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. □

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)**.** *Let E be a field extension of F and suppose that $\alpha \in E$ is algebraic over F. We define $F(\alpha)$ to be the smallest subfield of E contaning both F and α.*

Another way to work with algebraic extensions is to notice that $F(\alpha)$ is all of the polynomials in α, namely expressions of the form $a_0 + a_1\alpha + \ldots + a_n\alpha^n$.

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. Going forward we assume that all fields are contained in some universal algebraically closed field. In the characteristic zero case this is the complex numbers. This allows us to say things like, let α be algebraic over F without concerning ourselves with where α comes from.

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 we can lift ϕ to 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 $\phi : F \to K$ and 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 $m_\alpha(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 \in F[x]$. Now since ϕ is an isomorphism of fields we get an irreducible polynomial

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

Notice that since this polynomial is irreducible it is the minimal polynomial of some β algebraic over K. Now consider the map $\overline{\phi} : F(\alpha) \to K(\beta)$ given by

$$a_0 + a_1\alpha + \ldots + a_n\alpha^n \mapsto \phi(a_0) + \phi(a_1)\beta + \ldots + \phi(a_n)\beta^n.$$

We now need to verify that this is an isomorphism. The fact that this is well defined is clear ϕ is well defined and that elements in $F(\alpha)$ are uniquely represented by their coefficients. We see that this function is also a bijection since we can give an inverse

$$b_0 + b_1\beta + \ldots + b_n\beta^n \mapsto \phi^{-1}(b_0) + \phi^{-1}(b_1)\beta + \ldots \phi^{-1}(b_n)\beta^n.$$

This inverse is well defined for the same reasons as above and thus ϕ is an isomorphism as we needed. □

Moving on from algebraic numbers we are now interested in exploring the second class, trancendental numbers. These are all numbers which are not the root of any polynomial over the ground field. In particular if E is a field extension of F, $\alpha \in E$ is trancendental if it is not algebraic 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 1.1.9. *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 chocies for coefficients. Thus there are at most $|F|$ many algebraic numbers. □

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

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

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

Lemma 1.1.11. *If F is a field and β is trancendental over F then $F(x) \cong F(\beta)$*

Proof. 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 □

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

Lemma 1.1.12. *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. □

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

Proposition 1.1.13. *Let M and N be field extensions of F and K respectively. If $\phi : F \to K$ is an isomorphism and $\alpha \in M \setminus F$ is trancendental over F then there is $\beta \in N \setminus K$ which is trancendental over 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 1.1.9 there is an element β which is trancendental over K. Now by Lemma 1.1.11 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 1.1.12 there is an isomorphism $\phi' : F(x) \to K(x)$ which lifts ϕ to an isomorphism between the rational polynomials. From these we get the following diagram:

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

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

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. Suppose we have a set X recall that a linear order is a relation $<$ on X satisfying the following properties:

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 $y < x$.

We are going to focus on a specific type of linear order known as a well order.

Definition 1.2.1 (Well-Orders)**.** *A linear order $(X, <)$ is said to be a well order if every $S \subseteq X$ has a minimal element.*

If $(X, <_X)$ and $(Y, <_Y)$ are linear orders we say that a bijective map $\phi : X \to Y$ is an isomorphism of linear orders if for all $x, y \in X$ we have that if $x < y$ then $\phi(x) < \phi(y)$. We say that $(X, <_X), (Y, <_Y)$ are isomorphic if there is a linear order isomorphism between them.

Something that is worth noting is that one consequence of the axiom of choice is known as the Well Ordering Principle. The well ordering principle states that on every set there exists an ordering which is a well ordering. Notice that neither $\mathbb{Q}$ nor $\mathbb{Z}$ are well orders in their usual ordering as they don't have a least element. The well ordering principle tells us that there exist orderings on both $\mathbb{Q}$ and $\mathbb{Z}$.

Next let 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.

$$\begin{aligned} 0 &= \{\} \\ 1 &= \{\{\}\} \\ 2 &= \{\{\}, \{\{\}\}\} \\ 3 &= \{\{\}, \{\{\}, \{\{\}\}\}\}. \end{aligned}$$

Or we can re-write this as

$$\begin{aligned} 0 &= \{\} \\ 1 &= \{0\} \\ 2 &= \{0, 1\} \\ 3 &= \{0, 1, 2\}. \end{aligned}$$

Notice that these sets have the property that containment and inclusion are the same thing. For example $2 \in 3$ and $2 \subseteq 3$ based on how 2 and 3 are defined. This is what is known as a transitive set.

Definition 1.2.2 (Transitive)**.** *A set X is said to be transitive if whenever $x \in X$ then $x \subseteq X$.*

We are now able to give the defintion of an ordinal.

Definition 1.2.3 (Ordinal)**.** *An ordinal is a transitive set α such that $(\alpha, \in)$ is a well-ordering.*

Lemma 1.2.4. *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 $\in$.*

Ordinals, as the name implies, are designed to capture and extend the notion of "order" beyond just the natural numbers. Indeed if we take any well ordering $(A, <)$ there is a unique ordinal α which is isomorphic to A. So any well ordered set corresponds to a unique ordinal.

There are two types of ordinals, successor and limit. We say that α is a successor ordinal if $\alpha = \beta + 1 = \beta \cup \{\beta\}$ for some ordinal β. We say that α is a limit ordinal if $\alpha = \bigcup_{\beta < \alpha} \beta$. To illustrate this consider the natural numbers ω. Notice that each natural number is a successor ordinal for example $2 = 1 + 1$, $3 = 2 + 1$, and so on. However the ω itself is a limit ordinal as $\omega = \bigcup_{n \in \mathbb{N}} n$.

Lemma 1.2.5. *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 $\beta < \gamma$.*

The details about how ordinals work can be found in [2] however for our purposes we are simply going to assume the above facts about ordinals. With these facts in mind we are now able to state the most important results from this section

Theorem 1.2.6 (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 want to relate our usual notion of cardinality to the above discussion about ordinals. Recall that two sets have the same cardinality if there is a bijection between them. Now let A be a set, by the well ordering principle we can assign A a well ordering $<$. We define the cardinality of A, denoted $|A|$, to be the least ordinal α in bijection with A. The importance of cardinals for our purposes is that they are going to allow us "enumerate" sets, similar to how one would enumerate $\mathbb{Z}$ or $\mathbb{Q}$. Suppose that $|A| = \kappa$ then since κ is an ordinal we can enumerate A as $\{a_\alpha : \alpha < \kappa\}$.

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 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?

The above process can be formulated in many ways but we are going to be using 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 sequence 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 $f : M \to N$.

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. Suppose that $\mathcal{M}, \mathcal{N}$ are two (uncountably) infinite $\mathcal{L}$ structures such that $|M| = |N| = \kappa$. 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 $f : \bigcup_{\beta<\kappa} A_\beta \to \bigcup_{\beta<\kappa} B_\beta$ where $f = \bigcup_{\beta<\kappa} f_\beta$ 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 $\phi : F \to K$ and 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 1.1.13. *Let M and N be field extensions of F and K respectively. If $\phi : F \to K$ is an isomorphism and $\alpha \in M \setminus F$ is trancendental over F then there is $\beta \in N \setminus K$ which is trancendental over 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

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

We now wish to construct a sequence of field extensions $E_0 \subseteq E_1 \subseteq E_\alpha \subseteq \ldots \subseteq M$ and $K_0 \subseteq K_1 \subseteq \ldots \subseteq K_\alpha \subseteq N$ such that $|E_\alpha|, |K_\alpha| < \kappa$ 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 1.1.9 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. □

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.