Summary of Steinitz's Theorem

Final Report

Mat498: Model Theory

Giovanni Tedesco

Contents

1 Background

The result that we are interested in discussing is known as Steinitz's Theorem.

Theorem 1.0.1 (Steinitz's Thoerem)**.** *If M and N are algebraically closed fields of characteristic 0 such that $|M| = |N| = \aleph_0$ then $M \cong N$.*

In essence what this says is that any two algebraically closed fields of characteristic 0 that have the same cardinality are isomorphic. In order to provide a proof of this result we are going to need to introduce a handful of notions from both model theory and algebra.

1.1 Algebraic Background

We begin with some of the relevant algebraic background which is needed to understand both the statment of the problem and the proof. First recall the definition of a field:

Proposition 1.1.1. *Every field homomorphism is injective*

Proof. Suppose that F, K are fields and let $\phi : F \to K$ a field homomorphism between them. Let $a, b \in F$ and suppose that $\phi(a) = \phi(b)$. This implies that $\phi(a) - \phi(b) = 0$ so $\phi(a - b) = 0$ if $a \neq b$ then this means that $\phi(a - b) = 0$ for $a - b \neq 0$. Taking $c = a - b$ then we know that $\phi(cc^{-1}) = 1 = \phi(c)\phi(c^{-1}) = 0$ which is a contradiction. Thus $a = b$ necessarily and so ϕ is injective. $\square$

This fact that field homomorphisms are always injective lies at the heart of field theory, in particular it is the reason why we are able to focus so heavily on what are known as field extensions.

Definition 1.1.2 (Field Extension)**.** *We say that E is a field extension of F if there is an injective field homomorphism $\phi : F \to E$*

Field extensions come in two main flavours: algebraic extensions and trancendental extensions. We focus on the former first.

Definition 1.1.3 (Polynomial Ring over *F*)**.** *Suppose that F is a field we define the polynomial ring F[x] over F as*

$$F[x] := \left\{ \sum_{i=1}^{n} a_i x^i : a_i \in F, n \in \mathbb{N} \right\}.$$

We take the operations to be the usual polynomial addition and product.

Definition 1.1.4 (Irreducible)**.** *We say that a polynomial $p(x) \in F[x]$ is irreducible if it cannot be factored into two polynomials of lesser degere.*

This notion of irreducibility is one that we are already very familiar with. Consider the example of $x^2 + 1$ as a polynomial over $\mathbb{Q}$. Clearly this polynomial has no factors over $\mathbb{Q}$ (in particular since $i \notin \mathbb{Q}$) and so as a result we know that we cannot factor this polynomial any further. A similar example is that of $x^2 - 2$. This polynomial taken over $\mathbb{R}$ has a root of $\sqrt{2}$ however $\sqrt{2}$ is famously not a rational number. Something we might wish to do now is "extend" $\mathbb{Q}$ in order to contain these elments so that these polynomials factor over them.

Definition 1.1.5 (Algebraic Numbers). *Let F be a field and E a field extension of F. We say that $\alpha \in E$ is algebraic over a field F if there is a polynomial $p(x) \in F[x]$ such that $p(\alpha) = 0$ when viewed as a polynomial over E.*

Without going into too many details about how these extensions work we are going to loosely define what it means to be an algebraic extension of F. Just know that this is a process that can be done rigorously for any irreducible polynomial in $F[x]$. The smallest (in degree) irreducible polynomial containing α as a root is known as the minimal polynomial of α and is denoted m_α.

Definition 1.1.6 (Algebraic Extension). *Suppose that α is algebraic over F. We define $F(\alpha)$ as the smallest field which contains F and α.*

We know that algebraic numbers satsify some polynomial $p(x)$ over F, so we can think of the field $F(\alpha)$ as adding in the root of this polynomial. One important fact that we are going to make heavy use of later is that we are able to lift isomorphisms of fields up to isomorphisms of their extensions. In the case of algebraic extensions this is relatively straightforward since we know "exactly" what algebraic numbers look like in terms of the ring of polynomials.

We first notice that we can lift isomorphisms between fields to an isomorphism between their polynomial rings.

