Part VI (§29-33) Extension Fields

Satya Mandal

University of Kansas, Lawrence KS 66045 USA

January 22

29 Introduction to Extension Fields

Example 29.1. The polynomial $f(x) = x^2 + 1$ does not have a solution in $\mathbb{R}$, but it has a solution in the bigger field $\mathbb{C}$.

The author has been working to develop similar theorems for any field F.

Definition 29.2. *Let F, E be two fields. If F is a subfield of E, then E is called an* **extension field** *of F. I write $\hookrightarrow E$ is an* **extension of fields** *to mean the same.*

Examples:

1. $\mathbb{R}$ is an extension field of $\mathbb{Q}$.
2. $\mathbb{C}$ is an extension field of $\mathbb{Q}$.
3. $\mathbb{C}$ is an extension field of $\mathbb{R}$.
4. Suppose F is any field and $F[x]$ the polynomial ring. Let $F(X)$ be the quotient field of $F[x]$. Then, $F(X)$ is an extension field of F.

The following has been author's primary goal for some time.

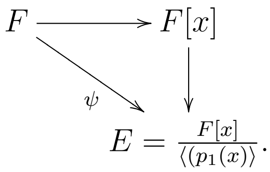
Theorem 29.3 (29.3 Kronecker's Theorem)**.** *Let F be a field and $f(x)$ be a nonconstant polynomial in $F[x]$. Then there is an extension field E of F so that $f(x)$ has a root in E.*

Proof. By theorem 23.20, $f(x) = p_1(x)p_2(x)\cdots p_r(x)$, where p_i are irreducible polynomials in $F[x]$. Write $E = \frac{F[x]}{\langle(p_1(x)\rangle}$. Now, $\langle(p_1(x)\rangle$ is a maximal ideal and so E is a field.

1. The map

$$\psi : F \longrightarrow E \quad defined\ by \quad \psi(a) = a + \langle p_1(x)\rangle$$

   is an injective homomorphism. In fact, ψ is the composition of two homomorphisms, as given by the commutative diagram:



   To prove it is injective, we need to show that the kernel is $\{0\}$. So, let $\psi(a) = \langle p_1(x)\rangle$. This means $a + \langle p_1(x)\rangle = \langle p_1(x)\rangle$ or $a \in \langle p_1(x)\rangle$. So, $a = \lambda(x)p_1(x)$ for some $\lambda(x) \in F[x]$. Comparing degrees, we have $\lambda(x) = 0$ and hence $a = 0$. So, ψ is injective.

   Identifying, F with $\psi(F) \subseteq E$, we have F is a subfield of E.

2. **Important Notation**: For $g \in F[x]$, we denote, its coset $\overline{g} := g + \langle p_1(x)\rangle \in E$.
   Because of the identification of F with $\psi(F)$, notationally, we have $\forall\ a \in F,\ a = \overline{a}$.

3. Now, write $p_1(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ and $\alpha = \overline{x} = x + \langle p_1(x)\rangle$. We have

$$\begin{aligned} p_1(\alpha) = p_1(\overline{x}) &= a_0 + a_1\overline{x} + a_2\overline{x}^2 + \cdots + a_n\overline{x}^n \\ &= \overline{a_0 + a_1x + a_2x^2 + \cdots + a_nx^n} = \overline{p_1(x)} = 0 \end{aligned}$$

   So, α is a zero of $p_1(x)$ in E and hence is a zero of $f(x)$ in E.

The proof is complete. ∎

Example 29.4 (29.4). *We know $f(x) = x^2 + 1$ is irreducible in $\mathbb{R}[x]$. According to the above proof, in the field $E = \frac{\mathbb{R}[x]}{\langle x^2+1\rangle}$ the element $\alpha = x + (f(x))$ is a root of $f(x)$. Also establish an isomorphism*

$$E = \frac{\mathbb{R}[x]}{\langle x^2 + 1\rangle} \approx \mathbb{C}.$$

Example 29.5 (29.5). *Let $f(x) = x^4 - 12x^2 + 35 \in \mathbb{Q}[x]$. We have a factorization*
$f(x) = (x^2 - 5)(x^2 - 7)$ in $\mathbb{Q}[x]$. However, $f(x)$ does not factor any further in $\mathbb{Q}[x]$.

