Proof. Let K be a field and suppose that L_1 and L_2 are two algebraic closures of K. We want to exhibit an isomorphism of L_1 with L_2.

Let P be denote the set of all triples $a = (M_1, M_2, \phi)$, where ϕ is an isomorphism of $M_1 \subset L_1$ with $M_2 \subset L_2$. We say that the triple $a < b = (N_1, N_2, \psi)$ if $M_1 \subset N_1$, $M_2 \subset N_2$ and ψ extends ϕ.

We want to apply Zorn's Lemma. Let Q be a totally ordered subset of P.

Let N_1 be the union of the M_1 and let N_2 be the union of the M_2. Define $\psi\colon N_1 \longrightarrow N_2$ in the obvious way. Given $m \in N_1$, pick $a \in Q$, such that $m \in M_1$. Then set $\psi(m) = \phi(m)$. ψ is well-defined as Q is totally ordered. It is easy to check that ψ is an automorphism. Thus Q is dominated by the triple (N_1, N_2, ψ).

By Zorn's Lemma, there is a maximal triple a. Suppose that $M_1 \neq L_1$. Pick $\alpha \in L_1 - M_1$. Let $N_1 = M_1(\alpha)$. Let $m(x)$ be the minimum polynomial of α over K. Then $m(x)$ splits in L_2. Pick $\beta \in L_2$ a root of $m(x)$. Then we may extend ϕ to $\psi\colon N_1 \longrightarrow N_2 = M_2(\beta)$, a contradiction. □

A similar proof ought to work to establish existence. However there are some subtleties. Here is one way to proceed.

Lemma 10.15. *Let K be a field and let L be an algebraic extension.*

If K is finite then L is countable. If K is infinite then the cardinality of L is the cardinality of K.

Proof. The elements of L are a disjoint union of the zeroes of some set of irreducible polynomials of K. If one fixes the degree d of a polynomial then the number of polynomials of that degree is at most the cardinality of K raised to the power $d+1$, which is either finite, or the cardinality of K. But the countable union of countable (respectively infinite cardinality κ) sets is countable (respectively cardinality κ) (by the axiom of choice!). □

Lemma 10.16. *The algebraic closure of a field exists.*

Proof. Let K be a field. If K is finite, then let E be any countable set. Otherwise let $E = K$. Note that the collection P' of all field structures on all subsets of E is naturally a set (indeed note that the operations of addition, inverses and multiplication are all functions on the given subset of E). We will abuse notation and identify an element of P' with the corresponding field. There is a natural order on P', given by field extension. If A and B belong to P', we say that $A < B$, if B/A is a field extension. Fix an element K' of P' which is isomorphic to K and let P be subset of P' consisting of all fields that contain this copy K' of K and which are algebraic over K'.

The key point, is that given any algebraic extension L/K, we may find $L' \in P$ such that the corresponding extension L'/K' is isomorphic to L/K. Indeed the only thing we need to do is observe that the cardinality of L' is at most the cardinality of E.

By a now standard argument, it is clear that given a chain Q in P, we may find an element L/K that dominates Q. The union of the corresponding subsets with the induced operations is obviously a field, which dominates every element of Q.

By Zorn's Lemma, it follows that P has a maximal element, call it L. I claim that L is algebraically closed. Suppose not. Then there would be a non-trivial finite extension N/L. By N/K is algebraic, so that N has cardinality the cardinality of K. We may assume that $N \in P$, by reasons of cardinality, so that $L < N$. But this contradicts our choice of L. □