

A Little Bit on Zorn's Lemma (ZL)

Charlie Tang and Benjamin Mason

August 2021

1 Introduction

Zorn's Lemma is one of the most well known statements within set theory. Even a film has been named after this lemma. Over the years Zorn's Lemma has become an integral part of mathematics and is now used in all kinds of proofs of crucial importance. In 1935 Max Zorn, a German born mathematician who later emigrated to the United States, proposed to add the statement that was originally called 'the maximum principle' to the list of standard axioms of set theory. Zorn's Lemma provides a way to simplify the situation by offering a safer passage of just satisfying its requirements and circumventing the more arduous journey of repeating transfinite inductions. To quote the Fields Medalist Sir Timothy Gowers [5]:

'If you are building a mathematical object in stages and find that (i) you have not finished even after infinitely many stages, and (ii) there seems nothing to stop you from continuing to build, then Zorn's Lemma may well be able to help you.'

Even though the statement sounds almost trivial and you might expect that we can just assume things like that, mathematics is all about being clear and precise. You can't just assume things that just sound logical, it must be in accordance with the known axioms and established assumptions. Zorn's Lemma gives us a very precise and structured statement to hold onto. Without further ado, let's look at the formulation of Zorn's Lemma:

Zorn's Lemma (ZL): If S is a nonempty partially ordered set for which all subsets with total ordering have an upper bound, then S has a maximal element.

The lemma has many applications in fields such as algebra, analysis and topology [12]. We shall first start with understanding the lemma itself and explaining some of key words of the statement. Since Zorn's lemma is the topic of this paper it will be mentioned frequently and hence we will often use ZL as an abbreviation.

Definition 1.1. If S is a set with a binary relation acts denoted by $\leq$, then S is a **partially ordered set** if:

1. For all $s \in S$, $s \leq s$ (Reflexive)
2. If $s \leq s'$ and $s' \leq s''$ then $s \leq s''$ (Transitive)
3. If $s \leq s'$ and $s' \leq s$ then $s = s'$

S becomes a **totally ordered set** as soon as:

4. For all $s, s' \in S$, $s \leq s'$ or $s' \leq s$

We now give an example to give you an idea of the definition.

Example 1.2. (Ordering by subgroups) Let S be the set of all subgroups of some group G . For this ordering we define the binary relation by $A \leq B$ if A is a subgroup of B . We know the elements in S are groups and are thus subsets of themselves, satisfying the first property. We also know it is transitive, since if $A \leq B$ and $B \leq C$ then $A \subset C$ and $A \neq \emptyset$. Since for all $a, a' \in A$, $aa'^{-1} \in A$ we have that $aa'^{-1} \in B$ (because every element in A is also contained in B). This means that $aa'^{-1} \in C$ (because every element in B is also contained in C), thus by the subgroup criterion $A \leq C$. Finally we also have for $A, B \in S$ that if $A \leq B$ and $B \leq A$ that $A \subset B$ and $B \subset A$ thus $A = B$, thus S is partially ordered.

It does not however have to be totally ordered. Take as an example S_4 . We know that $\langle(12)\rangle, \langle(12)(34)\rangle \leq S_4$, however $(12) \in \langle(12)\rangle$ and not in $\langle(12)(34)\rangle$ thus $\langle(12)\rangle \not\leq \langle(12)(34)\rangle$. Also $(12)(34) \in \langle(12)(34)\rangle$ while not in $\langle(12)\rangle$ and so it follows that $\langle(12)(34)\rangle \not\leq \langle(12)\rangle$, so that by definition 1.1 S is not generally a total ordering.

Another important term in the lemma is **upper bound**.

Definition 1.3. An **upper bound** on a subset T of a partially ordered set S is an $s \in S$ such that $t \leq s$ for all $t \in T$. Please notice that by this definition s doesn't have to be in T , only in S .

We now give some examples to give you some intuition for the concept.

Example 1.4. Using the example of the ordering by subgroups, if we once again consider S the set of all subsets but on the group S_5 and T to be some subset consisting of all the subgroups of S_4 we find that both S_4 and S_5 are upper bounds of T because subgroups of a group always have the group as an upper bound.

Example 1.5. Let's look at the subgroups of $\mathbb{Z}$ ordered by inclusion. If we have $\{6\mathbb{Z}, 9\mathbb{Z}, 15\mathbb{Z}\}$, then we get the upper bound $3\mathbb{Z}$, since $6\mathbb{Z}, 9\mathbb{Z}, 15\mathbb{Z}$ all consists of numbers which are a multiple of 3. (We now also see why the upper bound doesn't have to be in the subset, as $3\mathbb{Z} \notin \{6\mathbb{Z}, 9\mathbb{Z}, 15\mathbb{Z}\}$.)

The next Lemma is very important and actually a fundamental statement, because it basically says that any finite totally ordered subset of a partially ordered set has an upper bound. This is one of the requirements for Zorn's Lemma, but the Lemma is also used in other proofs concerning infinite sets.

Lemma 1.6. Let S be a partially ordered set. If $\{s_1, \dots, s_n\}$ is a finite totally ordered subset of S then there is an s_i such that $s_j \leq s_i$ for all $j = 1, \dots, n$.

Proof. We are going to give a proof by induction on n . For $n = 1$, the only element in the subset is s_1 , so $s_i = s_1$. It is clear that since this is the only element and $s_i \leq s_i$ holds as it is the first property of the definition of the binary relation $\leq$ (reflexive), the Lemma holds for $n = 1$. Let's now assume that the Lemma holds for all $n = 1, \dots, k$ and in particular for $n = k$. Then the Lemma says that there is an element $s_i \in \{s_1, \dots, s_k\}$ such that $s_j \leq s_i$ for all $j = 1, \dots, k$. Now let's add another element s_{k+1} to this subset, we now see that there are $k + 1$ elements. If $s_k \leq s_i$, then s_i is still the element with the property $s_j \leq s_i$ for all $j = 1, \dots, n$ and the lemma holds for $n = k + 1$. If $s_i \leq s_{k+1}$, then we can make use of the binary relation's third property (transitivity) to get that because $s_j \leq s_i$ for all $j = 1, \dots, k$ and $s_i \leq s_{k+1}$, it follows that $s_j \leq s_{k+1}$ for all $j = 1, \dots, k$. And because $s_{k+1} \leq s_{k+1}$, we get the required element $s_j \leq s_{k+1}$ for all $j = 1, \dots, k + 1$ and the lemma holds for $n = k + 1$. We conclude by induction that the lemma holds for all finite totally ordered subsets $\{s_1, \dots, s_n\}$ for $n \in \mathbb{N}$.

The final piece of the puzzle is **maximal** element.

Definition 1.7. A **maximal** element m of a partially ordered set S is an element such that for all $s \in S$ to which m is comparable, there holds $s \leq m$. Note that this doesn't mean that $s \leq m$

for all $s \in S$, because not every element in S is comparable to m .

Example 1.8. (Maximal subgroups) Examples of maximal elements are the maximal subgroups of S_4 , these elements are maximal in the set S given by the proper subgroups (a group which isn't equal to the group itself) of S_4 , where S is ordered by subgroups as in examples 1.2 and 1.4. An example of a maximal element in S is A_4 we notice that this element is not comparable to all of the smaller subgroups, for example $\langle(1\ 2)\rangle \not\leq A_4$ since $(1\ 2) \notin A_4$.

We now have all the required definitions to understand the statement of Zorn's Lemma. It can now be used as a powerful tool to shorten proofs in algebra. However, the lemma itself is non-constructive. This means that even though you know that there is a maximal element in S , it doesn't tell you how many there are or how to find them. This doesn't deter us from using the lemma, because it can often give you a strong starting point for proving what the maximal element of a set is. We will now give a not so rigorous, but more intuitive example of what Zorn's Lemma can do.

Example 1.9. Let's say you meet a greengrocer who only happens to sell apples and oranges. Since his truck doesn't collapse under the weight of his produce, we may assume that the total weight of his cargo is a finite number. You want to know whether or not he has a fruit that is the heaviest. In this case we have the set of all the fruits as the partially ordered set and the ordering is by weight. Obviously, it would be silly to compare apples and oranges. Thus we have two totally ordered sets, one with all the apples and one with all the oranges, as you can compare apples with apples and oranges with oranges. Because we also know that the total weight of his cargo is a finite number, the total weight of the apples and the total weight of the oranges must be as well. This also means that there must be an upper bound to the weight of an individual apple and an upper bound to the the weight of single orange. By Zorn's Lemma that means there must be a heaviest fruit.

This indeed very strong as even though the weight is finite, the number of apples or oranges does not need to be (even though it would sound more logical). Zorn's Lemma allows us to circumvent the laborious path of comparing each of the possibly infinite amount of fruits to each other individually. However, we also see the non-constructiveness of Zorn's Lemma as we still don't know which one is the so called heaviest fruit, and we don't even know if it is an apple or an orange or there might be one of both types.

If we reverse the meaning of Zorn's Lemma, we get that if every totally ordered subset of a partially ordered set S has a *lower bound* in S , then S contains a *minimal* element. This really isn't that interesting as it comes down to the definition of *partial ordering*. If we reverse the meaning of it, then we get that *lower bounds* become *upper bounds* and *minimal* becomes *maximal*.

To cap it all off, we shall now give an example of why it holds for subgroups of $\mathbb{Z}$.

Example 1.10. We know that all the subgroups of $\mathbb{Z}$ are of the form $m\mathbb{Z}$ with $m \in \{0, 1, 2, \dots\}$. If we look at the subgroups ordered by inclusion, then an upper bound of a totally ordered subset $\{a_1\mathbb{Z}, \dots, a_n\mathbb{Z}\}$ is $\gcd(a_1, \dots, a_n)\mathbb{Z}$. This is because the $\gcd(a_1, \dots, a_n)$ divides all of $a_1, \dots, a_n$ and thus each of $a_1\mathbb{Z}, \dots, a_n\mathbb{Z}$ are contained in $\gcd(a_1, \dots, a_n)\mathbb{Z}$. Zorn's Lemma then states that $\mathbb{Z}$ has a maximal element. In fact, the maximal elements are $p\mathbb{Z}$ for p is prime.

2 History

Zorn's Lemma was proven in 1935 by Max Zorn as a means to simplify proofs in algebra that previously used the well-ordering principle or the axiom of choice (in fact it can be shown that it is equivalent to these two statements as we discuss in another section). The Polish Kazimierz Kuratowski had proven the statement [8] in 1922 (!), even though Zorn proved it independently and would be the one to show its usefulness. Today, in countries like Poland and Russia, the name 'Kuratowski-Zorn lemma' prevails. In "A Remark on Method in Transfinite Algebra" Max Zorn says to have proven Zorn's lemma to simplify the proofs of some theorems on algebraic closure [11]. These proofs tended to use the well-ordering principle which is less algebraic according to Zorn.