Lemma 1.1.7. *Let F and K be fields and if $\phi : F \to K$ be an isomorphism between them then there exists a (ring-)isomorphism $\overline{\phi} : F[x] \to K[x]$. Moreover, if $f(x)$ is irreducible over F then $\overline{\phi}(f)$ is irreducible over K.*

Proposition 1.1.8. *If F and K are fields and there is an isomorphism $\phi : F \to K$ then if α is algebraic over F then there is a β algebraic over K such that ϕ can be extended to an isomorphism $\overline{\phi} : F(\alpha) \to K(\beta)$*

Proof. If α is algebraic over F then we know that α is the root of some minimal polynomial $m_\alpha(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in F[x]$. Now since ϕ is an isomorphism of fields we get an irreducible polynomial

$$\overline{m_\alpha}(x) = x^n + \phi(a_{n-1})x^{n-1} + \ldots + \phi(a_1)x + a_0 \in E[x].$$

Since this polynomial is irreducible of degree n it is the minimal polynomial of some β which is algebraic over E. Now considering $F(\alpha)$ and $E(\beta)$ we see that we can extend ϕ to an isomorphism $\overline{\phi} : F(\alpha) \to F(\beta)$ by $\alpha \mapsto \beta$. This is clearly an isomorphism as we needed. $\qquad\square$

Moving on from algebraic numbers we are now interested in exploring the second class, trancendental numbers. This case is slightly more complicated. A trancendental number is something which is not an algebraic number. Loosely speaking these are all numbers which are not the root of any polynomial over the ground field. Classical examples of these are e and π, however showing that either of these are actually trancendental is quite difficult. The classical example of where these come into play is considering how $\mathbb{Q}$ embeds into $\mathbb{R}$. We see that there are elements of $\mathbb{R}$, such as e and π which are not in $\mathbb{Q}$. Which cannot be expressed by polynomials with rational coefficients.

Definition 1.1.9 (Trancendental Number). *Suppose that E is some field extension of F and let $\alpha \in E$. We say that α is trancendental if there are no polynomials $p(x) \in F[x]$ such that $p(\alpha) = 0$ when viewed as a polynomial over F.*

Remark 1.1.10. *It is important to notice here that the choice of ground field and extension field matters a lot. For example in the case of $\mathbb{R}$ over $\mathbb{Q}$ we have that π is trancendental over $\mathbb{Q}$ as there are no polynomials in $\mathbb{Q}[x]$ which have π as a root. However in the case of $\mathbb{C}$ over $\mathbb{R}$ then π is no longer trancendental as it is the root of $x - \pi$. Actually $\mathbb{C}$ is an algebraic extension of $\mathbb{R}$ and so there are no trancendental numbers.*

Definition 1.1.11 (Trancendental Extension). *Similar to the case of algebraic extensions, there are also trancendental extensions. Namely if F is a field, we say that a field extension E over F is trancendental if there is some $\alpha \in E$ such that α is trancendental over F.*

Recall that our goal is to prove an analogous result to Proposition 1.1.8 for trancendental numbers / extensions. In order to do this we are first going to need to prove a couple of facts.

Proposition 1.1.12. *Let F be a field. There are at most $|F|$ many algebraic elements over F.*

Proof. This is just a counting problem. Each algebraic number α over F is the root of some polynomial $x^n + \ldots + a_1 x + a_0$. There are at most countably many polynomials in which we have $|F|$ many choices for coefficients. Thus there are at most $|F|$ many algebraic numbers. $\square$

This proposition lets us make sense of why there *must* be trancendental numbers in $\mathbb{R}$ when viewed as an extension of $\mathbb{Q}$. This is because there are uncountably infinitely many real numbers and only countably many algebraic numbers over $\mathbb{Q}$.

The next tool that we are going to need is the quotient field / field of fractions associated with the polynomial ring $F[x]$. The details about this space can be found in [1] but for us we are going to strictly think about them as formal expresstions.

Definition 1.1.13 (Rational Polynomials). *Let F be a field, we define $F(x)$ as*

$$F(x) := \{\frac{p(x)}{q(x)} : p(x), q(x) \in F[x]\}.$$

This is known as the rational polynomials over $F[x]$.