1. *In $E = \frac{\mathbb{Q}[x]}{\langle x^2-5\rangle}$, with $\alpha = x + ((x^2 - 5))$, it factors as $f(x) = (x - \alpha)(x + \alpha)(x^2 - 7)$ in $E[x]$.*

2. *Check, $E \approx \mathbb{Q}[\sqrt{5}] = \mathbb{Q} \oplus \mathbb{Q}\sqrt{5}$.*

3. *In $E' = \frac{E[x]}{\langle x^2-7\rangle}$, with $\beta = x + \langle x^2 - 7\rangle$, it factors as*

$$f(x) = (x - \alpha)(x + \alpha)(x - \beta)(x + \beta),$$

in to linear factors, in $E'[x]$.

Devine Goals: In example 29.5, we started with a polynomial in $\mathbb{Q}[x]$ and constructed an field extension E' of $\mathbb{Q}$ so that $f(x)$ factors into linear factors in $E'[x]$. This is same as saying that $f(x)$ has four roots in E'.

1. This is a typical process that we would like to immitate for any field F and any polynomial $f(x) \in F[x]$.

2. Better still, given any field F, we would like to construct an extension E', so that all polynomials in $F[x]$ factors into linear factors in $E'[x]$.

3. Even better is to find an extension E' of F so that all polynomial in $E'[x]$ factors in to linear factors in $E'[x]$. In fact, $\mathbb{C}$ is such an extension of $\mathbb{R}$ or $\mathbb{C}$. Such a field E' will be called **algebraically closed field**.

29.1 Algebriac and Trancendental Elements

Definition 29.6. *Let $F \hookrightarrow E$ be a field extension and $\alpha \in E$.*

1. *We say that α is* **algebraic** *over F, if*

$$f(\alpha) = 0 \quad for\ some \quad 0 \neq f(x) \in F[x].$$

2. *We say α is* **trancendental** *over F, if it is not algebraic over F.*

Example 29.7. Reading Assignment: *§29 all Examples.*

1. *(29.7) $\sqrt{2}$ is algebraic over $\mathbb{Q}$.*

2. *(29.9) π, e are trancendetal over $\mathbb{Q}$.*

Definition 29.8. *Let $\alpha \in \mathbb{C}$. We say α is an* **algebraic number**, *if it is algebraic over $\mathbb{Q}$.*

Theorem 29.9. *Let $F \hookrightarrow E$ be a field extension and $\alpha \in E$. Define the evaluation map*

$$\varphi_\alpha : F[x] \longrightarrow E \quad by \quad \varphi_\alpha(f(x)) = f(\alpha).$$

Then α is trnacedental if and only if φ_α is injective.

Proof. Execise.

The following is "irreducible polynomial" of α.

Theorem 29.10 (Thm29p13)**.** *Let $F \hookrightarrow E$ be a field extension and $\alpha \in E$ be algebraic over F. Then, there is a polynomial $p(x) \in F[x]$, with the following properties:*

1. *$p(\alpha) = 0$.*

2. *$p(x)$ is irreducible.*

3. *For any polinomial* $f(x) \in F[x]$, $f(\alpha) = 0 \Longrightarrow p(x)|f(x)$ *in* $F[x]$.

4. *This irreducible polynomial* p *is determined uniquely upto a unit in* F. In fact, any polynomial q of minimal degree, with the property $q(\alpha) = 0$ will satisfy the above properties of p.

Proof. Since α is algebraic over F, there are nonzero polynomials $f(x) \in F[x]$ such that $f(\alpha) = 0$. Let

$$d = \min\{n \in \mathbb{Z}^+ : f(\alpha) = 0, for\ some \quad f \in F[x] \quad with \quad \deg(f) = n\}.$$

Let $p(x)$ be one with minimal degree (i.e. $\deg(p) = d$) such the $p(\alpha) = 0$.