For quite a while there has been some controversy related to applying Zorn's lemma in proofs. This is primarily due to its equivalence to the axiom of choice (AOC). The existence of some objects were proven using AOC which didn't seem natural to many mathematicians. Namely, the existence proofs were given without an explicit method for constructing the object, which was not generally accepted at the time. An example of such a result is the proof that $\mathbb{R}$ is well-ordered by Zermelo in 1904. Another result aptly named the Banach-Tarski paradox states that a sphere of radius r split up into 5 parts can be rearranged using a finite number of rigid motions to create a sphere of radius r' [2].

Many similar statements were proven at the time. According to a quote from Suppes, supplied in "The origin of 'Zorn's lemma'" by Paul Campbell [1], names of people who considered similar statements include but are not limited to, Felix Hausdorff, Kazimierz Kuratowski and R.L. Moore. In this same document there is a statement from Zorn in which he attests that the lemma is attributed to many people referring in particular to K. Kuratowski and Claude Chevalley from the Bourbaki group. In fact Zorn remarks that at the time Emil Artin proved that a similar statement to Zorn's lemma implies the axiom of choice, which brings us to the next section: the equivalence of Zorn's lemma to two other statements [1].

3 The Axiom of Choice and The Well Ordering Principle

As we saw earlier Zorn's Lemma was used to simplify the proofs that previously involved the Axiom of Choice or the Well Ordering Principle. This was possible because the three statements are actually equivalent. This means that by assuming one of them holds true, it enables us to also prove the other two. We shall first give a formulation of the Axiom of Choice [10].

The Axiom of Choice: If A is a set, let $\mathcal{P}^\#(A)$ denote the family of all its nonempty subsets. There exists a function $\beta : \mathcal{P}^\#(A) \rightarrow A$ with $\beta(S) \in S$ for every nonempty subset S of A .

To understand the Well Ordering Principle one must first understand what it means if something is *well-ordered*.

Definition 3.1. A partially ordered set X is **well-ordered** if every nonempty subset S of X contains a smallest element. That means that there exists a $s_0 \in S$ with $s_0 \leq s$ for all $s \in S$.

Remark 3.2. Note that a well-ordered set X is totally ordered, namely, for two elements $a, b \in X$, $\emptyset \neq \{a, b\} \subset X$ and thus must have a minimal element, either $a \leq b$ and/or $b \leq a$.

The Well Ordering Principle tells us:

Well Ordering Principle: Every partially ordered nonempty set X has a well-ordering.

This means that you can define an ordering on the set, such that it actually is well-ordered. However, this might have nothing to do with the original partial ordering.

The three are equivalent because as we will see, the Axiom of Choice implies Zorn's Lemma, Zorn's Lemma in turn implies the Well Ordering Principle and the Well Ordering Principle in turn implies the Axiom of Choice. This equivalence is proved in J. Rotman, "Advanced Modern Algebra" [10]. So, if one statement holds true, then you can eventually get the other two as well. However, the implication from the Well Ordering Principle to the Axiom of Choice is much more direct than the other way around.

We will now give the three equivalences, from which follows that these three statements are equivalent.

Theorem 3.3. *The Well Ordering Principle implies the Axiom of Choice.*

Proof. Let's assume the Well Ordering Principle holds for a nonempty set X , this means that for every nonempty subset there exists a smallest element $s_0 \in S$ such that $s_0 \leq s$ for all $s \in S$. We now can define a choice function $\beta : \mathcal{P}^\#(X) \rightarrow X$ such that $\beta(S) = s_0$ for all $S \in \mathcal{P}^\#(X)$. So we basically send every nonempty subset to its smallest element and this function fulfills the requirement for the Axiom of Choice. $\square$

Before we begin to prove the remaining two implications we introduce a couple of definitions and lemmas that aid the proofs.

Definition 3.4. An **open segment** in a well-ordered set $(X, \leq)$ denoted $\text{Seg}(c)$ for some $c \in X$ is defined as follows, $\text{Seg}(c) = \{x \in X : x \leq c\}$.

On the other hand, a **closed segment** is some $A \subset X$ such that

$$A = \{x \in X : x \leq c\}$$

for some $c \in X$. We say that A is **closed** in X precisely when $\forall x \in X, c \in A : x \leq c \implies x \in A$.

Lemma 3.5. Let $(X, \leq)$ be partially ordered and let $\{(A_i, \sqsubseteq)\}_{i \in I}$ be a set of well-ordered sets such that for any S_i, S_j if $S_i \subset S_j$, then $S_i = S_j$ or S_i is an open segment in S_j . Then it holds that $\bigcup_{i \in I} A_i$ is a well-ordered subset of X .

Proof. We refer the reader to the proof given in "Advanced Modern Algebra" (by J. Rotman) in the appendix lemma A.6 [10]. $\square$

Lemma 3.6. Let $(X, \leq)$ be a well-ordered set, then for some segment $A \subset X$, $A \leq X$ if and only if A is closed in X . A is closed in X if $A = X$ or A is a segment in X .

Proof. We once again refer the reader to the proof given in "Advanced Modern Algebra" (by J. Rotman) in the appendix lemma A.5 [10]. $\square$

For the next proof we give a very similar approach as given by J. Rotman in "Advanced Modern Algebra", which in itself was inspired by Daniel Grayson's proof [6].

Theorem 3.7. *Axiom of Choice $\implies$ Zorn's Lemma*

Proof. This shall be done with a proof by contradiction. Let's assume that the Axiom of Choice holds true for a nonempty partially ordered set X , and that Zorn's Lemma does not hold true. This means that for a nonempty partially ordered X for which all totally ordered subsets are upper bounded, X has no maximal elements. For each nonempty well ordered subset A of X , there is an upper bound $x \in X$ such that $x \notin A$. If not, then the only upper bound lies in A , let's call this element y_0 , and by the well ordering of this subset y_0 would be a maximal element in A . We now prove that y_0 is also a maximal element in X . If this is not the case, then there is another element y in X such that $y_0 \leq y$. By definition $y \notin A$ and y is an upper bound of A . This is in contradiction with the fact that the only upper bound of A lies in A . This means that y_0 is indeed a maximal element in X and this is in turn in contradiction with our assumption that X has no maximal elements and Zorn's Lemma does not hold true. We now conclude that for each nonempty well ordered subset A of X , there is an upper bound $x \in X$ such that $x \notin A$. Thus every nonempty subset has a upper bound outside the subset itself. We now define S as the family of well-ordered subsets of X and $U_A = \{\text{all upper bounds } u \text{ of } A \text{ and } u \notin A\}$. Since we know that $U_A \neq \emptyset$, we can use the Axiom of Choice to get that there exists a function $g : S \rightarrow X$ such that $g(A) \notin A$ is the upperbound of A . We now call a well-ordered subset B of X a g -set if $b = g(B \cap \text{Seg}(b))$ and $b_0 = g(\emptyset) \in B$ for all $b \in B$. This means that every element in the chain B is the upper bound of its open segment in B .

We now are going to show that the union of all g -sets is also a g -set. Then we can use the fact that this union has a upper bound outside the union. This upper bound will be a g -set by definition, so that the union of all g -sets and this upper bound is also a g -set. This means that you can always find a larger union. This will provide the contradiction needed for our proof.

Let C and D be g -sets, then we claim that either $C \leq D$ or $C \geq D$. Let W be the union of all subsets $B \subseteq X$ with $B \leq C$ and $B \leq D$. The union of closed subsets is also closed, that means that $W \leq C$ and $W \leq D$. (This is well-known fact and has a straightforward proof: take $c \in C$ and $w \in W$ such that $c \leq w$, then we know that w lies in some subset B of W . Since B is closed in C , we get that $c \in B$ and thus $c \in W$ and the same goes for D .) If $W = C$ or $W = D$, then we indeed get either $C \leq D$ or $C \geq D$ and we are done. So now assume $W < C$ or $W < D$.

Because C is a g -set and $W < C$, we know that $W = \{c' | c' < c\}$ for at least one element $c \in C$ and we see that $c = g(C \cap \text{Seg}(W)) = g(W)$. The same goes for D and we get that $d = g(D \cap \text{Seg}(W)) = g(W) = c$ for some element $d \in D$. But now we can take $W' = W \cup \{c\}$ and we see that $W' \leq C$ and $W' \leq D$, this is in contradiction to the maximality of W we had assumed since $W < W'$. We now see that there must hold either $W = C$ or $W = D$ and we get the claimed $C \leq D$ or $C \geq D$.

Let U be the union of all g -sets. We now see with our claim that Lemma 3.5 holds and we get that U is a well-ordered subset. We now are going to show that U is also a g -set. If $y \in U$, then there is a g -set Y such that $y \in Y$. Because $Y \leq U$, we get from Lemma 3.6 that Y is closed in U and thus either $U = Y$ or $Y = \text{Seg}(u)$ for some $u \in U$. Either way, we get that $Y \cap \text{Seg}(y) = U \cap \text{Seg}(y)$ and $y = g(U \cap \text{Seg}(y))$ and U is a g -set. We assumed that U is the union of all g -sets and thus also is the largest g -set, but we see that $U' = U \cup \{g(U)\}$ is a larger g -set and we have a contradiction. We conclude that there is no such function g and X must have a maximal element.

□

In the following theorem will present the first detailed application of Zorn's lemma. As we will see proofs involving ZL follow a general format, they generally begin by creating some partially ordered set on which we want to apply ZL. As we shall see, the ordering is often by inclusion. Then we show that all totally ordered subsets have an upper bound (with the proofs we will

be working with this is quite often the union of all elements in the totally ordered subset). We conclude by applying ZL to prove existence of a maximal element in the set, and then (in this document generally by contradiction) we can prove the statement. The set up and the actual use of Zorn's Lemma often comprises the first half of the proof as in the second half you usually want to find out what the maximal element actually is. Thus, even though Zorn's Lemma is used in very different situations, the structure of the proof often look similar.

Theorem 3.8. *Zorn's Lemma $\implies$ Well-Ordering Principle*

Proof. We will prove that some arbitrary set X is well-ordered given that Zorn's lemma holds. If $X = \emptyset$ then it is vacuously well-ordered as it contains no non-empty subsets, thus we may assume $X \neq \emptyset$. Take $S = \{A \subset X : A \text{ is well-ordered}\}$, thus such an element in S takes the form $(A, \sqsubseteq)$ where $\sqsubseteq$ is the well-ordering on A . Since we want S to be partially ordered we want to define some ordering $\leq$, which we define as follows. We say that

$$(A, \sqsubseteq) \leq (A', \sqsubseteq')$$

when either $A = A'$ and $\sqsubseteq = \sqsubseteq'$ or $A \subset A'$ (with A an open segment in A') and for $a, b \in A$ we have that $a \sqsubseteq b \iff a \sqsubseteq' b$.