Remark 1.1.14. *Note the difference between $F(x)$ and $F(\alpha)$, the former denotes the rational polynomials. The latter denotes the extension of F by an algebraic number α.*

Remark 1.1.15. *It is important to keep in mind that $F(x)$ consists of purely formal expressions. For example*

$$\frac{x-1}{x^2-1} \tag{1}$$

and

$$\frac{1}{x+1} \tag{2}$$

*Are not the same element in this field. Despite the fact that once one factors (1) we get (2). Since these are **purely formal expressions**. They are not the same.*

Notice that if α is some algebraic number over F then there is a natural map $ev_\alpha : F[x] \to F(\alpha)$ given by $p(x) \mapsto p(\alpha)$. This map is of course not injective as every polynomial which contains m_α as a factor is sent to 0.

This type of evaluation map is helpful since it allows us to recognize $F(\alpha)$ as a quotient of $F[x]$. In the case of trancendental numbers we are going to consider a similar map. Suppose that β is trancendental over F then we define the map $ev_\beta : F(x) \to F(\beta)$ which is given by

$$\frac{p(x)}{q(x)} \mapsto \frac{p(\beta)}{q(\beta)}.$$

First note that if β was not trancendental then this map is not injective (or well defined) as we end up dividing by 0 whenever $m_\alpha(x) \mid q(x)$. However since β is not trancendental, this map is not only injective, but it is infact an isomorphism! Since $F(x)$ is a field by construction and $F(\beta)$ is also a field. Thus ev_β is certainly surjective. Moreover, it is also an isomorphism as it is also clearly surjective. From this we have proven the following result:

Lemma 1.1.16. *If F is a field and β is trancendental over F then $F(x) \cong F(\beta)$*

Lastly we are going to need a lemma that allows us to lift isomorphisms between fields to isomorphisms between their rational polynomials

Lemma 1.1.17. *Suppose that F and K are fields and $\phi : F \to K$ is an isomorphism. Then ϕ can be lifted to an isomorphism $\overline{\phi} : F(x) \to K(x)$.*

Proof. This follows immediately from the fact that ϕ is an isomorphism. We can simply apply ϕ to the coefficients of the coefficients of any polynomials. Since equality is done coefficient wise this gives our result. $\square$

Now knowing this we can prove our main result for trancendental numbers.

Proposition 1.1.18. *Let F, K, M, N be fields such that $|M| = |N|$ and M (resp. N) is a trancendental extension of F (resp. K) and $|F| < |M|$ (resp $|K| < |N|$) then if $\phi : F \to K$ is an isomorphism and $\alpha \in M \setminus F$ is transcendental over F there is a $\beta \in N \setminus K$ such that ϕ can be extended to an isomorphism $\overline{\phi} : F(\alpha) \to K(\beta)$.*

Proof. Since we know that $|K| < |N|$ by Proposition 1.1.12 there is an element β which is trancendental over K. Now by Lemma 1.1.16 we have the following:

$$F \hookrightarrow F(x) \cong F(\alpha)$$

and

$$K \hookrightarrow K(x) \cong K(\beta).$$

Labelling the isomorphism between $F(x)$ and $F(\alpha)$ as ψ_α and the isomorphism between $K(x)$ and $K(\beta)$ as ψ_β. Additionally by Lemma 1.1.17 there is an isomorphism $\phi' : F(x) \to K(x)$ which lifts ϕ to an isomorphism between the rational polynomials.

Fromt these we get the following diagram:

$$
\begin{array}{ccc}
F & \longrightarrow & K \\
\downarrow & & \downarrow \\
F(x) & \longrightarrow & K(x) \\
\psi_\alpha \downarrow & & \downarrow \psi_\beta \\
F(\alpha) & \dashrightarrow & K(\beta) \\
& \psi_\beta \phi' \psi_\alpha^{-1} &
\end{array}
\tag{3}
$$

Therefore taking $\overline{\phi} : F(\alpha) \to F(\beta) = \psi_\beta \phi' \psi_\alpha^{-1}$ gives us the extension we require, as we needed. $\qquad\square$

This result similar to our previous is strong. It allows us to extend isomorphisms between fields to isomorphisms between extensions by trancendental numbers.

