Field Theory and Galois Theory.

Alec Zabel-Mena

January 13, 2023

Contents

Chapter 1

Fields.

1.1 Field Extensions.

Definition. We define the **characteristic** of a field F to be the smallest positive integer p, such that $p \cdot 1 = 0$, where 1 is the identity of F. We write $\operatorname{char} F = p$, and if no such p exists, then we write $\operatorname{char} F = 0$.

Lemma 1.1.1. *Let F be a field, then $\operatorname{char} F$ is either 0, or a prime integer.*

Proof. Let $\Gamma F = p$. If $p = 0$, then we are done. Now suppose that $p = mn$, with $m, n \in \mathbb{Z}^+$. Then $p \cdot 1 = (mn)1 = (n \cdot 1)(m \cdot 1) = mn = 0$, which makes m and n 0 divisors. Since F is a field, and hence an integral domain, this is impossible, and hence p must be prime. ■

Corollary. *If $\operatorname{char} F = p$, then for all $a \in F$, $pa = \underbrace{a + \cdots + a}_{p \text{ times}}$.*

Proof. We have $pa = p(a \cdot 1) = (p \cdot 1)a$. ■

Example 1.1. (1) Both $\mathbb{Q}$ and $\mathbb{R}$ have char $= 0$. Similarly, $\operatorname{char} \mathbb{Z} = 0$, even though $\mathbb{Z}$ is just an integral domain.

(2) $\operatorname{char} \mathbb{Z}/p\mathbb{Z} = p$ and $\operatorname{char} \mathbb{Z}/p\mathbb{Z}[x] = p$ for any prime p.

Definition. We define the **prime subfield** of a field F to be the subfield of F generated by 1.

Example 1.2. (1) The prime subfields of $\mathbb{Q}$ and $\mathbb{R}$ is $\mathbb{Q}$.

(2) Let $\mathbb{Z}/p\mathbb{Z}(x)$ the field of rational functions over $\mathbb{Z}/p\mathbb{Z}$. Then the prime subfield of $\mathbb{Z}/p\mathbb{Z}(x)$ is $\mathbb{Z}/p\mathbb{Z}$. Similarly, the prime subfield for $\mathbb{Z}/p\mathbb{Z}[x]$ is also $\mathbb{Z}/p\mathbb{Z}$.

Definition. If K is a field containing a field F, then we call K **field extension** over F, and write K/F (not the quotient field!) or denote it by the diagram

$$\begin{array}{c} K \\ | \\ F \end{array}$$

Lemma 1.1.2. *Every field is a field extension of its prime subfield.*

Lemma 1.1.3. *Let K an extension over a field F. Then K is a vector space over F.*

Definition. Let ${}^{K}\!/_{F}$ a field extension. We define the **degree** of K over F, $[K : F]$ to be the dimension of ${}^{K}\!/_{F}$ as a vector space.

Definition. Let F be a field, and $f \in F[x]$ a polynomial. We call am element $\alpha \in R$ a **root** (or **zero**) of f if $f(\alpha) = 0$.

Lemma 1.1.4. *Let $\phi : F \to L$ a field homomorphism. Then either $\phi = 0$, or ϕ is 1–1.*

Lemma 1.1.5. *Let F be a field, and $p \in F[x]$ an irreducible polynomial. Then there exists a field K containing an embedding of F, such that p has a root in K.*

Proof. Consider $K = {}^{F[x]}\!/_{(p)}$. Siince p is irreducible in a principle ideal domain, (p) is a maximal idea, and hence K is a field. Now consider the canonical map $\pi : F[x] \to K$ taking $f \to f \mod (p)$ and let $\phi = \pi|_F$. Then $\phi \neq 0$, since $\pi : 1 \to 1$. Then ϕ is 1–1. And so $\phi(F) \simeq F$.

Now, consider F as a subfield of K. Then $p(x \mod (p)) \equiv p(x) \mod (p) \equiv 0 \mod (p)$, so that $x \mod (p)$ is a root of p in K. ■

Corollary. *There exists a field extension of F containing a root of p.*

Theorem 1.1.6. *Let F be a field, and let $p \in F[x]$ an irreducible polynomial of degree n, and let $K = {}^{F[x]}\!/_{(p)}$, and $\theta = x \mod (p)$. Then $\{1, \theta, \dots, \theta^{n-1}\}$ forms a basis for K as a vector space over F and $[K : F] = n$.*

Proof. Let $a \in F[x]$, since $F[x]$ is Euclidean domain, there exist $q, r \in F[x]$, $q \neq 0$ for which

$$a(x) = q(x)p(x) + r(x) \text{ where } \deg r < n$$

Now, since $pq \in (p)$, $a(x) \equiv r(x) \mod (p)$, and every element of K is a polynomial of degree less than n. Then the elements $\{1, \theta, \dots, \theta^{n-1}\}$ span K.

