CHAPTER X

INFINITE EXTENSIONS

1. The Algebraic Closure

Recall that a field K is algebraically closed if every non-constant polynomial over K splits into linear factors. We have referred earlier to the fact that for any field F there is an algebraic extension of F which is algebraically closed. We now propose to show that such an extension exists and moreover it is unique up to an isomorphism fixing F.

THEOREM. *Let F be a field. There is an algebraic extension Ω of F which is algebraically closed.*

PROOF. At first glance this theorem looks like a good candidate for Zorn's Lemma. That is, we could order algebraic extensions of F by inclusion, show that the set of all such is inductively ordered, and pick a maximal element—which by rights should be algebraically closed. Unfortunately, the 'set of all algebraic extensions of F'is one of those very large sets which leads us directly to one or the other self referential paradoxes like Russell's Paradox. One can get around this difficulty by only looking at fields which are subsets of an appropriate 'ordinary set'which is large enough for the proof to work. (See *Commutative Algebra*, vol. I by Zariski and Samuel for such a proof.) Instead, we shall use a proof originally due to Artin which we take from Lang' s *Algebra*.

Let S be a set in one-to-one correspondence with the set of all non-constant polynomials in $F[X]$. Taking S as a set of indeterminates, form the ring $A = F[S]$. If $f \in F[X]$ is not constant, we denote by X_f the indeterminate corresponding to f. For such an f, we can form $f(X_f)$ the polynomial in X_f obtained by replacing the indeterminate X in $f = f(X)$ by X_f. Let $\mathfrak{a}$ be the ideal in A generated by all $f(X_f)$ as f ranges over all non-constant polynomials in $F[X]$.

LEMMA. $A \neq \mathfrak{a}$.

PROOF OF LEMMA. Suppose $A = \mathfrak{a}$. Then 1 can be written

$$1 = \sum_{i=1}^{n} g_i(S) f_i(X_i)$$

where we have abbreviated the indeterminate associated to f_i by X_i. The polynomials $g_i(S)$ can in fact involve only finitely many indeterminates, and we suppose those not already accounted for by $X_1, X_2, \ldots, X_n$ are renamed $X_{n+1}, \ldots, X_m$. This yields an equation in $F[X_1, \ldots, X_m]$

$$1 = \sum_{i=1}^{n} g_i(X_1, \ldots, X_m) f_i(X_i)$$

Put $X_{n+1} = \cdots = X_m = 0$ in this relation, so we obtain a similar relation in $F[X_1, \ldots, X_n]$. Let E be a splitting field for $f_1(X) f_2(X) \ldots f_n(X)$ over F. Choose roots y_i for $f_i(X)$ in K. If we put $X_i = y_i$ in K, we obtain from the above equation, the equation

$$1 = 0$$

which is nonsense. □

To continue with the proof of the theorem, choose a maximal proper ideal $\mathfrak{m}$ containing $\mathfrak{a}$. (We proved earlier using Zorn's Lemma that such an ideal exists.) Let $M = A/\mathfrak{m}$, and imbed F in M by associating with $a \in F$ the image of the constant polynomial a in $A = F[S]$. By construction, any nonconstant polynomial $f(X) \in F[X]$ has a root in M. For, $f(X_f) \equiv 0 \bmod \mathfrak{m}$ (since $f(X_f) \in \mathfrak{a} \subseteq \mathfrak{m}$.) Hence, in $A/\mathfrak{m}$, we have $f(X_f + \mathfrak{m}) = 0$, i.e. the coset of X_f is the desired root.

Let $M_1 = M$, and iterate the above process to form an extension $M_2 \supseteq M_1$ such that every nonconstant polynomial in $M_1[X]$ has a root in M_2. Continue in this way and form a tower of fields

$$M_1 \subseteq M_2 \subseteq \cdots \subseteq M_k \subseteq \ldots$$

such that every nonconstant polynomial in $M_k[X]$ has a root in M_{k+1}. Let M be the union of this tower of fields. It is clear how to make M into a field, and it has the property that every non-constant polynomial in $M[X]$ (which must have coefficients in some M_k) has a root in M. From this it follows easily that M is algebraically closed. To complete the proof of the theorem let Ω be the subfield of M consisting of all elements which are algebraic over F. Ω is algebraically closed, since any nonconstant polynomial splits in some (finite) extension contained in M and since that extension is algebraic over Ω, it is also algebraic over F so it is already contained in Ω. □