Now that we constructed this partially-ordered set $(S, \leq)$ we want to prove that all totally ordered subsets $A \subset S$ have upper bounds and thus that Zorn's lemma is applicable. Take a totally ordered subset $N = (\{(A_i, \sqsubseteq)\}_{i \in I}, \leq)$ where I is a set of indices. We claim that an upper bound of this totally ordered subset is $U = \bigcup_{i \in I} A_i$, we take the union rather than finding some maximal element as we do not assume S to be finite. We first show that $U \in S$. We have to show that U is well-ordered. We know by lemma 3.5 that, since for $A_i, A_j : A_i \subset A_j$ in the totally ordered set $A_i = A_j$ or A_i is open in A_j , U must be a well-ordered subset of X , and thus $U \in S$.

To show that U is an upper bound we now need only to show that $A_i \leq U$ for all $i \in I$. We will begin by discussing how the partial ordering on U is constructed such that the orderings of A_i and U coincide for all elements in A_i . Take some $\alpha, \beta \in U$ thus $\exists i, j : \alpha \in A_i, \beta \in A_j$ since these are in a totally ordered set, either $A_i \leq A_j$ or $A_j \leq A_i$. W.l.o.g. we assume $A_i \leq A_j$ thus $A_i \subset A_j$ so $\alpha, \beta \in A_j$, now define the ordering as $\alpha \sqsubseteq \beta$ if $\alpha \sqsubseteq_j \beta$ and vice versa. Now if our ordering is well-defined it should follow quickly that U is partially ordered. Suppose instead that $\alpha \in A_{i'}$ and $\beta \in A_{j'}$ and w.l.o.g. $A_{i'} \leq A_{j'}$, thus now $\alpha \sqsubseteq \beta$ if $\alpha \sqsubseteq_{j'} \beta$. Since we are considering a totally ordered family N either $A_j \leq A_{j'}$ or $A_{j'} \leq A_j$ w.l.o.g. take the prior. Per definition of the binary relation it now follows that either $\sqsubseteq_j = \sqsubseteq_{j'}$ or $a \sqsubseteq_j b \iff a \sqsubseteq_{j'} b$ for $a, b \in A_j$ thus well-defined. Now properties 1 and 3 of partial ordering follow quickly and to show transitivity we make use of the fact that any 3 elements fall under one common set due to the total ordering of N , thus U is partially ordered under our relation. Now we need only to show that A_i is closed in U , and apply lemma 3.6, for U to be a maximal element. Suppose $u \sqsubseteq a$ for $u \in U$ and $a \in A_i$, we know that $u \in A_j$ for some $j \in I$ and out of total ordering of N that either $(A_j, \sqsubseteq_j) \leq (A_i, \sqsubseteq_i)$ or vice versa. In the first case $A_j \subset A_i$ and thus $u \in A_i$. In the latter case, either $A_j = A_i$ or A_j is open in A_i in which case since $u \sqsubseteq a \implies u \sqsubseteq_i a, u \in A_i$. Now according to lemma 3.6 either $A_i = U$ or A_i is open in U . Thus U is an upper bound in N .

The set S satisfies the criteria of Zorn's lemma and thus S must have some maximal element $(M, \sqsubseteq)$. We know that $X \subset M$, assume by contradiction that $x \in X$ and $x \notin M$. Then take the well-ordering $\sqsubseteq'$ on $M \cup \{x\}$, with $m \sqsubseteq' x$ for every $m \in M$. We know that $M = \text{Seg}(x)$ and thus $(M, \sqsubseteq) < (M \cup \{x\}, \sqsubseteq')$, contradiction. We conclude that $M = X$ and thus X is well-ordered. $\square$

In this section we looked into the equivalence between Zorn's lemma (ZL), the Axiom of Choice and the Well-Ordering principle. We saw that in particular Theorems 3.7 and 3.8 were quite advanced with the proof of Theorem 3.8 being the first application of the lemma in this document. These equivalences also allow us to assert the truth of ZL assuming the Axiom of Choice holds. Incidentally, we now have useful machinery that as we will see in the sections below provide us with neat approaches for proving some theorems in group theory, ring theory and algebraic closure.

4 Applications of ZL: Group Theory

In general Zorn's Lemma is used for two reasons. The first is to find the largest possible subset under certain conditions. The second is to show that a function on a subset can be extended to the whole set while preserving certain conditions. In group theory this idea still holds true, but then it is about maximal subgroups instead of largest subsets and homomorphisms instead of general functions. In the following section we shall be exploring the maximal (proper) subgroups.

We have already looked into maximal subgroups during the introduction. But now we give the definition of a maximal subgroup. A subgroup M of a nontrivial group G is a **maximal subgroup** if M is a proper subgroup of G (i.e. $M \neq G$) and there is no subgroup strictly contained between M and G . We now give a simple example about maximal subgroups of $\mathbb{Z}$ (we have already mentioned this during the introduction).

Example 4.1. That the maximal groups of $\mathbb{Z}$ are the subgroups $p\mathbb{Z}$ for prime p . Proper subgroups of $\mathbb{Z}$ are the subgroups of the form $n\mathbb{Z}$ with $n \neq \pm 1$, because we know that all the subgroups of $\mathbb{Z}$ are of the form $n\mathbb{Z}$. Let $n\mathbb{Z}$ be a maximal (proper) subgroup of $\mathbb{Z}$, then we have that there is a prime $p \in \mathbb{N}$ such that $p|n$ and thus $n = pd$ for $d \in \mathbb{Z}$, this means that every element $nm \in \mathbb{Z}$ (which gives $nm = p(dm)$) is also contained in $p\mathbb{Z}$ and because of the maximality of $n\mathbb{Z}$ we get that $n = p$. On the other hand, $p\mathbb{Z}$ is a maximal subgroup of $\mathbb{Z}$ since if $a\mathbb{Z}$ is a subgroup of $\mathbb{Z}$ such that $p\mathbb{Z} \subset a\mathbb{Z} \subset \mathbb{Z}$ then we get that $a|p$ and we get that $a = \pm 1$ or $a = p$. Thus $a\mathbb{Z} = \mathbb{Z}$ or $a\mathbb{Z} = p\mathbb{Z}$.

We are now going to give a useful proposition for proving maximal subgroups.

Proposition 4.2. *If H is a maximal subgroup of G and the index is $|G : H| = p$ for p prime, then H is a maximal subgroup.*

Proof. In the book Dummit and Foote Abstract Algebra book we see in exercise 11 of 3.2 (page 96) that if there is a subgroup K such that $H \leq K \leq G$, then we get that $|G : H| = |G : K| \cdot |K : H| = p$. (Note that G doesn't even need to be finite in this statement.) This means that either $|G : K| = 1$ or $|K : H| = 1$ and we get that $G = K$ or $K = H$ and H is a maximal subgroup. $\square$

We are now going to give two more examples on finite groups.

Example 4.3. In the dihedral group D_8 a maximal subgroup is for example the cyclic subgroup $\langle r \rangle$.

Proof. We know that the subgroup $\langle r \rangle$ has index 2. 2 is obviously a prime number, thus by Proposition 4.2 we get that $\langle r \rangle$ is a maximal subgroup. $\square$

Example 4.4. A maximal subgroup of S_4 is the alternating group A_4 .

Proof. We know that the alternating group A_4 has index 2. 2 is obviously a prime number, thus by Proposition 4.2 we get that the alternating group A_4 is a maximal subgroup. $\square$

In the next example we will be considering the additive group $\mathbb{Q}$. Conrad outlines that $\mathbb{Q}$ has no maximal subgroups, in his document [2] (in the paragraph above Theorem 2.2). But if you leave out the 1, then you can actually find some. We will now prove, using ZL, that there is a maximal subgroup that does not contain 1. We shall first show that the set of subgroups that don't contain 1 actually has maximal elements using Zorn's Lemma. From this important result we can deduce the rest. (This is actually an exercise from the document 'Zorn's Lemma and some applications' by Keith Conrad [2]. We just did the exercise and turned the results into this example.)

Example 4.5. a) Consider the set containing all subgroups of $\mathbb{Q}$ not containing a 1 and partially ordered by inclusion. We denote this set $S = \{H : H \leq \mathbb{Q}, 1 \notin H\}$, and since $\{0\} \in S$, $S \neq \emptyset$ (if 1 can be in H then $\mathbb{Q} \in S$ and so the maximal element of S would be $\mathbb{Q}$ which isn't a proper subgroup of $\mathbb{Q}$). Now take some $I \subset S$, with $I = \{H_j\}_{j \in J}$, that is totally-ordered for inclusion. We will prove that $H := \bigcup_{j \in J} H_j$ is an upper bound in I . First we prove that $H \in S$. It follows that for $i, i' \in H$, there exist $j, j' \in J$ such that $i \in H_j$, $i' \in H_{j'}$. Now out of total ordering of I w.l.o.g. we take $H_j \leq H_{j'}$. Then $i, i' \in H_j$ and since H_j is a group $i - i' \in H_j$ and so $i - i' \in H$. By the subgroup criterion $H \leq \mathbb{Q}$. Now suppose $1 \in H$, then there exists a $j \in J$ such that $1 \in H_j$, contradiction, thus $H \in S$. For any $H_j \in I$ we know that $H_j \subset H$, we conclude that H is an upper bound in I .

Now we can apply ZL to find that S has a maximal element M . Since $M \in S$, $1 \notin M$. Now consider some H with $1 \notin H$ such that $M \subset H \subset \mathbb{Q}$, we know that $H \in S$ so $H \leq M$ thus $H = M$.

Now we actually know that there are maximal subgroups that don't contain 1, we start to wonder how they look like.