1.2 Ordinals and Transfinite Induction

The next tool that we are going to need to use is transfinite induction. Intuitively this is a way for us to extend the notion of usual induction on the natural numbers and allows us to perform a similar process on using what are known as ordinals.

Before we can talk about what ordinals are, it is important for us to introduce some other concepts first.

Definition 1.2.1 (Linear Ordering). *A linear order is a set X and a relation $< \subseteq X \times X$ that satisfies the following properites:*

1. *Irreflexive: $\neg a < a$*

2. *Transitive: If $a < b$ and $b < c$ then $a < c$.*

3. *Linearity: For all $x, y \in X$ either $x < y, x = y$ or $y < x$.*

If $(X, <)$ is a linear order we say that it is dense if for all x, y there is a z such that $x < z < y$.

To solidify this idea let's think of some common examples of linear orders and some of the properties that they may have.

Example 1.2.2. *The natural numbers with their usual ordering is an example of a linear order. Notice that this is not dense as, for example, there are no numbers between 1 and 2.*

Example 1.2.3. $\mathbb{Q}$ *with it's usual ordering is dense however notice that between any two numbers we can pick a midpoint between them.*

With these examples in mind we consider the next special case. Well orders.

Definition 1.2.4 (Well-Orders). *A linear order $(X, <)$ is said to be a well order if ever $S \subseteq X$ S has a minimal element.*

Consider the two examples above. We see that while they are both certainly linear orders, the natural numbers are a well order and the rationals are not. For example the set $(0,1) \cap \mathbb{Q}$ does not have a minimal element, while every set contained within the naturals certainly does. An interesting thing to notice is that the integers do not form a well order either. For example the set $S = \{n \in \mathbb{Z} : n < 0\}$ is a set without a minimal element.

Remark 1.2.5. *Something that is worth mentioning is that by the Axiom of Choice we can place a well order on every set. The above examples of $\mathbb{Q}$ and $\mathbb{Z}$ have well orders, but that does not mean that they are well ordered in their usual order.*

Let's look at the "set theorists natural numbers". One of the main things we can try and do to motivate the definition of an ordinal is to turn everything we care about working with into sets. The main goal of an ordinal is to extend a sort of "order" into an (uncountbly) infinite setting. First lets encode the natural numbers as sets.

$$0 = \{\}$$
$$1 = \{\{\}\}$$
$$2 = \{\{\}, \{\{\}\}\}$$
$$3 = \{\{\}, \{\{\}\}, \{\{\}\}\}\}.$$

Or we can re-write this as

$$0 = \{\}$$
$$1 = \{0\}$$
$$2 = \{0, 1\}$$
$$3 = \{0, 1, 2\}.$$

We can continue this process onwards and it gives us the natural numbers $\omega = \{1, 2, 3, \ldots\}$. But where do we go from here? Well naturally we can continue on doing what we were doing. Notice that in the previous process $n + 1 = n \cup \{n\}$. We are going to do the exact same thing now. We take $\omega + 1 = \omega \cup \{\omega\}$. We can again do this infinitely and that gives us $\omega + \omega$. Repeating a similar process for multiplication and exponentiation and onwards allows us to continue this process further and further. Notice that at each step we are doing one of 2 things. We are either adding a new set, for example in the case of $\omega + 1$, or we are taking the union of many sets, for example $\omega = \bigcup_{n \in \mathbb{N}} n$. Going forward these are going to be known respectively as the successor case, and the limit case.

Stepping back for a moment we look at the "set theorists natural numbers" again. Notice here that $2 \in 3$ by the definition of the set but we also have that $1 \subseteq 3$ when we look at their definition as sets. This is true beyond just the naturals. Notice that $\omega + 1 = \omega \cup \{\omega\}$. Thus not only is $\omega \in \omega + 1$ but $\omega \subseteq \omega + 1$.

Definition 1.2.6 (Transitive). *A set X is said to be transitive if whenever $x \in X$ then $x \subseteq X$.*

Notice that the sets we defined above are all transitive. For example $2 \in 3$ and $2 \subseteq 3$ based on how 2 and 3 are defined.