1. To see that $p(x)$ is irreducible, use contrapositive argment. Write $p(x) = q(x)g(x)$ where $q, g \in F[x]$ are nonconstant. Then $0 = p(\alpha) = q(\alpha)g(\alpha)$ So, either $q(\alpha) = 0$ or $g(\alpha) = 0$. Since degree of both are less than d, it contradicts the minimality of degree of p. So, (1), (2) are established.

2. Suppose $f(\alpha) = 0$ for some $f(x) \in f[x]$. By division algorithm

$$f(x) = q(x)p(x) + r(x) \quad for\ some \quad q(x), r(x) \in F[x]$$

$$and \quad r(x) = 0\ or\ degree(r(x)) < d.$$

By substituting:

$$0 = f(\alpha) = q(\alpha)p(\alpha) + r(\alpha) = r(\alpha).$$

By minimality of p, $r(x) = 0$. So $f(x) = q(x)p(x)$. So, (3), is established.

3. Now, if $q(x) \in F[x]$ is another irreducible polynomial, wirh $q((\alpha)) = 0$, then by (3), $q(x) = u(x)p(x)$. Since $q(x)$ is irreducible $u(x) = u \in F$ must be a unit.

The proof is complete. ∎

Definition 29.11. *Let F be a field.*

1. *A polynomial $f(x) \in F[x]$ with degree$(f) = n$ is called a* **monic polynomial**, *if the coefficient of the top-degree term x^n is 1. So a monic polnomial looks like*

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

2. *Let $F \hookrightarrow E$ be a extension of fields. and $\alpha \in E$ be algebraic over F. The monic irreducible polynomial $p(x)$ give by theorem 29.10 is called the* **irreducible polynomial for** *α over F.*
   It is also called the **minimal monic polynomial** *of α over F.*
   It is denoted by $irr(\alpha, F)$.

3. *The degree of this polynomial is also called the* **degree of** α **over** F *and denoted by $deg(\alpha, F)$.*

Example 29.12 (19p14)**.** We have

$$irr(\sqrt{2}, \mathbb{Q}) = x^2 - 2, \quad irr(\sqrt{2}, \mathbb{R}) = x - \sqrt{2}.$$

Exercise. Find the irreducible polynomila of $\alpha = \sqrt{1+\sqrt{3}}$ over $\mathbb{Q}$.

29.2 Simple Extensions

Definition 29.13. *Let $F \hookrightarrow E$ be a field extension. We say E is a* **simple extension** *of F, if there is an $\alpha \in E$ such that E is the smallest subfield of E generated by F and α. This means, if K is a subfield of E:*

$$F \subseteq K, \ \alpha \in K \quad \Longrightarrow \quad K = E.$$

Theorem 29.14 (page 270)**.** *Let $F \hookrightarrow E$ be a field extension and $\alpha \in E$. Define the evaluation map*

$$\varphi_\alpha : F[x] \longrightarrow E \quad by \quad \varphi_\alpha(f(x) = f(\alpha).$$

Then image of φ_α is given by

$$\varphi_\alpha(F(x]) = \{f(\alpha) : f(x) \in F[x]\} \subseteq E$$

We also denote

$$F[\alpha] := \varphi_\alpha(F[x]) = \{f(\alpha) : f \in F[x]\}$$

$$= \{a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 : a_i \in F\}$$

Caution: $F[\alpha]$ is not to be confused with a polynomial ring.

1. *If α is algebraic over F then $F[\alpha]$ is a field.*

2. *If α is trancendental, then φ_α is injective. So, $F[x] \xrightarrow{\sim} F[\alpha]$*

Proof. Let $I = \ker(\varphi)$. Then, I is an ideal of $F[x]$. By a theorem in §21, $I = F[x]p(x)$. In fact, $p(x) = irr(\alpha, F)$ (*because the generator of the ideal is the polynomial with minimal degree*). It follows, from Group Theory, that

$$\frac{F[x]}{F[x]p(x)} \xrightarrow{\sim} F[\alpha]$$

is an isomorphism. Since p is irreducible, $\frac{F[x]}{F[x]p(x)}$ is a field (see §27).