THEOREM. *Let $\Omega \supseteq F$ and $\Omega' \supseteq F$ be algebraically closed algebraic extensions of F. There is an isomorphism $\sigma : \Omega \to \Omega'$ which fixes F.*

PROOF. We use Zorn's Lemma. (Note that set theoretic difficulties do not arise because we need only consider functions between subsets of previously given sets.) Consider monomorphisms $\tau : E \to \Omega'$ where $E \supseteq F$ and τ fixes F. Order such monomorphisms by the relation $\tau < \tau'$ if τ' extends τ. It is easy to check that these monomorphisms form an inductively ordered set. Hence, there is a maximal element $\sigma : L \to \Omega'$. We must have $L = \Omega$. For, otherwise, we can form a finite extension $L[x] \subseteq \Omega$. If $g(X) \in L[X]$ is the minimal polynomial of x over L, then $\sigma(g(X))$ must have a root x' in Ω' since the latter is algebraically closed. Thus by our basic extension theorem, we may extend σ to $\sigma' : L[x] \to \sigma(L)[x'] \subseteq \Omega'$ thus contradicting the maximality of σ. Finally, σ is onto Ω'. For, $\sigma(\Omega)$ is certainly an algebraically closed extension of F and since $\Omega' \supseteq \sigma(\Omega)$ is algebraic, it follows that $\Omega' = \sigma(\Omega)$. □

Note. The above theorem may be extended as follows: Any isomorphism $\tau : F \cong F'$ may be extended to an isomorphism $\sigma : \Omega \cong \Omega'$ of any algebraic closures of those fields. The proof is basically the same. In particular, any isomorphism of subfields of an algebraically closed field may be extended to an automorphism of the enclosing field. (We have only proved this in the case that the large field is an algebraic extension of the smaller fields, but it is in fact true in general.)

Exercises.

1. (a) Suppose that every polynomial of odd degree in F has a root in F. Let $K \supseteq F$ be a finite normal separable extension. Show that $G(K/F)$ is a 2-group. (**Hint:** Use Sylow's theorem to find an intermediate field such that $[L : F]$ is odd.)

(b) Let K be a finite normal extension of $\mathbf{R}$ which also contains $\mathbf{C}$. How do you know there is such an extension and why does (a) apply to this extension? Show that there is an intermediate subfield L such that $[L : \mathbf{C}] = 2$ and conclude $L = \mathbf{C}[\alpha]$ where $\alpha^2 \in \mathbf{C}$. (Why can you conclude that?) Show that $L = \mathbf{C}$.

(c) Why can you now conclude that $\mathbf{C}$ is algebraically closed? Hint: You may establish (a) for $\mathbf{R}$ using elementary analysis. (There exist purely algebraic proofs of this fact, but they are more involved. See Lang for his discussion of totally real fields, for example.)

2. Transcendental extensions

Let k be a field and suppose Ω is a field containing k. Let S be a subset of Ω and let $\tilde{S}$ be a set of indeterminates in one to one correspondence with S. We say that S is *algebraically independent* over k if the mapping $\tilde{X} \to x$ (where $\tilde{X}$ is the indeterminate corresponding to $x \in S$) induces an isomorphism $k[S] \to k[S]$. In other words, if $x_1, \ldots, x_n \in S$ then $f(x_1, \ldots, x_n) = 0$ in Ω if and only if the polynomial $f(X_1, \ldots, X_n)$ is

trivial. In that case, we may extend the above isomorphism to an isomorphism of fields $k(\tilde{S}) \cong k(S)$. (The right hand side the the field of rational functions in the—possibly infinite—set of indeterminates $\tilde{S}$.)

If S is an algebraically independent over $k \subseteq \Omega$ and $\Omega = k(S)$, then we say that Ω is a *purely transcendental* extension. More generally, if Ω is algebraic over $k(S)$, where S is algebraically independent over k, we call S a *transcendence basis* for Ω over k. This concept is similar to the definition of a (linear) basis for a vector space over a field except that we require the set to be algebraically independent rather than linearly independent. The theorems about transcendence bases parallel those about (linear) bases.