Definition 1.2.7 (Ordinal). *An ordinal is a transitive set α such that $(\alpha, \in)$ is a well-ordering.*

This in particular tells us that $\alpha = \{\beta : \beta < \alpha\}$. There are two main types of ordinals. Successor ordinals, and limit ordinals.

Definition 1.2.8 (Successor and Limit Ordinals)**.** *We say that an ordinal β is a successor ordinal if $\beta = \alpha + 1$ for some ordinal α. Ordinals which are not successor ordinals are called limit ordinals.*

The details about how ordinals work can be found in [2] however for our purposes we are going to assume the following facts about ordinals.

Lemma 1.2.9. *The class of ordinals is well ordered by inclusion. In particular if α, β are any two ordinals then either $\alpha < \beta$, $\beta < \alpha$ or $\alpha = \beta$. Here $<$ is being used interchangably with $\in$.*

Lemma 1.2.10. *If α is an ordinal then $\alpha + 1 = \alpha \cup \{\alpha\}$ is an ordinal and $\alpha < \alpha + 1$. If γ is an ordinal and A is a collection of ordinals such that $\alpha < \gamma$ for all $\alpha \in A$ then $\beta = \bigcup_{\alpha \in A} \alpha$ is an ordinal and $\beta < \gamma$.*

With these facts in mind we are now able to state the most important results from this section

Theorem 1.2.11 (Transfinite Induction)**.** *Suppose that $P(\alpha)$ is a statement in a variable α. Assume that for every ordinal β we have that*

$$(\forall \alpha < \beta) \, P(\alpha) \implies P(\beta).$$

Then $P(\gamma)$ holds for every ordinal γ.

A proof of this statement can be found in [2] but for our purposes it suffices to notice that this allows us to prove things for all ordinals. In practice, we break this up into cases in a similar fashion to what we do for regular induction on the natural numbers.

1. Does the statement hold for 0

2. Assume that $P(\alpha)$ is true, show that this implies $P(\alpha + 1)$.

3. Suppose that β is a limit ordinal and $P(\alpha)$ holds for all $\alpha < \beta$ show that this implies $P(\beta)$.

This effectively allows us to do induction on ordinals and allows us to perform "induction style" proofs in settings where that might not necessarily be appropriate. We will see more examples of this in the next section.

The last tool that we are going to need from this section are Cardinals. We have an intuitive notion for what it means for finite sets to be of the same size. In particular this is when they have the same number of elements. For infinite sets we need a better criteria for when they are the "same size". Suppose that $(A, <)$ is any well order. By a result in [2] we know that there is a least ordinal α isomorphic to $(A, <)$. We define $|A| = \alpha$.

Definition 1.2.12 (Cardinal)**.** *We say that an ordinal α is a cardinal if $|\alpha| = \alpha$.*

We see that ω is a cardinal, we can define $\omega_1 = \{\alpha : |\alpha| = \omega\}$. In a similar fashion we can define $\omega_2 = \{\alpha : |\alpha| = \omega_1\}$ and so on. Notice that ω_1 is uncountable as if ω_1 was countable then $\omega_1 \in \omega_1$ which is not possible. Similarly for the case of ω_2 and so on. This means that each ω_i has strictly larger cardinality than the previous. In this fashion we can describe the cardinal ω_α for an ordinal α using transfinite induction.

1. The base case is $\omega_0 = \omega$

2. For the successor case suppose that we have defined ω_α then we can define $\omega_{\alpha+1} := \{\beta : |\beta| = \alpha\}$

3. If α is a limit ordinal we can define $\omega_\alpha = \sup_{\beta < \alpha} \omega_\alpha$

Since ordinals and cardinals are fundamentally different things, we want to make that distinction. When talking about the ordinal ω_α we will write it as such. When we are talking about the cardinal ω_α we write it as $\aleph_\alpha$. The important thing from this section to know is that if A is a set and $|A| = \kappa$ then we can "enumerate" this set by considering the ordinal β corresponding to κ and writing $A = \{a_\alpha : \alpha < \beta\}$. This is something that we already do for countable sets. For example we can enumerate $\mathbb{Q}$ by $\{q_1, q_2, \ldots, q_n\}$, we are now just extending that notion to an infinite setting.