Example 4.6. b) Now we show that for this $M \leq \mathbb{Q}$, $M \cap \mathbb{Z} = q\mathbb{Z}$ for some prime q . We begin by showing that $M \cap \mathbb{Z} \neq \{0\}$. Assume to the contrary that $M \cap \mathbb{Z} = \{0\}$, then $M \cap n\mathbb{Z} = \{0\}$ for any $n > 0$, since $0 \in n\mathbb{Z} \subset \mathbb{Z}$ and so $\{0\} = M \cap n\mathbb{Z} = M \cap \mathbb{Z}$. We know that $M + n\mathbb{Z} \leq \mathbb{Q}$ since $M + n\mathbb{Z} \subset \mathbb{Q}$ and for $a, a' \in M + n\mathbb{Z}$ we have $a = m + ni$ and $a' = m' + ni'$ thus $a + a' = m + m' + n(i + i')$ thus since $m + m' \in M$ and $i + i' \in \mathbb{Z}$, $a + a' \in M + n\mathbb{Z}$. We also have that $-a = -m - ni$, and $a - a = 0 \in M + n\mathbb{Z}$, so $M \leq M + n\mathbb{Z}$. If $n\mathbb{Z} \not\subset M$ then assume $1 \in M + n\mathbb{Z}$, then, since $1 \notin n\mathbb{Z} : n > 1$ we have $1 \in M$ or an integer o that is coprime to n is in M , contradiction. Thus then $M \subset M + n\mathbb{Z} \in S$, contradicting maximality of M . So $M \cap \mathbb{Z} \neq \{0\}$. Now we prove $M \cap \mathbb{Z} = q\mathbb{Z}$ for some prime q . We know that $M \cap \mathbb{Z} \subset \mathbb{Q}$, since $0 \in M \cap \mathbb{Z}$, for $a, a' \in M \cap \mathbb{Z}$ we have $a, a' \in M$ so $a - a' \in M$ and $a, a' \in \mathbb{Z}$ so $a - a' \in \mathbb{Z}$ thus $a - a' \in M \cap \mathbb{Z}$. Since $M \cap \mathbb{Z} \subset \mathbb{Z}$, thus $M \cap \mathbb{Z}$ is subgroup of $\mathbb{Z}$. We deduce that $M \cap \mathbb{Z}$ is of the form $n\mathbb{Z}$ for some $n \in \mathbb{Z}_{\geq 0}$ thus $M \cap \mathbb{Z} \subset q\mathbb{Z}$ for some prime q . Because $q\mathbb{Z}$ are the maximal subgroups of $\mathbb{Z}$. We know from earlier that $M \subset M + q\mathbb{Z} \leq \mathbb{Q}$. Assume $1 \in M + q\mathbb{Z}$, then there exists an $i \in \mathbb{Z}$ and an $m \in M$ so that $1 = m + qi$. So then, $m = 1 - qi$ must be in $\mathbb{Z}$ and q can't divide m , however $M \cap \mathbb{Z} \subset q\mathbb{Z}$, contradiction. So $M + q\mathbb{Z}$ is in S thus if $M \cap \mathbb{Z} \neq q\mathbb{Z}$, M is not maximal since then we have a larger element $M + q\mathbb{Z}$. Thus there exists a prime q such that $M \cap \mathbb{Z} = q\mathbb{Z}$.

c) Now we are first going to show that numerator of each fraction is divisible by q from b). Assume the contrary, that the numerator a of $\frac{a}{b} \in M$ is not divisible by q . We may assume that since $a, b \in \mathbb{Z}$, $\gcd(a, b) = 1$ and $b \neq 0$. Then we have that $a \notin q\mathbb{Z}$. But because the subgroup M is closed under the group action addition, we get that by adding $\frac{a}{b}$ b times that

$\frac{a}{b} + \dots + \frac{a}{b} = \frac{ab}{b} = a \in M \cap \mathbb{Z} = q\mathbb{Z}$. This is a contradiction, thus the numerator is divisible by q .

d) Let $H_q = \{a/b : a, b \in \mathbb{Z}, q|a, q \nmid b\}$, we now prove that this is a subgroup of $\mathbb{Q}$. We have that $0 \in H_q$ since $q|0$ and thus $H_q \neq \emptyset$. If $\frac{a_1}{b_1}, \frac{a_2}{b_2} \in H_q$, then we have that $q|a_1, q|a_2$ and b_1 and b_2 are not divisible by q . Because q is prime, we know that b_1b_2 is also not divisible by q . Furthermore, $a_1b_2 - a_2b_1 \equiv 0b_2 - 0b_1 = 0 \pmod{q}$ and we have $q|a_1b_2 - a_2b_1$. Thus we have that

$$\frac{a_1}{b_1} \left(\frac{a_2}{b_2} \right)^{-1} = \frac{a_1}{b_1} - \frac{a_2}{b_2} = \frac{a_1b_2 - a_2b_1}{b_1b_2} \in H_q$$

We see that H_q is a subgroup of $\mathbb{Q}$.

We now prove that $H_q \cap \mathbb{Z} = q\mathbb{Z}$. We know that $0 \in H_q$ and $0 \in \mathbb{Z}$, thus $0 \in H_q \cap \mathbb{Z}$ and it is not empty. If $x, y \in H_q \cap \mathbb{Z}$ then $x, y \in H_q$ and $x, y \in \mathbb{Z}$. We know that H_q and $\mathbb{Z}$ are (sub)groups, thus we know that $xy^{-1} \in H_q$ and $xy^{-1} \in \mathbb{Z}$ and this gives $xy^{-1} \in H_q \cap \mathbb{Z}$. Thus $H_q \cap \mathbb{Z}$ is a subgroup in $\mathbb{Z}$. We know that all the subgroups of $\mathbb{Z}$ are of the form $n\mathbb{Z}$ for $n \in \mathbb{Z}$ and the maximal subgroups of $\mathbb{Z}$ are of the form $p\mathbb{Z}$ for p is prime. We know that $1 \notin H_q$, because otherwise you get that $\frac{a}{b} = 1$ and $a = b$, which gives $q|a$ and $q|b$ in contradiction to the description of H_q . This means that $1 \notin H_q \cap \mathbb{Z}$ and we have that $H_q \cap \mathbb{Z} \neq \mathbb{Z}$. This gives us the fact that $H_q \cap \mathbb{Z} = n\mathbb{Z}$ for $n \neq \pm 1$ and because we know that $q \in H_q \cap \mathbb{Z} = n\mathbb{Z}$, we get that $n|q$ and thus $n = q$. This gives us the much wanted $H_q \cap \mathbb{Z} = q\mathbb{Z}$. We know that $M \subset H_q \subset \mathbb{Q}$ and $1 \notin H_q$, from a) follows that $M = H_q$ and H_q is a maximal subgroup.

Therefore by c), the maximal subgroups in a) are the subgroups $H_q = \{a/b : a, b \in \mathbb{Z}, p|a, p \nmid b\}$. We would now like to give an example of a proper subgroup in $\mathbb{Q}$ (that does contain 1) that contains H_q .

Example 4.7. e) An example of a proper subgroup of $\mathbb{Q}$ containing H_q is the subgroup $G = \{\frac{a}{b} \in \mathbb{Q} : a, b \in \mathbb{Z}, q \nmid b\}$. We now prove that this is indeed a subgroup of $\mathbb{Q}$. We have that $1 \in G$ and G is not empty. If $\frac{a_1}{b_1}, \frac{a_2}{b_2} \in G$, then we have that $q \nmid b_1$ and $q \nmid b_2$. Because q is prime, we know that b_1b_2 is also not divisible by q . And obviously $a_1b_2 - a_2b_1, b_1b_2 \in \mathbb{Z}$. Thus we have that

$$\frac{a_1}{b_1} \left(\frac{a_2}{b_2} \right)^{-1} h = \frac{a_1}{b_1} - \frac{a_2}{b_2} = \frac{a_1b_2 - a_2b_1}{b_1b_2} \in G$$

We see that G is a subgroup of $\mathbb{Q}$. G contains H_q because it is the same subgroup except it has one less condition (that $q|a$).

We now use Zorn's lemma to prove the existence of a maximal subgroup in every finitely generated group that contains a proper subgroup, we took the proof from "Zorn's lemma and some applications" by Keith Conrad [2].

Theorem 4.8. Let $\{0\} \neq G = \langle g_1, g_2, \dots, g_n \rangle$ for some finite set of generators $g_1, \dots, g_n$. Then every proper subgroup of G is a subset of some maximal subgroup in G .

Proof. Suppose G' is some proper subgroup of G . Define $G_j := \langle G', g_1, \dots, g_j \rangle$ for $0 \leq j \leq n$ and let $l \in \mathbb{Z}_{\geq 0}$ be the largest index so that $G_l \subsetneq G$ and $G_{l+1} = G$. We cannot choose $l = n - 1$, although this may seem logical, since G' is arbitrarily generated (take for example $G' = \langle g_n \rangle$, this would not work with this alternative choice of l). In consequence, $G_{l+1} = \langle G_l, g_{l+1} \rangle$.

Define $S = \{H : H \not\subseteq G, G_l \subset H, g_{l+1} \notin H\}$. We want to show that every totally ordered $I \subset S$ has an upper bound. Let $I = \{H_j\}_{j \in J}$ be an arbitrary totally ordered subset of S . We claim $H = \bigcup_{j \in J} H_j$ is an upper bound of I . For $h, h' \in H$ there exist some $j, j' \in J$ such that $h \in H_j$

and $h' \in H_{j'}$. Since I is totally ordered w.l.o.g. $H_j \subset H_{j'}$ and thus $h, h' \in H_{j'}$ so $hh'^{-1} \in H_j$ and $G_l \subset H$ so $H \neq \emptyset$ so since $hh'^{-1} \in H_{j'} \subset H$, $H \leq G$. Now assume $g_{l+1} \in H$ then there is some $j \in J$ for which $g_{l+1} \in H_j$, however $H_j \in S$, contradiction. Now we have shown that H meets all conditions of S hence $H \in S$. Finally take some $i \in I$, we know that $i = H_j$ for some index $j \in J$ and that $H_j \subset \bigcup_{j \in J} H_j = H$ consequently H is an upper bound. By ZL it follows that S has some maximal element M . We know that $M \in S$ therefore $M \leq G$ and $G_l \subset M$ so by transitivity of inclusion $G' \subset M$. Suppose there is an H so that $M \leq H \leq G$, then $H \notin S$ (otherwise contradiction due to maximality of M). Since $M \leq H$, $G_l \subset H$ and also $H \leq G$; therefore by elimination we must have that $g_{l+1} \in H$ as it satisfies the other two conditions of S . Consequently implying that $H = \langle g_{l+1}, H \rangle \supset \langle g_{l+1}, G_l \rangle = G_{l+1} = G$, also a contradiction. Hence M is in fact a maximal subgroup in G . $\square$

Remark 4.9. ZL is only really interesting in the proof of Theorem 4.8 when the group is infinite. If the group were finite we would be able to approach the proof in a much simpler way. We know that $|G| < \infty$ and take some arbitrary $G' \leq G$. If G' is not a maximal subgroup, then there is some $G' \leq G_1 \leq G$, if G_1 is also not a maximal subgroup we can find a G_2 and so continue the chain. Since these groups are not equal to one another they increase in order. Yet since G is a finite group we know this chain must stop at some point, and thus there exists an $n \in \mathbb{Z}^+$ for which $G_n \leq G$ is a maximal subgroup.

In Remark 4.9 we see how Theorem 4.8 can be proven for a finite group G . The sketch we provide uses ideas similar to those used in the theorem and it is interesting to see how ZL can extend this proof 'infinitely' to find the maximal subgroup for infinite groups.