THEOREM. *Let k be a field and let $\Omega \supseteq k$ be an extension. There exists a transcendence basis S for Ω over k.*

PROOF. Let T be any subset of Ω such that $\Omega = k(T)$. Consider the collection of all algebraically independents subsets U of T, and order it by inclusion. This collection is nonempty because the null set is trivially algebraically independent. Moreover, the collection is inductively ordered. (Prove it!) Hence, by Zorn's Lemma, there is a maximal algebraically independent subset S of T. We claim that Ω is algebraic over $k(S)$. To see this, it suffices to show that every $y \in T$ is algebraic over $k(S)$. However, by maximality we know that $S \cup \{t\}$ is not algebraically independent. Hence, we can find a non-trivial polynomial $f(X_1, \ldots, X_n, Y)$ in appropriate indeterminates such that

$$f(x_1, \ldots, x_n, y) = 0$$

for some $x_1, \ldots, x_n \in S$. Collect terms involving the same power of Y to rewrite this

$$f_0(x_1, \ldots, x_n)y^k + f_1(x_1, \ldots, x_n)y^{k-1} + \cdots + f_k(x_1, \ldots, x_n) = 0$$

where we may assume that $f_0(X_1, \ldots, X_n)$ is nontrivial. By algebraic independence, it follows that

$$f_0(x_1, \ldots, x_n) \neq 0,$$

so we may divide to get

$$y^k + (f_1(x_1, \ldots, x_n)/f_0(x_1, \ldots, x_n))y^{k-1} + \cdots + f_k(x_1, \ldots, x_n)/f_0(x_1, \ldots, x_n) = 0$$

which shows that y is algebraic over $k(S)$. □

Note that in the above proof, it we can find a finite set T such that $\Omega = k(T)$, then the maximal algebraically independent set S is also finite.

EXAMPLE. The above theorem tells us that $\mathbf{C}$ is an algebraic extension of a purely transcendental extension $\mathbf{Q}(S)$ of $\mathbf{Q}$. In this case S must be *uncountable*. For, it is easy to see that if S were countable, $\mathbf{Q}(S)$ would also be countable. Since it is also true that any algebraic extension of a field K must have the same cardinality as K (why?), if S were countable so also would $\mathbf{C}$ be countable.

The cardinality of a transcendence basis for Ω over k is called the *transcendence degree* of Ω over k. It is an analogue of the concept of the dimension of a vector space over a field. As in the vector space case, we must show that this concept is well defined, which is a consequence of the following result.

THEOREM. *Let $\Omega \supseteq k$ be a field extension and suppose S and S' are transcendence bases for Ω over k. Then S and S' have the same cardinality.*

PROOF. We do the proof in case one of the sets—say S—is finite. The case in which both sets are infinite requires familiarity with transfinite methods.

Let $S = \{x_1, \ldots, x_n\}$, and let $\{y_1, \ldots, y_m\}$ be any other algebraically independent set. We shall show that $m \leq n$. Clearly that suffices to prove the theorem since we may reverse the roles of the two sets if Ω is algebraic over $k(y_1, \ldots, y_m)$.

By assumption, Ω is algebraic over $k(x_1, \ldots, x_n)$ so y_1 is algebraic over it. Hence, there is a relation

$$y_1^r + c_1 y_1^{r-1} + \cdots + c_r = 0$$

where $c_1, \ldots, c_r \in k(x_1, \ldots, x_n)$. Since the c_i are rational functions in the x's, we may multiply through by a common denominator to obtain a polynomial relation

$$f(y_1, x_1, \ldots, x_n) = 0.$$

Consider subsets of $\{x_1, \ldots, x_n\}$ which appear in such relations, and choose one as small as possible. Renumber the elements if necessary and suppose $\{x_1, \ldots, x_k\}$ is such a subset. Then $k > 0$ or else y_1 would be algebraic over k, and every x_i actually appears in the relation. Rewrite it

$$f_0(y_1, x_2, \ldots, x_k)x_1^r + f_1(y_1, x_2, \ldots, x_k)x_1^{r-1} + \cdots + f_r(y_1, x_2, \ldots, x_k) = 0.$$