1.3 The Back and Forth Method

The actual technique that we are going to use in the proof of Steinitz's Theorem is going to be a combination of transfinite induction, and an analogue of what is known as a back and forth argument.

A back and forth argument is a useful tool in constructing isomorphisms between two structures. In order to talk about these we need to introduce the notion of a partial embedding.

Definition 1.3.1 (Partial Embedding). *Suppose that $\mathcal{M}$ and $\mathcal{N}$ are $\mathcal{L}$ structures. Suppose that $A \subseteq M$ and $B \subseteq N$. We say that $f : A \to B$ is a partial emebedding if $f \cup \{(c^{\mathcal{M}}, c^{\mathcal{N}})\}$ preserves the relations and functions of $\mathcal{L}$*

The general goal now is to build a sequence of partial embeddings $f_0 \subseteq f_1 \subseteq f_2 \subseteq \ldots$ such that $f_i : A_i \to B_i$ with $A_i \subseteq A_{i+1}$ and $B_i \subseteq B_{i+1}$ with the additional property that $\bigcup_{i \in \mathbb{N}} A_n = M, \bigcup_{i \in \mathbb{N}} B_i = N$. Once all of these maps have been defined we will be able to define our isomorphism $f : M \to N$ by simply choosing an appropriate A_n that our input lies in. The question now becomes how do we do this?

Remark 1.3.2. *Notice that all of these are being done in the countable case. This is fine but is a point that we will return to shortly.*

The above process can be formulated in many ways but my personal favourite is to describe it is through the use of games. Suppose that there are two players, at the i-th stage of the game, the first player will "play" either an element $m_i \in M$ or an element $n_i \in N$ and the goal of player 2 is to place this element in the domain by playing an element n_i or m_i respectively. Going back and forth in this way gives a sequene of partial embeddings f_i and sets A_i and B_i satisfying the conditions that we outlined above. Player 2 wins the game if this process can be continued indefinitely thus resulting in a map $f : M \to N$.

Example 1.3.3. *We can now give a much weakened proof of Steinitz's Theorem. Suppose that F and K are countable algebraically closed fields (of characteristic 0). We construct our partial isomorphism as follows. Since we know that both F and K contain $\mathbb{Q}$ as a subfield we let $f_0 : \mathbb{Q} \to \mathbb{Q}$ be our first partial isomorphism. Next we let $M = \{\alpha_i \in F : \alpha_i \notin \mathbb{Q}\}$ and $N = \{\beta_i \in N : \beta_i \notin \mathbb{Q}\}$ be an enumeration of M and N respectively. Now suppose that on turn 1 Player 1 plays $\alpha_1 \in M$ (we take this without loss of generality, as the case for $\beta_1 \in N$ is the same) then by Proposition 1.1.8 there is a $\beta_i \in N$ such that f_0 can be lifted to an isomorphism $f_1 : \mathbb{Q}(\alpha_1) \to \mathbb{Q}(\beta_i)$. So we can take $A_1 = \mathbb{Q}(\alpha_1)$ and $B_1 = \mathbb{Q}(\beta_i)$. At the i-th turn of the game we can do this exact same process again by applying Proposition 1.1.8 regardless of what the first player plays. This gives us a winning strategy for the second player and gives us our result as we needed.*

As we will come to see, the uncountable case is more difficult. The issue now is that we need to keep in mind that there is a limit case we need to account for. Let $\mathcal{M}$, $\mathcal{N}$ be two (uncountably) infinite $\mathcal{L}$ structures such that $|M| = |N| = \kappa$. Let α be the ordinal corresponding to κ. Our goal is going to be to construct sets

$$A_0 \subseteq A_1 \subseteq \ldots \subseteq A_\beta \subseteq M$$

and
$$B_0 \subseteq B_1 \subseteq \ldots \subseteq B_\beta \subseteq N$$

and a sequence of partial isomorphisms $f_0 \subseteq f_1 \subseteq \ldots f_\beta \subseteq \ldots$. With these we would have a full isomorphism $f : \bigcup_{\beta < \alpha} A_\beta \to \bigcup_{\beta < \alpha} B_\beta$ where $f = \bigcup_{\beta < \alpha} f_\beta$ will be our full isomorphism. We notice that this is the exact same thing that we want from above. It is more difficult to formulate this in terms of games. However coming up with such a construction suffices for us to prove that these two sets are isomorphic.