It is because the generators do not necessarily have to be of finite order that this proof is not possible by induction and so makes ZL a practical alternative. A known alternative of the proof is using transfinite induction which is a stronger version of induction for well-ordered sets (this topic extends beyond the scope of this essay for more information on the topic see https://en.wikipedia.org/wiki/Transfinite_induction). This alternative proof does not make use of ZL. The proof was explained in 'Some Remarks on Infinite Groups' by B.H. Neumann [9] (from 1937!). Theorem 4.8 is a useful theorem and we shall now consider three short examples of how it can be applied in group theory.

Example 4.10. We once again can look into the most simple example, namely that of $(\mathbb{Z}, +)$. It has one generator (and thus a finite amount of generators), namely 1. So by Theorem 4.8 we get that every proper subgroup is contained in a maximal subgroup. This is obviously the case as every subgroup $n\mathbb{Z}$ is contained in a maximal subgroup $p\mathbb{Z}$ for p a prime factor of n .

Example 4.11. (Existence of maximal subgroups in S_n) An alternative way of showing existence of a maximal in some group is by using theorem 4.8. Consider the finite symmetric group S_n , $n > 2$. We know that S_n is generated by the set of transpositions since for $\sigma \in S_n$ we can decompose this σ using a procedure outlined in "Abstract Algebra" by Dummit and Foote [4] (p.107). There are $\frac{n!}{(n-2)! \times 2!}$ (a finite number of) transpositions in S_n thus it can be finitely generated. Take the cycle generated by any of these transpositions, this is a subgroup that is proper since $n > 2$ and so the order of the cycle is strictly less than the order of the group. Thus by theorem 4.8 we have that S_n contains a maximal subgroup and every proper subgroup is contained in one. However if we consider S_ω for $|\omega| = \infty$ then we wouldn't be able to use 4.8 as S_ω has infinite transpositions and so is infinitely generated.

The above example is an application of Theorem 4.8, however we could have used a weaker result as it concerns a finite group and thus even using this approach ZL is not ultimately necessary.

We now consider an example where the strength of Theorem 4.8 is necessary.

Example 4.12. Theorem 4.8 also gives us a way of proving that $\mathbb{Q}$ is not finitely generated. It can be shown that $\mathbb{Q}$ does not contain any maximal subgroups (see Conrad p.5 [2]). Therefore out of the contrapositive of Theorem 4.8 follows that $\mathbb{Q}$ is not finitely generated.

We have looked into the application of Zorn's Lemma for maximal subgroups in group theory. But as we said, another domain where Zorn's Lemma is particularly useful is the domain of homomorphisms. In one theorem (below) from Conrad's document [2] we get that Zorn's Lemma can be used to extend the domain of a homomorphism. We first introduce the definition of *divisible*. An abelian group D is called *divisible* if the function $x \rightarrow nx$ is surjective for every $n \geq 1$. This means that for every $d \in D$ and $n \geq 1$ there is an x such that $d = nx$ (x need not be unique). For example, $\mathbb{Q}$ is a divisible group, while $\mathbb{Z}$ is not.

Theorem 4.13. *Let D be a divisible group. If A is an abelian group and $B \subset A$ is a subgroup, each $f : B \rightarrow D$ can be extended to a homomorphism $\tilde{f} : A \rightarrow D$.*

For the proof we refer to Conrad in his paper [2]. This theorem is useful if you want to prove that there is a homomorphism between an abelian group and a divisible group: now you only need to prove that there is a homomorphism between a subgroup (of the abelian group) and the divisible group. This wouldn't have been possible if the theorem itself wasn't derived from Zorn's Lemma. Thus we see that Zorn's Lemma is a very useful tool within the world of group theory.

5 ZL Applied to Ideals

In Ring theory, particularly when it comes to ideals, some interesting results can be proven using ZL. For example, we can prove that rings containing 1 have maximal ideals, a compelling argument for why rings should always have a multiplicative identity. But first, we will introduce a lemma that will be very useful when proving the next few theorems.

Lemma 5.1. *The union of a totally ordered set of ideals in a nonzero commutative ring is also an ideal.*

Proof. Let $\{I_\alpha\}_{\alpha \in A}$ be a totally ordered set of proper of ideals in R . We will now prove $I = \cup_{\alpha \in A} I_\alpha$ is an ideal. We first prove that it is a subring. Since (0) is always an ideal, thus $(0) \subset I$ and I is not empty. If $i_1, i_2 \in I$, then that means that there are ideals $I_1, I_2 \subset I$, such that $i_1 \in I_1$ and $i_2 \in I_2$. This gives that $i_1 + i_2 \in I_1 + I_2 \subset I$, since the sum of two ideals is also an ideal, thus we see that $i_1 + i_2 \in I$ and I is closed under addition. Furthermore, we see that $i_1 i_2 \in I_1 \subset I$ as I_1 is an ideal and thus $i_1 i_2 \in I$. I is thus also closed under multiplication is a subring. Now we show that it is closed under multiplication by elements from R . It holds that for $r \in R$ and $i \in I$, there holds that $i \in I' \subset I$ for some ideal I' in I . This gives $ri = ir \in I' \subset I$ and we get that $ri = ir \in I$. We now conclude that I is an ideal. $\square$

Using the above lemma and a theorem proven by Krull we can prove two interesting statements in ring theory that at first glance don't seem related. We will even see that one of these statements is in fact equivalent to ZL. But let's first start of with another very useful lemma. This lemma will make the proofs of the two theorems 5.3 and 5.11 (of our own document) a lot shorter. (These are in fact Theorems 3.1 and 3.3 from Conrad's 'Zorn's Lemma and some applications' [2]. In his document you can find the original proof, which is a lot longer.)

Lemma 5.2. *Let D be some multiplicatively closed subset of a commutative ring R that contains 1. Let $D \neq \emptyset$, and $0 \notin D$. There exists an ideal which is maximal with respect to being disjoint from D . In fact this ideal is a prime ideal.*

Proof. We begin by defining the set S to which we will apply ZL. We will define the set as the set containing all ideals that are disjoint from D . We know that the ideal (0) is disjoint from D and so $(0) \in S$, so that S is nonempty. We define the partial ordering $\leq$ on S as ordering by inclusion.

We now take some totally ordered subset of S denoted $\{I_\alpha\}_{\alpha \in A}$ and define $I_{\max}$ as $I_{\max} = \bigcup_{\alpha \in A} I_\alpha$. We will show that $I_{\max}$ is an upper bound on this subset. To begin with we know that $I_\alpha \subset I_{\max}$ and so $I_\alpha \leq I_{\max}$ for any $\alpha \in A$. Additionally, we know by Lemma 5.1 that $I_{\max}$ is an ideal. Now assume $I_{\max}$ is not disjoint from D then there is an x in there intersection. However, $x \in I_{\max}$ implies that there is an $\alpha \in A$ so that $x \in I_\alpha$, so $x \notin D$, contradicting the assumption and therefore $I_{\max}$ is disjoint from D . We conclude that $I_{\max} \in S$ and so is an upper bound.

Thus we have proven the premise and can now apply ZL. By ZL S must have a maximal element M . To show this is a prime ideal, suppose to the contrary that there exists an $xy \in M$ so that $x, y \notin M$. Now construct $(x) + M$ and $(y) + M$. Both contain M as a proper subset and are ideals (as the sum of two ideals is an ideal) and so must not be in S or else maximality of M is contradicted. Hence, $(x) + M \neq \emptyset \neq (y) + M$ and so there exist $i, j \in R$ and $m, m' \in M$ so that $xi + m \in D$ and $yj + m' \in D$. However, since $(xi + m)(yj + m') = xyij + xim' + yjm + mm' \in M$ since $xy, m, m' \in M$ and M an ideal, and it is also in D since D is closed under multiplication, we have a contradiction. So either $x \in M$ or $y \in M$ and so M must be a prime ideal. $\square$

The following Theorems 5.3 and 5.11 are special cases of lemma 5.2, showing just how powerful this lemma actually is. We adjusted the proofs of 5.3 and 5.11 by using Lemma 5.2 to make it a lot shorter and without using ZL directly. We put the original proofs of Theorem 5.3 and 5.11, where ZL is directly used, in Appendix A.

Theorem 5.3. (Krull) *A nonzero commutative ring containing a multiplicative identity also has a maximal ideal.*

Proof. For a nonzero commutative ring R , take a subset $D = \{1\}$ (note that 1 exists in R because it has a multiplicative identity). This subset is multiplicatively closed as 1 to any power is 1. Also $0 \notin D \neq \emptyset$. According to Lemma 5.2, there exists a maximal ideal disjoint from D , call this M . We know that M is maximal among the ideals not containing 1 which are precisely the proper ideals. Hence M is maximal amongst the proper ideals and so is a maximal ideal. $\square$

Remark 5.4. We know that in a commutative ring with the multiplicative identity every maximal ideal is a prime ideal. So the above theorem not only proves the existence of maximal ideals but also of prime ideals in every nonzero commutative ring with multiplicative identity.

We can apply this theorem very broadly. Here is an example with a general field.

Example 5.5. A field F is by definition a nonzero commutative ring containing a multiplicative inverse. Thus, by theorem 5.2, it has a maximal ideal. However, the only maximal ideal is $\{0\}$. Because in a field every nonzero element has a multiplicative inverse such that $ab = ba = 1$ for $b = a^{-1}$ the multiplicative inverse of a . This means that for all ideals containing $a \neq 0$, you get that every $a(a^{-1}b) = b \in F$ is also contained in the ideal. Thus the only maximal ideal is $\{0\}$.

We can also apply this generally to polynomial rings over a field. In fact we can find examples of maximal ideals in general polynomial rings over fields as we see in the below example.

Example 5.6. For a field F the polynomial ring $F[X]$ contains a multiplicative identity 1, so by Theorem 5.3 it contains a maximal ideal. An example of such a maximal ideal for the polynomial ring is any ideal $(ax - b)$ for $a, b \in F$ and $a \neq 0$. To prove this statement, since $a^{-1}b \in F$, we prove that $\phi : F[x] \rightarrow F : f(x) \mapsto f(a^{-1}b)$ is a surjective homomorphism and thus by the 1st isomorphism theorem $F[x]/(ax - b) \simeq F$ and so $F[x]/(ax - b)$ field which implies that $(ax - b)$ is a maximal ideal.

Now we move on to the well known rings $\mathbb{Z}$ and $\mathbb{Z}[X]$.

Example 5.7. $\mathbb{Z}$ is a nonzero commutative ring and has a multiplicative inverse 1, so that means that it must have at least one maximal ideal. The maximal ideals in $\mathbb{Z}$ are the principal ideals generated by a prime number.

Example 5.8. $\mathbb{Z}[X]$ is a nonzero commutative ring and has a multiplicative inverse 1, so that means that it must also have at least one maximal ideal. The maximal ideals in $\mathbb{Z}$ are the ideals of the form $(p, f(x))$, with p a prime number and $f(x)$ a polynomial irreducible modulo p .