$f_0(y_1, x_2, \ldots, x_k) \neq 0$ since the set of x's appearing in the original relation was minimal. Hence we can divide by it and thereby show that x_1 is algebraic over $k(y_1, x_2, \ldots, x_n)$. Since $x_2, \ldots, x_n$ are also certainly algebraic over $k(y_1, x_2, \ldots, x_n)$, it follows that $k(x_1, x_2, \ldots, x_n)$ is algebraic over $k(y_1, x_2, \ldots, x_n)$, and hence so is Ω. $\{y_1, x_2, \ldots, x_k\}$ is also algebraically independent. Otherwise, there would be a polynomial relation

$$g(y_1, x_2, \ldots, x_n) = 0.$$

y_1 would have to occur in this relation since otherwise $\{x_2, \ldots, x_n\}$ would be algebraically dependent. However, in that case y_1 would be algebraic over $k(x_2, \ldots, x_n)$ and hence so would x_1— which is nonsense.

Suppose in general we have shown that $\{y_1, \ldots, y_i, x_{i+1}, \ldots, x_n\}$ is an algebraically independent set, after suitable renumbering, such that Ω is algebraic over the field it generates. Then y_{i+1} is algebraic over this field, and as above, we choose a relation

$$f(y_1, \ldots, y_i, y_{i+1}, x_{i+1}, \ldots, x_n) = 0.$$

Choose such a relation involving as small a subset of $\{x_{i+1}, \ldots, x_n\}$ as possible. The above argument may be repeated to conclude that $\{y_1, \ldots, y_{i+1}, x_{i+2}, \ldots, x_n\}$ is algebraically independent and Ω is algebraic over the field it generates. If $m > n$ then eventually we would run out of x's, and we could conclude that y_{n+1} is algebraic over $k(y_1, \ldots, y_n)$ which is nonsense. □

The basic theory of transcendental extensions parallels in part the theory of algebraic extensions but with some differences. For example, transcendence degrees add when we further extend rather than multiply. We won't pursue the subject further at this time. However, the student should be aware than transcendence degree plays an extremely important role in commutative algebra and algebraic geometry.

Exercises.

1. (a) Let $L \supseteq F$ be subfields of the field Ω. Suppose S is an algebraically independent over F subset of Ω. Show that if L is algebraic over F then $L(S)$ is algebraic over $F(S)$.

(b) Assume $\Omega \supseteq F$ and let S and T be subsets of Ω. Show that if S is algebraically independent over F and T is algebraically independent over $F(S)$ then $S \cup T$ is algebraically independent over F.

(c) Suppose $\Omega \supseteq L \supseteq F$ and that the transcendence degree n of L over F and the transcendence degree m of Ω over L are finite. Show that the transcendence degree of Ω over F is $n + m$.

2. (a) Show that the only automorphism of $\mathbf{R}$ is the identity. Hint: First show that any *continuous* automorphism is the identity by using the fact that $\mathbf{Q}$ is dense in $\mathbf{R}$. Why must it be the identity on $\mathbf{Q}$? Then show that every automorphism of $\mathbf{R}$ must preserve order and hence must be continuous. (Why is an order preserving bijection of $\mathbf{R}$ continuous? Is any order preserving transformation continuous?)

(b) Show that the only automorphisms of $\mathbf{C}$ which fix $\mathbf{R}$ are complex conjugation and the identity.

(c) Show that there are infinitely many automorphisms of $\mathbf{C}$ which do not fix $\mathbf{R}$. Hint: Write $\mathbf{C}$ as an algebraic extension of a purely transcendental extension $\mathbf{Q}(S)$ where S is an algebraically independent set. (This will use the general case of the appropriate theorem although we only proved the theorem in the finitely generated case.) Using cardinality considerations, show S must be infinite (even nondenumerable.) Construct infinitely many automorphisms of $\mathbf{Q}(S)$ and extend these to $\mathbf{C}$ quoting the appropriate theorem discussed in the text. (Again, the actual case you will use was mentioned but proved only in case of extensions of finite degree.)