When α is trancendental, by definition the statement is true. The proof is complete. ■

Definition 29.15. *Use all the notations as in (29.14).* Let $F \hookrightarrow E$ be an extension of fields and $\alpha \in E$. Recall that $F(\alpha)$ denotes the smallest subfieled of E generated by F and α.

1. If α is algebraic over F, then $F[\alpha]$ is a field. Therefore, $F[\alpha] = F(\alpha)$.

2. If α is trancendental over F, then $F[x] \approx F[\alpha]$ is ONLY an integral doamian, not a field. In this case, the field of quotients of $F[\alpha]$ is $= F(\alpha)$.

Important Remark: Suppose $F \hookrightarrow E$ is a field extension. Then E is a vector space over F. More generally, for a field F, and a ring R, any ring homomorphism $F \longrightarrow R$ provides an $F-$vector space structure on R. (*The author avoided stating this at this stage, becasue he is introducing Vector Space in next section §30.*)

Theorem 29.16 (29.18)**.** *Suppose $F \hookrightarrow E$ be a field extension and $\alpha \in E$ be algebraic over F. As said above, then $F(\alpha) = F[\alpha]$. Let*

$$degree(irr(\alpha, F)) = n.$$

In fact,

$$1, \alpha, \alpha^2, \ldots, \alpha^{n-1} \quad forms\ a\ Vector\ Space\ basis\ of F(\alpha)\ over\ F.$$

Proof. As before, let $\varphi_\alpha : F[x] \longrightarrow E$ be the evaluation map. Then,

$$F(\alpha) = F[\alpha] = image(\varphi_\alpha).$$

Let

$$irr(\alpha, F) = p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \quad with \quad a_i \in F.$$

By definition, $p(\alpha) = 0$. Let $\beta \in F(\alpha) = F[\alpha]$. Then, there is a polynomial $f \in F[x]$ such that $\beta = f(\alpha)$. By division algorithm,

$$f(x) = p(x)q(x)+r(x) \quad with \quad q, r \in F[x] \quad and \quad r = 0 \quad or \quad degree(r) < n.$$

Write

$$r(x) = b_0 + b_1x + b_2x^2 + \cdots + b_{n-1}x^{n-1} \quad b_i \in F.$$

So,

$$\beta = f(\alpha) = p(\alpha)q(\alpha) + r(\alpha) = b_0 + b_1\alpha + b_2\alpha^2 + \cdots + b_{n-1}\alpha^{n-1}.$$

So, is a β is F-linear combination of $1, \alpha, \ldots, \alpha^{n-1}$ and hence this set spans $F[\alpha]$. To prove, $1, \alpha, \ldots, \alpha^{n-1}$ is linearly independent, let

$$a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1} = 0 \quad \text{with} \quad a_i \in F.$$

Write

$$r(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1}. \text{ then } r(\alpha) = 0.$$

By minimality of $p(x)$, we have $r(x) = 0$. That means, $a_0 = a_1 = \cdots = a_{n-1} = 0$. Hence the above set is linearly independent; hence a basis. The proof is complete. ■

Reading Assignment: Read Example 29.19, page 271.

30 Vector Spaces

Refer to Math 790.

31 Algebraic Extension

Abstract

Given a field F and a non-constant $f \in F[x]$, we want to find extension $F \hookrightarrow E$ so that $f(x)$ has a root in E

31.1 Finite Extensions

Definition 31.1. *Let $F \hookrightarrow E$ be an extension of fields.*

1. Recall, an element $\alpha \in E$ is said to be **algebraic over** F, if there is a non-constant $f \in F[x]$ so that $f(\alpha) = 0$.
2. *The extension $F \hookrightarrow E$ is said to be an* **algebraic extension**, *if every $\alpha \in E$ is algebraic over F.*
3. *Given an extension $F \hookrightarrow E$ of fields, we can consider E as a vector space over F. Define*

   $[E : F] := \dim_F(E)$ = *the vector space dimension of E over F.*

   This $[E : F]$ can be finite of ∞.
4. *If $[E : F] = n < \infty$, then we is say E* **is a finite extension of degree n over F**.