In 1978 Wilfrid Hodges showed that the inverse is also true in a paper titled "Krull implies Zorn" [7]. Hodges proves this using the following statement: 'each Unique Factorisation Domain contains a maximal ideal, implies Axiom of Choice', instead of more generally any commutative ring. However, Theorem 5.3 implies this statement and thus we would indeed get that the result from Krull implies Axiom of Choice. Additionally as we have seen in Theorem 3.7 Axiom of Choice implies ZL and so Krull implies ZL as advertised by the author. Thus both these statements imply each other and are thus equivalent.

Theorem 5.9. *Assuming that every Unique Factorisation Domain contains a maximal ideal, Axiom of Choice holds.*

Note that this is actually a stronger statement than stating that if 5.3 holds, that the Axiom of Choice also holds. This is because in 5.3 we assume that for all commutative rings there is a maximal ideal contained in it. But since all Unique Factorisation Domains are contained in the set of all commutative rings, this means that every Unique Factorisation Domain contains a maximal ideal. However, this statement shows you only need the fact that all the Unique Factorisation contain a maximal ideal to get the Axiom of Choice. Hodges' proof goes beyond the scope of this essay [7].

Since we have seen that Theorem 5.3 is equivalent to ZL we can attempt to answer the question of whether or not Theorem 5.3 can be proven without ZL. For some statement S that implies Theorem 5.3 we know that it must also imply ZL and therefore we could construct an argument that posits that ZL holds if S holds. Since S must lead to ZL through some argument we believe the answer to the question "Is the theorem provable without ZL?" to be yes, but the method used is stronger than ZL.

We now look at another result in ring theory that can be proven using ZL. In fact this result is the second theorem lemma 5.2 implies. As we will see below it can also be proven that the intersection of the prime ideals in a commutative ring containing 1 is the set of all nilpotent elements in that ring.

Definition 5.10. *In a ring R an element r is said to be **nilpotent** if there exists an integer n so that $r^n = 0$.*

Now that we know what nilpotent elements are we will prove the theorem using ZL. The following

proof was inspired by Conrad's 'Zorn's Lemma and some applications' [2], where we took the original proof and adjusted the approach using Theorem 5.2. This made the proof a lot shorter.

Theorem 5.11. *The intersection of all prime ideals in a nonzero commutative ring is the set of nilpotent elements in the ring.*

Proof. Let R be nonzero commutative ring. If $r \in R$ is nilpotent, then we have that $r^n = 0$ for some $n \geq 1$. If P of R is a prime ideal, then we know that $0 \in P$, thus we have that $r^n \in P$. We now prove that $r \in P$. This we can do by a simple proof of contradiction, let's assume that $r \notin P$, then we get that $r \cdot r^{n-1} = r^n \in P$. Because P is prime, we get that $r^{n-1} \in P$. Then we can do the same to r^{n-1} and get that $r^{n-2} \in P$. With induction it is now possible to prove that $r \in P$, but this is in contradiction to our original assumption that $r \notin P$. We thus conclude that $r \in P$. Thus every nilpotent element of R is in the intersection of all prime ideals of R .

Now we want to show the intersection of all prime ideals of R consists only of nilpotent elements: if $r \in P$ for all prime ideals P then $r^n = 0$ for some $n \geq 1$. We shall prove this by a contrapositive statement: if $r \in R$ is not nilpotent then some prime ideal of R does not contain r . So an element of R lying in all prime ideals of R must be nilpotent.

We now prove this contrapositive statement using Lemma 5.2. Let r be non nilpotent and $r \in R$. This means that we can arbitrarily choose a nonempty multiplicatively closed subset $D = \{1, r, r^2, r^3, \dots\}$. Because we assume that r is non nilpotent and D only contains 1 and all the positive powers of r , this means that D can't contain 0. This would otherwise be in contradiction with the fact that r is non nilpotent. With Lemma 5.2 we see that there is an ideal that is maximal with respect to being disjoint from D and this ideal is also a prime ideal. This means that this prime ideal of R was the prime ideal that we were looking for in our contrapositive statement and thus the contrapositive statement has been proven. $\square$

For the original proof, where ZL was applied directly, see Conrad [2].

Corollary 5.11.1. *Every proper ideal in a nonzero commutative ring is a subset of some maximal ideal*

Proof. Take I to be a proper ideal in R . So, R/I is nonzero and by Theorem 5.3 contains a maximal ideal. Since there is a bijection between the ideals of R and R/I for which for $J \in R$, $I \in J$ there is some maximal ideal K containing I . $\square$

There is an alternative proof of theorem 5.11 provided by Conrad (p.13) that follows from ZL but indirectly using Theorem 5.3. The proof is pretty interesting as it makes use of polynomial rings and goes as follows:

Proof. The first inclusion $r \in R$ nilpotent $\implies r$ in all prime ideals is shown in the above proof directly and not using ZL. We now consider the second inclusion $\bigcap P \subseteq \{r \in R : \exists n \in \mathbb{Z} : r^n = 0\}$ and prove the contraposition; that if $r \in R$ is not nilpotent then there is some prime ideal P for which $r \notin P$. If $r \in R$ is not nilpotent then we have that $rx - 1 \in R[x]$ is not a unit. Namely assume $(rx - 1)(a_0 + a_1x + a_2x^2 + \dots + a_nx^n) = 1$ we have that $a_0 = -1$ and need $rx a_0 - a_1x = 0$ and so $a_1 = -r$. More generally we require $rx a_{i-1} x^{i-1} - a_i x^i = 0$ since the result must be of degree 0. Therefore $a_i = r a_{i-1}$ and so by induction $a_i = -r^i$. Polynomials in $R[x]$ must be of degree $n \in \mathbb{Z}^+$ and $r^n \neq 0$ for all $n \in \mathbb{Z}^+$. We see the sum is telescoping, $(rx - 1)(a_0 + a_1x + \dots + a_nx^n) = 1 + (\sum_{i=1}^n (r a_{i-1} - a_i) x^i) + r x a_n x^n = 1 + (\sum_{i=1}^n (0) x^i) + r^{n+1} x^{n+1} = 1 - r^{n+1} x^{n+1}$ and consequently we have that $rx - 1$ is not a unit since $1 - r^{n+1} x^{n+1} \neq 1$. So the ideal $(rx - 1) \neq 1$ and so $(rx - 1)$ is a proper ideal. We see in the above Corollary of Theorem

5.3 that every proper ideal in a ring containing identity is in a maximal ideal. Hence $(rx - 1)$ is contained in some maximal ideal M . Since $R \rightarrow R[x] \rightarrow R[x]/M$ is a homomorphism (with $R[x]/M$ a field since M is a maximal ideal), where the first homomorphism is inclusion and the second is reduction. We have that the kernel P of the homomorphism $\phi : R \rightarrow R[x]/M$ is prime since by the since the quotient R/P is an integral domain. This is true since, by the 1st isomorphism theorem $\varphi : R/P \rightarrow \phi(R)$ is an isomorphism, and $\phi(R)$ is a subring of $R[x]/M$ and all the subrings of a field are integral domains, R/P is thus an integral domain. We know that $rx - 1$ is in the kernel of $R[x]/M$ since $(rx - 1) \in M$ so $rx - 1 \equiv 0 \pmod{M}$ and $rx \equiv 1 \pmod{M}$ so that $r \notin \ker(R[x]/M) \implies r \notin P$. This finishes the proof. $\square$

Now we shall add another example for good measure of how ZL is used in the world of ideals this is a good example of the reversal of ZL to find a minimum. (This is actually the solution to an exercise from Advanced Modern Algebra by Rotman [10].)

Example 5.12. (a) We shall first start by mentioning that there are commutative rings for which the intersection of two prime ideals P and Q does not need to be a prime ideal. For example, $\mathbb{Z}$ contains prime ideals $2\mathbb{Z}$ and $3\mathbb{Z}$, but the intersection $6\mathbb{Z}$ is certainly not a prime ideal. This is different from 'normal' ideals as the intersection of a nonempty set of ideals is also an ideal.

(b) Now we shall prove that every commutative ring R has a minimal prime ideal, this means a prime ideal I for which there is no prime ideal $P \subsetneq I$. We shall prove this by using ZL.

Define S as the set of all ideals and order it by reverse inclusion (this means $P \subseteq Q$ gives $P \geq Q$). S is thus a partially ordered set. Now we prove that all the totally ordered subsets have an upper bound. Take the chain $P_1 \supseteq P_2 \supseteq \dots P_n \supseteq P_{n+1} \dots$, which as a of decreasing sequence of prime ideals. Now we prove that the intersection $P = \bigcap_{n \geq 1} P_n$ is a prime ideal. We know that the intersection of any nonempty collections of ideal is also an ideal, this is a pretty well known fact and we shall omit the proof of this statement. We shall prove that it is a prime ideal by a proof by contradiction. If $xy \in P$, this means that $xy \in P_i$ for all i . Now let's assume that $x, y \notin P$, this means there is at least one prime ideal in the chain that does not contain x and at least one prime ideal in the chain that does not contain y . Thus we may assume that $x \notin P_k$ and $y \notin P_m$ and without loss of generality that $P_k \supseteq P_m$. We know that P_k and P_m are prime ideals and that they contain xy , this means that $y \in P_k$ and $x \in P_m \subseteq P_k$, this is in contradiction to the fact that $x \notin P_k$. Thus we conclude that P is a prime ideal.

Since we know that $P \subseteq P_n$ for all $n \geq 1$ and we get that P is an upper bound for this chain. By ZL we get that S has a maximal element and thus R has a minimal prime ideal.

Thus we see that ZL is used in variety of ways in the world of ideals. Often it is possible not to use ZL in the proof of a statement, but the lemma's used in the proof were proven using ZL. Especially with the proofs of Theorem 5.3 and 5.11, we see that by not using ZL directly, but indirectly by using it to prove another lemma, we get the shortest proofs. Moreover, we have seen that one of the statements, Theorem 5.3, has in fact been proven to be equivalent to ZL which shows how any argument for that Theorem can also lead to an argument that implies the truth of ZL.

6 Uniqueness of Algebraic Closure

After we have seen what ZL's influence in groups and rings is, we shall look into how ZL is used within the world of fields. In particular ZL can be used to prove the uniqueness of algebraic closure up to field isomorphism which as stated in the history section was one of the motivations

for ZL. The proof itself is quite short, however, we will need the following lemma

Lemma 6.1. *If $\bar{k}/k$ is an algebraic closure, and if F/k is an algebraic extension, then there is an injective k -map $\psi : F \rightarrow \bar{k}$.*

The proof of this lemma makes use of ZL. However, the background for the proof is quite extensive and not only that, but the lemma itself can be quite difficult to understand as it makes use of a number of more advanced concepts. So we shall begin by introducing a couple of definitions of concepts to do with algebraic closure, for this we will follow a section from Rotman's book quite closely [10] (p.185–188 & p.352–p.357). We will be starting with the definition of an extension.