2 Steinitz's Theorem

We now know enough to begin proving Steinitz's Theorem. First let's recall the statement of Theorem 1.0.1

Theorem 1.0.1 (Steinitz's Thoerem). *If M and N are algebraically closed fields of characteristic 0 such that $|M| = |N| = \aleph_0$ then $M \cong N$.*

Next we recall the following two results from Section 1.1.

Proposition 1.1.8. *If F and K are fields and there is an isomorphism $\phi : F \to K$ then if α is algebraic over F then there is a β algebraic over K such that ϕ can be extended to an isomorphism $\overline{\phi} : F(\alpha) \to K(\beta)$*

Proposition 1.1.18. *Let F, K, M, N be fields such that $|M| = |N|$ and M (resp. N) is a trancendental extension of F (resp. K) and $|F| < |M|$ (resp $|K| < |N|$) then if $\phi : F \to K$ is an isomorphism and $\alpha \in M \setminus F$ is transendental over F there is a $\beta \in N \setminus K$ such that ϕ can be extended to an isomorphism $\overline{\phi} : F(\alpha) \to K(\beta)$.*

The first result allows us to create algebraic extensions, the next one allows us to create transcendental extensions. Combining these two results with the back and forth method and transfinite induction is going to enable us to give a proof of Theorem 1.0.1

Proof of Theorem 1.0.1. Suppose that M and N are algebraically closed fields of characteristic 0 such that $|M| = |N| = \kappa > \aleph_0$. We enumerate M and N as

$$M = \{a_\alpha : \alpha < \kappa\} \qquad and \qquad N = \{b_\alpha : \alpha < \kappa\}.$$

We now wish to construct a sequence of field extensions $E_0 \subseteq E_1 \subseteq E_\alpha \subseteq \ldots \subseteq M$ and $K_0 \subseteq K_1 \subseteq \ldots \subseteq K_\alpha \subseteq N$ as well as a sequence of functions $f_0 \subseteq f_1 \subseteq \ldots f_\alpha \subseteq \ldots$ such that $f_\alpha : E_\alpha \to K_\alpha$ is a partial isomorphism. Since M and N are of characteristic zero we know that both of their prime fields are $\mathbb{Q}$. This gives us our base case $f_0 : \mathbb{Q} \to \mathbb{Q}$ which is given by the identity map (as there are no non-trivial automorphisms of $\mathbb{Q}$).

Next we handle the successor case. Let $\beta = \alpha + 1$. Suppose that we have constructed subfields E_α and K_α as well as an isomorphism $f_\alpha : E_\alpha \to K_\alpha$. We are going to do both the back and the forth part in one step. First suppose that $b_\beta \in N \setminus K_\alpha$ then by either Proposition 1.1.8 or Proposition 1.1.12 there is an $a \in M \setminus E_\alpha$ and an extension $f'_\alpha : E_\alpha(a) \to K_\alpha(b)$. Now suppose that $c \in M \setminus E_\alpha(a)$ then once again by the appropriate proposition there is a $d \in N \setminus K_\alpha(b)$ and an extension $f''_\alpha : E_\alpha(c) \to E_\alpha(d)$. Thus we can take $f_\beta = f''$ and $E_\beta = E_\alpha(c)$ and $K_\beta = K_\alpha(d)$. As we needed.

Lastly in the limit case we can take $f_\alpha = \bigcup_{\beta < \alpha} f_\beta$, $E_\alpha = \bigcup_{\beta < \alpha} E_\beta$ and $K_\alpha = \bigcup_{\beta < \alpha} K_\beta$.

Therefore using transfinite induction we can define this recursively for all ordinals (including κ). The resulting function is an isomorphism as a union of partial isomorphisms. As we needed. $\square$

References

[1] David S. Dummit and Richard M. Foote. *Abstract algebra*. Wiley, New York, 3rd ed edition, 2004.

[2] Ernest Schimmerling. *A Course on Set Theory*. Cambridge University Press, Cambridge, England, July 2011.