Examples. Here are some:

1. Given any field F, F is a finite extension over itself, of degree $[F : F] = 1$.
2. $\mathbb{R} \hookrightarrow \mathbb{C}$ is a finite extension of degree 2 over $\mathbb{R}$. (*Give a basis.*).
3. Let $\mathbb{Q} \hookrightarrow \mathbb{Q}(\sqrt{2})$ is a finite extension of degree 2 over $\mathbb{Q}$. (*Give a basis.*).
4. Give a positive integer n let $\zeta_n = e^{\frac{2\pi i}{n}}$ and
   $$E = \mathbb{Q}\left(\zeta_n\right) = \mathbb{Q}\left(e^{\frac{2\pi i}{n}}\right).$$
   The $\mathbb{Q}\left(\zeta_n\right)$ is a finite extension of degree n over $\mathbb{Q}$. (*Give a basis.*).

Theorem 31.2 (31.3)**.** *Let $F \hookrightarrow E$ be a finite field extension. Then, if is an algebraic field extension. Let me display*

$$FINITE \quad \Longrightarrow \quad ALGEBRAIC.$$

Proof. Let $[E : F] = n < \infty$. Let $\alpha \in E$ be any element. Then,

$$1, \alpha, \alpha^2, \ldots, \alpha^n \quad cannot\ be\ linearly\ independent\ over \quad F.$$

So, there are $a_0, a_1, \ldots, a_n \in F$, not all of them zero, such that

$$a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0. \qquad Write \quad f(x) = a_0 + a_1 x + \cdots + a_n x^n.$$

Then, $f(x) \in F(x)$ is nonzero and $f(\alpha) = 0$. So, α is algebraic over F. The proof is complete. ∎

Theorem 31.3 (31.4)**.** *Let $F \hookrightarrow E$, $E \hookrightarrow K$ be two finite field extension. Then, $F \hookrightarrow K$ is a finite extension, and*

$$[K : F] = [K : E][E : F].$$

Proof. Let

$$[K : E] = m, \quad [E : F] = n.$$

We will prove $[K : F] = mn$. Let

$$\alpha_1, \alpha_2, \ldots, \alpha_n \in E \quad be\ a\ basis\ of\ E\ over F$$

$$and \quad \beta_1, \beta_2, \ldots, \beta_m \in K \quad be\ a\ basis\ of\ K\ over E.$$

We will prove $\{\alpha_i\beta_j : i = 1, \ldots, n; \quad j = 1, \ldots, m\}$ forms a basis of K over F. First, I will show they span K over F. Let $\gamma \in K$. Then,

$$\gamma = b_1\beta_1 + b_2\beta_2 + \cdots + b_m\beta_m = \sum_{j=1}^{m} b_j\beta_j \qquad for\ some \quad b_j \in E.$$

Again, since $b_j \in E$ we have

$$b_j = a_{1j}\alpha_1 + a_{2j}\alpha_2 + \cdots + a_{nj}\alpha_n = \sum_{i=1}^{n} a_{ij}\alpha_i \qquad for\ some \quad a_{ij} \in F.$$

So,

$$\gamma = \sum_{j=1}^{m} b_j\beta_j = \sum_{j=1}^{m}\left(\sum_{i=1}^{n} a_{ij}\alpha_i\right)\beta_j = \sum_{j=1}^{m}\sum_{i=1}^{n} a_{ij}(\alpha_i\beta_j).$$

So, γ is an $F-$linear combination of $\alpha_i\beta_j$. So,

$$\{\alpha_i\beta_j : i = 1, \ldots, n; \quad j = 1, \ldots, m\} \qquad spans \quad K \quad over \quad F.$$

Now, I will show $\{\alpha_i\beta_j : i = 1, \ldots, n; \quad j = 1, \ldots, m\}$ is linearly independent over F. So, suppose

$$\sum_{j=1}^{m}\sum_{i=1}^{n} a_{ij}(\alpha_i\beta_j) = 0 \qquad for\ some \quad a_{ij} \in F.$$