Definition 6.2. If k is a subfield of a field K then we call K a **field extension** of k . We can also write this as the field extension K/k . Extensions are not to be confused with the quotient group.

The next example of a field extension involving $\mathbb{R}$ and $\mathbb{Q}$ should be quite familiar.

Example 6.3. We know that $\mathbb{R}/\mathbb{Q}$ is a field extension since $\mathbb{Q}$ is a subfield of $\mathbb{R}$. We know already that $\mathbb{Q} \subset \mathbb{R}$, and $\mathbb{R}$ is a field. Moreover, $\mathbb{Q}$ is also a field and so a sub-field.

Now we consider when elements are *algebraic* over a certain field.

Definition 6.4. If K/k is a finite extension, then an element $\alpha \in K$ is **algebraic** over k if there is a nonzero polynomial $p(x) \in k[x]$ having α as a root.

Example 6.5. For example, $i \in \mathbb{C}$ is algebraic over $\mathbb{R}$ as i is a root of the polynomial $p(x) = x^2 + 1$.

Thus, by combining the two definitions, we get that an algebraic extension is an extension K/k such that every $\alpha \in K$ is algebraic in k . A well known algebraic extension is $\mathbb{C}$, which is an algebraic extension of $\mathbb{R}$. Now, let's introduce another important notation, namely that of $k(\alpha)$.

Definition 6.6. If K/k is an extension and $\alpha \in K$ then $k(\alpha)$ is the intersection of all subfields of K containing k and α . We call $k(\alpha)$ the subfield of K obtained by **adjoining** α to k .

Now we know what algebraic means, we introduce one of the lemma's needed to prove our lemma 6.1.

Lemma 6.7. *Take*

$$K_0 \subseteq K_1 \subseteq K_2 \subseteq \dots \subseteq K_n \subseteq \dots$$

as a tower of fields (a sequence of field extensions), where K_i for $i = 0, 1, \dots$ are fields. If K_{n+1}/K_n is algebraic for every $n \in \mathbb{Z}^+$, then $K^* = \cup_{n \geq 0} K_n$ is a field that is algebraic over K_0 .

We will prove this lemma, but for that we shall need another lemma.

Lemma 6.8. *If $k \subseteq K \subseteq E$ is a tower of fields with E/K and K/k algebraic, then E/k is also algebraic.*

Now we can finally start to prove Lemma 6.7.

Proof. We shall first start by proving that $K^* = \cup_{n \geq 0} K_n$ is actually a field. If $x, y \in K^*$, then there are K_m, K_n such that $x \in K_m$ and $y \in K_n$. We may assume without loss of generality that $m \leq n$, this means that K_n is a field extension of K_m . Thus $x, y \in K_n \subseteq K^*$. As K_n is simply a field, it is closed under multiplication, closed under addition and all its nonzero elements have an inverse. This means that $x + y \in K_n$, $xy \in K_n$ and $x^{-1} \in K_n$ for $x \neq 0$, but this also means that $x + y \in K^*$, $xy \in K^*$ and $x^{-1} \in K^*$ for $x \neq 0$ and K^* is a field.

Now we prove that K^*/K_0 is algebraic. If $z \in K^*$, then $z \in K_l$ for some l . We see that K_1/K_0 and K_2/K_1 are algebraic (as K_{n+1}/K_n is algebraic for every $n \in \mathbb{Z}^+$). By using Lemma 6.8, we get that K_2/K_0 is also algebraic. We can do the same with K_3/K_0 , thus we can use induction to prove that K_l/K_0 is algebraic. This means that z is algebraic over K_0 . This means that every element of K^* is algebraic over K_0 and we get that K^*/K_0 is algebraic. $\square$

Let's now finally introduce the meaning of *algebraic closed* and *algebraic closure*.

Definition 6.9. A field K is said to be **algebraically closed** if $\forall f(x) \in K[x]$, $f(x)$ has a root in F .

An **algebraic closure** of a field k is an algebraic extension $\bar{k}/k$ such that $\bar{k}$ is algebraically closed.

One of the most well known examples of an algebraically closed field, is that of the set of complex numbers $\mathbb{C}$. This is in fact exactly what the fundamental theorem of algebra tells us!

Now that we know what algebraically closed and algebraic closure mean we can introduce an existence theorem that will prove useful in the proof of the uniqueness of algebraic closure and in particular the proof of Lemma 6.1.

Theorem 6.10. For a field k there exists a $\bar{k}$ such that $\bar{k}$ is an algebraic closure of k

The proof of this theorem is quite extensive and not needed to understand the proof of Lemma 6.1, thus we shall omit this proof. This proof does not make use of ZL directly however it does rely on the Corollary 5.11.1 of Theorem 5.3, which in turn can be proven with ZL. For the more curious reader, the proof can be found on page 354–355 of Rotman's Advanced Modern Algebra book [10]. Another essential concept needed to understand the lemma, is the k -map.

Definition 6.11. Let F and K be field extensions of k . We define a **k -map** φ to be a ring homomorphism $\varphi : F \rightarrow K$ for which elements in k are mapped to themselves.

We now give an example for a k -map to give you some intuition of what a k -map could be.

Example 6.12. The well known complex conjugation $\phi : \mathbb{C} \rightarrow \mathbb{C}$. Then we have $\phi(z) = \bar{z}$. As $\overline{z + w} = \bar{z} + \bar{w}$ and $\overline{z\bar{w}} = \bar{z} \cdot \bar{\bar{w}}$, it is not difficult to see that this is actually a field homomorphism. We also know that $\mathbb{C}$ is an extension of $\mathbb{R}$. We thus conclude that the complex conjugate is a $\mathbb{R}$ -map.

We will now derive two important properties of a k -map. From this point onward we will write out the proofs of statements to make the proof of uniqueness of algebraic closure clearer. One important property of a k -map is that it permutes all of the roots $\alpha_1, \alpha_2, \dots, \alpha_n \in K$ of some polynomial $f(x) \in k[x]$.

Proposition 6.13. Let K/k be a field extension and $\varphi : K \rightarrow K$ be a k -map. Then for any monic irreducible $f(x) \in k[x]$ with roots $\alpha_i \in K$ it follows that φ permutes those roots: $\varphi(\alpha_j) = \alpha_j$ for some j .

Proof. For the given $f(x) := x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \dots + a_0$, we know that $f(\alpha_i) = 0$.

From the properties of a k -map it follows that

$$\begin{aligned}
\varphi(0) &= \varphi(f(\alpha_i)) \\
&= \varphi(\alpha_i^n + a_{n-1}\alpha_i^{n-1} + a_{n-2}\alpha_i^{n-2} + \dots + a_0) \\
&= \sum_{j=0}^n \varphi(a_i)\varphi(\alpha_i^j) \text{ (where } a_n = 1) \\
&= \sum_{j=0}^n a_i\varphi(\alpha_i)^j.
\end{aligned}$$

Consequently, $\varphi(\alpha_i)$ is a root of $f(x)$. Since k is a field $1 \in k$ and per definition of the k -map $1 \mapsto 1$, $\text{im } \varphi \neq \emptyset$. Furthermore, K is a field and hence, as the kernel of the homomorphism is a subring of K it is either $\{0\}$ or K . Now we know $1 \notin \ker \varphi$, hence the kernel is trivial and φ must be injective. We also know that the polynomial $f(x)$ is of finite degree and thus has finitely many roots, so $\varphi : \{\alpha_1, \dots\} \rightarrow \{\alpha_1, \dots\}$ is bijective as the domain and range have the same cardinality. $\square$

Now that we understand what a k -map is and have worked out one of its properties we will consider an interesting fact that will prove to be useful in our end goal.

Lemma 6.14. *Let K/k be an algebraic field extension. Every k -map of the form $\varphi : K \rightarrow K$ is an automorphism.*

Proof. From the same reasoning as provided in the above proposition it follows that the k -map is injective. Now we need only to prove surjection. Since K is an algebraic field extension of k every element of K is a root of some polynomial in $k[x]$. Now for an $a \in K = \text{im } \varphi$ we established it is a root of some polynomial $p(x)$. Hence, by Proposition 6.13 $\varphi^{-1}(a)$ is a root of the $p(x)$ that also lies in K . Therefore φ is surjective and is in consequence an automorphism. $\square$

The final piece of the puzzle to solve 6.1, is the following Lemma, the proof of which is given on page 188 in Advanced Modern Algebra by Rotman [10].

Lemma 6.15. *If K/k is an extension and $\alpha \in K$ is algebraic over k , then there is a unique monic irreducible polynomial $p(x) \in k[x]$ having α as a root. If $\alpha' \in K$ is another root of $p(x)$, then there is an isomorphism*

$$\theta : k(\alpha) \rightarrow k(\alpha')$$

with $\theta(\alpha) = \alpha'$ and $\theta(c) = c$ for all $c \in k$.

We are now ready to prove Lemma 6.1, we will prove this using ZL and it is particularly interesting to see how the general structure of a ZL proof is recognizable in this proof (the proof itself is taken from Rotman, p.356–357) [10]. Once again, Lemma 6.1 states that:

If $\bar{k}/k$ is an algebraic closure, and if F/k is an algebraic extension, then there is an injective k -map $\psi : F \rightarrow \bar{k}$.

Proof. We already know that k is a sub-field of F and that $\psi : k \rightarrow \bar{k}$ is a k -map trivially by sending each element to itself. We can frame the problem for ZL as follows. We want to find the maximal intermediate field $k \subseteq E \subseteq F$ such that $\psi : E \rightarrow \bar{k}$ is a k -map.

We define the set as the set of all pairs (E, f) for which $f : E \rightarrow \bar{k}$ is a k -map

$$S := \{(E, f) : E \text{ is an intermediate field and } f : E \rightarrow \bar{k} \text{ is a } k\text{-map}\}.$$

We define the partial ordering as

$$(E, f) \leq (E', f')$$

if E is a subfield of E' and $f'(e) = f(e)$ for all $e \in E$. Note that the set S contains the intermediate field k along with the trivial k -map $\psi : k \rightarrow \bar{k}$ and so $S \neq \emptyset$.