Then, we have

$$\sum_{j=1}^{m}\sum_{i=1}^{n} a_{ij}(\alpha_i\beta_j) = \sum_{j=1}^{m}\left(\sum_{i=1}^{n} a_{ij}\alpha_i\right)\beta_j = 0.$$

Since, $\beta_1, \ldots, \beta_m$ are linearly independent over E, for each j we have

$$\sum_{i=1}^{n} a_{ij}\alpha_i = 0.$$

Since $\alpha_1, \ldots, \alpha_n$ are lineraly independent ove F we have

$$a_{ij} = 0 \quad for \quad all \quad i = 1, \ldots, n;\ j = 1, \ldots, m.$$

So, $\{\alpha_i\beta_j : i = 1, \ldots, n; \quad j = 1, \ldots, m\}$ is also linearly independent over F. So, $\{\alpha_i\beta_j : i = 1, \ldots, n; \quad j = 1, \ldots, m\}$ is a basis of K over F. So,

$$[K : F] = nm = [K : E][E : F].$$

The proof is complete. ■

Corollary 31.4 (31.6)**.** *Suppose*

$$F_1 \hookrightarrow F_2 \hookrightarrow F_3 \cdots F_{r-1} \hookrightarrow F_r \quad be\ finite\ field\ extensions.$$

Then,

$$[F_r : F_1] = [F_r : F_{r-1}] \cdots [F_3 : F_2][F_2 : F_1]$$

Proof. By induction,

$$[F_r : F_1] = [F_r : F_{r-1}][F_{r-1} : F_1] = [F_r : F_{r-1}](F_{r-1} : f_{r-2}] \cdots [F_3 : F_2][F_2 : F_1].$$

The proof is complete. ■

Corollary 31.5 (31.7)**.** *Let $F \hookrightarrow E$ be a field extension and $\alpha \in E$ be algebraic over F. Let $\beta \in F(\alpha)$. Then*

$$deg(\beta, F) | deg(\alpha, F).$$

Proof. Recall, $deg(\alpha, F)$ is the degree of the irreducible polynomial of α and

$$deg(\alpha, F) = [F(\alpha) : F].$$

So, we have

$$deg(\alpha, F) = [F(\alpha) : F] = [F(\alpha) : F(\beta)][F(\beta) : F] = [F(\alpha) : F(\beta)]deg(\beta, F).$$

The proof is complete. ■

Reading Assignment: Read Example 31.7-31.10.

Theorem 31.6 (31.11)**.** *Let $F \hookrightarrow E$ be an algebraic extension and $E = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ for finitely many elements $\alpha_1, \alpha_2, \ldots, \alpha_n \in E$. Then, $F \hookrightarrow E$ is finite field extension.*

The converse of this theorem is also true (by (31.2)).

Proof. Suppuse $E = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ is algebraic. Write

$$E_0 = F, E_1 = F(\alpha_1), E_2 = F(\alpha_1, \alpha_2), \ldots, E_{n-1} = F(\alpha_1, \alpha_2, \ldots, \alpha_{n-1}),$$

$$E_n = E = F(\alpha_1, \alpha_2, \ldots, \alpha_n).$$

Note $E_{r-1} \hookrightarrow E_r = E_{r-1}(\alpha_r)$ and α_r is algebraic over E_{r-1}. So,

$$[E_r : E_{r-1}] = \deg(\alpha_r, E_{r-1}) =: m_r.$$

Then, we have a chain

$$F = E_0 \hookrightarrow E_1 \hookrightarrow E_2 \dots E_{n-1} \hookrightarrow E_n = E$$

of algebraic field extensions. So,

$$[E : F] = [E_n : E_0] = [E_n : E_{n-1}][E_{n-1} : E_{n-2}] \cdots [E_2 : E_1][E_1 : E_0]$$

$$= m_n m_{n-1} \cdots m_2 m_1 < \infty.$$

So, first part of the theorem is established.

For the converse, let $F \hookrightarrow E$ be a finite field extension and $[E : F] = n$. Let $\alpha_1, \dots, \alpha_n$ be a basis of E over F. Then, $E = F(\alpha_1, \dots, \alpha_n)$. Also, by (31.2), it is an algebraic extension. The proof is complete. ■.

Corollary 31.7 (Extra)**.** *Suppose $E = F(\alpha_1, \dots, \alpha_n)$ is finitely generateted field extension of F. Then, $F \hookrightarrow E$ is algebraic field extension if and only if $F \hookrightarrow E$ finite field extension.*

Let me display, for finitely generated extensions

$$FINITE \qquad \Longleftrightarrow \qquad ALGRBRAIC.$$

Proof. It is just reinterpretation of the above. ■

Corollary 31.8 (Extra)**.** *Suppose $E = F(\alpha_1, \dots, \alpha_n)$ is finitely generateted field extension of F. Assume $\alpha_1, \dots, \alpha_n$ are algebraic over F. Then E is a finite field extension of F.*

Proof. Exercise ■

31.2 Algebraically Closed Fields and Algebraic Closure

Theorem 31.9 (31.12)**.** *Suppose $F \hookrightarrow E$ be an extension of fields. Write*

$$\overline{F}_E = \{\alpha \in E : \alpha \quad \text{is algebraic over} \quad F\}.$$

Then, $\overline{F}_E$ is a subfield of E and $F \hookrightarrow \overline{F}_E$. This field $\overline{F}_E$ is called the **Algebraic Closure of F in E.**

Proof. Suppose $\alpha, \beta \in \overline{F}_E$. Then, by (31.8), $F \hookrightarrow F(\alpha, \beta)$ is finite field extension. Since $\alpha + \beta, \alpha - \beta \in F(\alpha, \beta)$ and if $\beta \neq 0$ then $\frac{\alpha}{\beta} \in F(\alpha, \beta)$, by (31.2), they are all algebraic over F, hence in $\overline{F}_E$. So, $\overline{F}_E$ is closed under addition, multiplication and each nonzero element in $\overline{F}_E$ has an inverse in it. So, $\overline{F}_E$ is a field. The proof is complete. ∎

Corollary 31.10 (31.13)**.** *The set $\overline{\mathbb{Q}}_{\mathbb{C}}$ of all algebraic numbers forms a subfield of $\mathbb{C}$.*

Proof. Recall, a complex number $\alpha \in \mathbb{C}$, is called an algebraic number if it is algebraic over $\mathbb{Q}$. So, it is an immediate consequence of the above. ∎

Definition 31.11. *A field F is called* **algebraically closed**, *if every nonconstant polynomial $f \in F(x)$ has a zero in F.*

Prime Example:

Theorem 31.12 (31.17)**.** *The field $\mathbb{C}$ is algebraically closed.*

Proof. (*Skip, if you did not have course in complex analysis.*) Suppose $f(x) \in \mathbb{C}[x]$ is a nonconstant polynomial. Suppose $f(x)$ does not have any zero in $\mathbb{C}$. Then, $1/f(x)$ is an entire function (*that means, holomorphic everywhere*). Also, $\lim_{|x| \to \infty} |f(x)| = \infty$. So, $\lim_{|x| \to \infty} |1/f(x)| = 0$. Thus, $1/f(x)$ is a bounded function, which is entire. By Liouville's theorem, $1/f$ is constant and hence so is f. This is a contradiction. ∎

Theorem 31.13 (31.15)**.** *A field is algebraically closed if and only if every (nonconstant) polynomial factors in to linear factor.*

Proof. Suppose F is algebraically closed and $f \in F[x]$ is (nonconstant) polynomial. If $\deg(f) = 1$, then there is nothing to prove. Now let $n = \deg(f) > 1$. Since F is algebraically closed, $f(a_1) = 0$ for some $a_1 \in F$. So, $f(x) = (x - a_1)g(x)$ for some $g \in F[x]$. Since, $\deg(g) = n - 1 < \deg(f)$, by induction, g factors as $g(x) = \lambda(x - a_2)(x - a_3) \cdots (x - a_n)$ for some $\lambda, a_i \in F$. So, $f(x) = (x - a_1)g(x) = \lambda(x-a_1)(x-a_2)(x-a_3) \cdots (x-a_n)$. So, this implication is established.