Take some totally ordered subset $\{(E_i, f_i) : i \in I\}$. Thus we want to prove that $(\bigcup E_i, \bigcup f_i)$ is an upper bound. We begin by proving $\bigcup E_i$ is an intermediate field. It is known that $\bigcup E_i$ is a sub-ring of F since addition and multiplication are closed. Moreover, for $0 \neq x \in \bigcup E_i$, $x \in E_{i_0}$ for some $i_0 \in I$ and so x has a multiplicative inverse, thus this is an intermediate field. Now we show that $\psi := \bigcup f_i$ is a k -map extending all f_i . Take an $e \in \bigcup E_i$, then $e \in E_{i_0}$ for an $i_0 \in I$ and so $\psi(e) = f_{i_0}(e)$. On the contrary, there may be another index $i_1 \in I$ for which $e \in E_{i_1}$ hence $\psi(e)$ is also equal to $f_{i_1}(e)$. However, since a totally ordered subset of S is being considered, either $(E_{i_0}, f_{i_0}) \leq (E_{i_1}, f_{i_1})$, or vice versa. Without loss of generality we assume the prior, then $f_{i_1}(e) = f_{i_0}(e)$ since $e \in E_{i_0}$, so ψ is well defined. We know this is a k -map as for any $k_0 \in k$, $k_0 \in \bigcup E_i$ and for any $i_0 \in I$, $k_0 \in E_{i_0}$. Consequently, $\psi(k_0) = f_{i_0}(k_0)$ and f_{i_0} is a k -map, so $\psi(k_0) \in k$. Thus $(\bigcup E_i, \bigcup f_i) \in S$. Since $E_i \subset \bigcup E_i$ and $\psi|_{E_i} = f_i$ for all $i \in I$, $(E_i, f_i) \leq (\bigcup E_i, \bigcup f_i)$, so it is an upper bound.

By ZL, there is a maximal element in S , we denote this by (E_0, f_0) . If we can show that $E_0 = F$ we have our answer. Suppose, on the contrary, that $E_0 \neq F$ then there exists some $a \in F$ so that $a \notin E_0$. Since given F/k is an algebraic extension, and F/E_0 is a field extension, by the definition of an algebraic extension F/E_0 is algebraic. This implies that there is an irreducible $p(x) \in E_0[x]$ so that $a \in F$ is a root. Define $f_0^* : E_0[x] \rightarrow \bar{k}[x]$ to be a homomorphism with $f_0^*(x) = x$ and $f_0^*|_{E_0} = f_0$. Since $\bar{k}$ is algebraically closed, $f_0^*(p(x))$ has a factorization,

$$f_0^*(p(x)) = f_0^*(x^n + c_{n-1}x^{n-1} + \dots + c_0) = \prod_{j=1}^n (x - b_j).$$

Suppose that all $b_j \in f_0(E_0)$ then we know that since f_0 is injective ($\text{im } f_0 \neq \{0\}$), $f_0^{-1}(b_j) \in f_0^{-1}(f_0(E_0)) = E_0 \subset F$. By Proposition 6.13, f_0 permutes the roots of $p(x)$ in E_0 so $p(x) = \prod_{j=1}^n (x - f_0^{-1}(b_j)) \in E_0[x]$. However, then $p(x)$ is reducible in $E_0[x]$ so $a \notin E_0$ cannot be a root as E_0 field implies $E_0[x]$ is a unique factorization domain, contradiction. There must then be a root $b_{j_0} \notin f_0(E_0)$ and we will want to use this fact to create a new pair in S that contradicts the maximality of (E_0, f_0) . Take the new field $E_0(a)$ which per definition is intermediate as E_0 is intermediate and $a \in F$. We will want to construct a k -map f_1 that extends f_0 . By Lemma 6.15 there exists an isomorphism $f_1 : E_0(a) \rightarrow E_0(b_{j_0}) \subset \bar{k}$ for which $f_1(a) = b_{j_0}$ and $f_1|_{E_0} = f_0$. Hence $f_1 : E_0(a) \rightarrow \bar{k}$, is a k -map (since it is homomorphic and maps elements of k within k). So $(E_0(a), f_1) \in S$ and $(E_0, f_0) < (E_0(a), f_1)$, contradicting maximality, so $E_0 = F$. We know that f_1 is injective since $\text{im } f_1 \neq \{0\}$. $\square$

Now we can finally use both Lemma 6.1 and 6.14 to prove the uniqueness of algebraic closure up to isomorphism.

Theorem 6.16. *Any two algebraic closures of a field k are isomorphic via a k -map.*

Proof. Let K and L be two algebraic closures of a field k . We know by Lemma 6.1 that there are injective k -maps $\phi : K \rightarrow L$ and $\psi : L \rightarrow K$. As k -maps are basically a type of homomorphisms, we now only have to prove that both ϕ and ψ are surjective. We shall prove this by looking at the composition of both functions. We get that $\phi \circ \psi : K \rightarrow K$ and $\psi \circ \phi : L \rightarrow L$ are both

automorphisms by Lemma 6.14. This means that $\phi \circ \psi$ and $\psi \circ \phi$ are both bijective and in particular surjective. We know that the rules of function composition states that because $\phi \circ \psi$ is surjective, this means that ϕ has to be surjective. The same goes for ψ as $\psi \circ \phi$ is surjective. Thus we have that ϕ and ψ are k -isomorphisms. $\square$

This means all the algebraic closure of a field have the same structure (isomorphic). For example we know that the algebraic closure of the real numbers $\mathbb{R}$ is the set of complex numbers $\mathbb{C}$, and now also know from the above Theorem that for any other algebraic closure A of $\mathbb{R}$, $A \simeq \mathbb{C}$.

In this section we considered another application of ZL. While we have previously seen how ZL can be used to prove existence of some object we have seen here that it can also be used to prove an object's uniqueness.

7 Conclusion

In this essay we aimed to cover how and why ZL plays an important role in algebra. Beginning by deciphering the statement to give the reader an understanding of ZL as a maximal principle and providing a conceptual example as a way of adding clarity. We proceeded by delving into the history of ZL and saw how the idea was "in the air" at the time. It was in fact co-discovered by many different people in equivalent or similar framing while, ultimately, Max Zorn popularized the idea. After a brief history, we choose to proceed by discussing its equivalence to the Axiom of Choice and Well-Ordering principle, which on first glance don't necessarily seem equivalent. We found this important as ZL arguments were preceded by arguments that made use of the Axiom of choice in algebra and, on the other hand, as it was also an interesting topic to look into that provided a difficult yet interesting preliminary example of a ZL argument. It was then time to cover some of the applications in algebra. We saw how ZL played an important role in proving the existence of certain objects in group theory. In particular we considered two examples, the existence of maximal subgroups and the existence of a homomorphic extension of a function with a particular domain and range and saw how ZL (as well as transfinite induction) played an important role in generalizing these results to groups of infinite order. To supplement these examples we considered a result in ring theory due to Krull, we saw with this example how, in particular, proofs could be shortened by an indirect use of ZL and that ZL's equivalence to one of the Theorems shows just how important a principle like ZL is in the proving of that result. We wanted to conclude with a more complicated example, the uniqueness of an algebraic closure, as this was one of the original motives for Zorn to introduce the lemma as evident in his "A Remark on Method in Transfinite Algebra" [11].

We can conjecture about several things after reading this essay. All throughout the essay we saw that ZL arguments followed a strict structure. This structure begins with the construction of a partially ordered set that satisfies certain conditions that would allow the existence of a maximal element in that set to imply the result at hand. From there we would want to show that the hypothesis of ZL was met so that it could be applied. After this we would then generally be able to find some contradiction using the maximality of an element to derive the result. We also saw how ZL allows us to avoid certain difficulties in an argument, for example in Example 1.9 we saw how ZL can be used to argue that there is a heaviest apple and a heaviest orange even though there may be an infinite number of them. Furthermore, because ZL is a quite easy to understand once you know what the keywords mean, you can use ZL in various situations. The versatility of this theorem is really something to behold, as throughout this essay it has been used in proofs that are almost trivial to some that already require a good understanding of mathematics. Thus,

we hope to have also left the reader with the impression of just how many applications there are.

We would like to conclude on this note by remarking that we only on touched the surface of the applications of ZL in the form of a list of topics we have encountered. First off, ZL has can be used to prove a result from Hausssdorf stating that every vector space has a basis so long it is nontrivial. There are also some more advanced applications to do with closure as discussed in Conrad's "Zorn's Lemma and Some Applications II" [3].

References

- [1] Paul J. Campbell. “The origin of “Zorn’s lemma””. In: *Historia Math.* 5.1 (1978), pp. 77–89. ISSN: 0315-0860. DOI: 10.1016/0315-0860(78)90136-2. URL: [https://doi.org/10.1016/0315-0860\(78\)90136-2](https://doi.org/10.1016/0315-0860(78)90136-2).
- [2] Keith Conrad. “Zorn’s Lemma and some applications”. In: (). URL: <https://kconrad.math.uconn.edu/blurbs/zorn1.pdf>.
- [3] Keith Conrad. “Zorn’s Lemma and some applications, II”. In: (). URL: <https://kconrad.math.uconn.edu/blurbs/zorn2.pdf>.
- [4] David S. Dummit and Richard M. Foote. *Abstract algebra*. Third. John Wiley & Sons, Inc., Hoboken, NJ, 2004, pp. xii+932. ISBN: 0-471-43334-9.
- [5] Sir William Timothy Gowers. “How to use Zorn’s Lemma”. In: (). URL: <https://gowers.wordpress.com/2008/08/12/how-to-use-zorns-lemma/>.
- [6] Daniel R. Grayson. “Zorn’s Lemma”. In: (). URL: <https://faculty.math.illinois.edu/~dan/ShortProofs/Zorn.pdf>.
- [7] Wilfrid Hodges. “Krull implies Zorn”. In: *J. London Math. Soc. (2)* 19.2 (1979), pp. 285–287. ISSN: 0024-6107. DOI: 10.1112/jlms/s2-19.2.285. URL: <https://doi.org/10.1112/jlms/s2-19.2.285>.
- [8] C. Kuratowski. “Une méthode d’élimination des nombres transfinis des raisonnements mathématiques.” French. In: *Fundam. Math.* 3 (1922), pp. 76–108. ISSN: 0016-2736. DOI: 10.4064/fm-3-1-76-108.
- [9] B. H. Neumann. “Some remarks on infinite groups.” English. In: *J. Lond. Math. Soc.* 12 (1937), pp. 120–127. ISSN: 0024-6107. DOI: 10.1112/jlms/s1-12.46.120.
- [10] Joseph J. Rotman. *Advanced modern algebra*. Prentice Hall, Inc., Upper Saddle River, NJ, 2002, xvi+1012+A8+B6+I14. ISBN: 0-13-087868-5.
- [11] Max Zorn. “A remark on method in transfinite algebra”. In: *Bull. Amer. Math. Soc.* 41.10 (1935), pp. 667–670. ISSN: 0002-9904. DOI: 10.1090/S0002-9904-1935-06166-X. URL: <https://doi.org/10.1090/S0002-9904-1935-06166-X>.
- [12] *Zorn’s lemma*. Aug. 2021. URL: https://en.wikipedia.org/wiki/Zorn's_lemma.