Conversely, suppose every (nonconstant) polynomial factors in to linear factors. Now, let $f \in F[x]$ be nonconstant. Then $f(x) = \lambda(x - a_1)(x-a_2)(x-a_3) \cdots (x-a_n)$ for some $\lambda, a_i \in F$. So, each a_i is a root of f.

The proof is complete. ■.

Corollary 31.14 (31.16)**.** *Suppose F is an algebraically closed field and $F \hookrightarrow E$ is an algebraic extension of fields. Then $F = E$.*

Proof. Suppose $a \in E$. Since a is algebraic over F, there is a nonconstant polynomial $f \in F[x]$, such that $f(a) = 0$. So, $f(x) = (x-a)g(x)$ for some $g \in E[x]$. Since F is algebraically closed, by the above theorem, $f(x) = \lambda(x - a_1)(x - a_2)(x - a_3) \cdots (x - a_n)$ for some $\lambda, a_i \in F$. So,

$$f(x) = \lambda(x - a_1)(x - a_2)(x - a_3) \cdots (x - a_n) = (x - a)g(x)$$

Since, every polynomial in $E[x]$ has unique factorization, $a = a_i \in F$ for some i. The proof is complete. ■

Theorem 31.15 (31.32)**.** *Suppose F is a field. Then there is a field extension $F \hookrightarrow E$ such that (1) E is algebraically closed, (2) $F \hookrightarrow E$ is an algebraic extension.* (Such an extension E is called the **algebraic closure** of F and is denoted by $\overline{F}$).

Proof. By some set theoratic argument, we assume that there is a set Ω such that if $F \hookrightarrow E$ is an algebraic extension then $E \subset \Omega$. Let

$$\mathcal{E} = \{E : F \hookrightarrow E \textit{ is an algebraic extension}\}$$

Then, inclusion $E_1 \subseteq E_2$ gives a structure of a partially ordered set on $\mathcal{E}$. Suppose

$$E_1 \subseteq E_2 \subseteq E_3 \subseteq E_4 \subseteq \cdots$$

is a chain of field extensions in $\mathcal{E}$. Write

$$E = \bigcup E_i$$

Then, E is a field such that $F \hookrightarrow E$ is an algebraic extension. So, $E \in \mathcal{E}$ and $E_i \subseteq E$ for all i. So, every chain in $\mathcal{E}$ has an upper bound in $\mathcal{E}$. Therefore, by Zorn's lemma (see §0) $\mathcal{E}$ has a maximal element K. We claim that K is algebraically closed field. So see this, let $f \in K[x]$ be a nonconstant polynomial and $f(x)$ does not have a zero in K. Write the unique factorization $f = p_1p_2 \cdots p_r$, where $p_i \in K[x]$ are irreducible in $K[x]$. So, $K \hookrightarrow \frac{K[x]}{(p_1)}$ is an algebraic extension and so $F \hookrightarrow \frac{K[x]}{(p_1)}$ is an algebraic extension. Since, $K \neq \frac{K[x]}{(p_1)}$, it is a contradiction to the maximality of E. So, E is algebraically closed. The proof is complete. ■

List of concepts we defined in this section:

1. Given field extension $F \hookrightarrow E$ and element $a \in E$, we defined when we say a **is algebraic over** F.
2. We defined when a field extension $F \hookrightarrow E$ is called **algebraic extension**.
3. We defined **finite field extensions** $F \hookrightarrow E$.
4. Given field extension $F \hookrightarrow E$ we defined $\overline{F}_E$, the **algebraic closure of** F **in** E.
5. Give a field F, we defined its algebraic closure $\overline{F}$ (see 31.15). This is the "Grand" closure.

32 Geometric Constructions

skip

33 Finite Fields

Theorem 33.1. *Let F be a field and $F \hookrightarrow E$ be a finite field extention. If F has q elements and $[E : F] = n$ then E has q^n elements.*

Proof. Exercise. ■

Theorem 33.2. *Suppose E is a finite field of characteristic $p > 0$. Prove E has p^n elements.*

Proof. Follows from the fact $\mathbb{Z}_p \hookrightarrow E$ is finite field extension. The proof is complete. ■