Now, suppose that there are $b_0, \dots, b_{n-1} \in F$ not all 0 for which

$$b_0 + b_1\theta + \dots + b_{n-1}\theta^{n-1} = 0$$

Then

$$b_0 + b_1\theta + \dots + b_{n-1}\theta^{n-1} \equiv 0 \mod (p)$$

so that $p|(b_0 + b_1\theta + \dots + b_{n-1}\theta^{n-1})$ in F. But $\deg p = n$ and p divides a polynomial of degree $n - 1$, which is a contradiction. Therefore we are left with $b_0 = \dots = b_{n-1} = 0$. ■

Corollary. $K = \{\alpha_0 + a_1\theta + \dots + a_{n-1}\theta^{n-1} : a_i \in F \textit{ for all } 1 \leq i \leq n-1\}$

Corollary. *If $a(\theta), b(\theta) \in K$, are elements of degree less than n, and the operations of polynomial addition, and polynomial multiplication mod (p) are defined, then K forms a field.*

Example 1.3. (1) Consider the polynomial x^2+1 over $\mathbb{R}$. Then one has the field

$$\mathbb{C} = \mathbb{R}[x] \big/ (x^2+1)$$

an extension of $\mathbb{R}$ of degree $[\mathbb{C} : \mathbb{R}] = 2$. Let i be a root of x^2+1 in this field, then $i^2 = -1$, and the elements of $\mathbb{C}$ are of the form $a+ib$ where $a, b \in \mathbb{R}$. Then we have described the field of complex numbers, and the addition and multiplication (mod x^2+1) of these elements are the addition and multiplication of complex numbers.

One might also construct $\mathbb{C}$ differently by defining the isomorphism

$$\mathbb{R}[x] \big/ (x^2+1) \to \mathbb{C} \text{ taking } a+xb \to a+ib$$

(2) Consider again x^2+1 over $\mathbb{Q}$. Then we get the field

$$\mathbb{Q}(i) = \mathbb{Q}[x] \big/ (x^2+1)$$

of degree $[\mathbb{Q}(i) : \mathbb{Q}] = 2$, and where i is a root of x^2+1, so that $i^2 = -1$. Then the elements of $\mathbb{Q}(i)$ are of the form $a+ib$ where $a, b \in \mathbb{Q}$, i.e. it is isomorphic to the set of all complex numbers with rational components.

(2) Consider x^2-2 over $\mathbb{Q}$. by Eisenstein's criterion for $p=2$, x^2-2 is irreducible over $\mathbb{Q}$. Let α a root of x^2-2, so that $\alpha^2 = 2$. Then we have the field

$$\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[x] \big/ (x^2-2)$$

of degree $[Q(\sqrt{2}) : \mathbb{Q}] = 2$, and whose elements are of the form $a + b\sqrt{2}$. One can define an isomorphism between $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{2})$ by taking $\sqrt{2} \to i$.

(3) The polynomial x^3-2 over $\mathbb{Q}$ gives us the field

$$\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}[x] \big/ (x^3-2)$$

of degree $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ over 2. Here the elements are of the form $a + b\xi + c\xi^2$ where $\xi^3 = 2$.

(4) Denote $\mathbb{F}_2$ to be a finite field of 2 elements. Consider the polynomial x^2+x+1 over $\mathbb{F}_2$ which is irreducible. Then the field

$$\mathbb{F}_2(\alpha) = \mathbb{F}_2[x] \big/ (x^2+x+1)$$

is a field of degree 2 over $\mathbb{F}_2$, whose elements are of the form $a + b\alpha$, where $\alpha^2 = \alpha + 1$. In fact, one can generate this field using the fact that $\alpha^2 = \alpha + 1$.

(5) Let $F = K(t)$ the field of rational functions in t over a field K. Let $p(x) = x^2 - t \in F[x]$, then by Eisenstien's criterion with the ideal (t), p is irreducible over $F[x]$. Let θ be a root for p, that is $\theta = \sqrt{t}$, then we get the field $K(t, \sqrt{t})$ of degree $[K(t, \sqrt{t}) : K] = 2$, whose elements are of the form $a(t) + b(t)\sqrt{t}$.

Lemma 1.1.7. *Let F be a subfield of a field K, and let $\alpha \in K$. Then there exists a unique minimal subfield of K containing F and α; more preciesly, it is the intersection of all subfields of K containing F and α.*

Definition. Let K be any extension of a field F, and let $\alpha, \beta, \dots \in K$. Then we define the subfield **generated** by $\alpha, \beta, \dots$ over F to be the unique minimal subfield containing all $\alpha, \beta, \dots$ and F and we denote it $F(\alpha, \beta, \dots)$. Moreover, we call K a **simple extension** of F if $K = F(\alpha, \beta, \dots)$. If $K = (F\alpha_1, \dots, a_n)$ for $\alpha_1, \dots, a_n \in K$, then it is a **finitely generated** simple extension.

Theorem 1.1.8. *Let F be a field, and $p \in F[x]$ irreducible, and let K an extension of F containing a root α of p. Then*

$$F(\alpha) \simeq F[x]/(p)$$

Proof. Consider the homomorphism $F[x] \to F(\alpha)$ taking $a(x) \to a(\alpha)$. Since $p(\alpha) = 0$, p is in the kernel of this homomorphism, and we get an induced homomorphsim from $F[x]/(p) \to F(\alpha)$. Now, since p is irreducible, $F[x]/(p)$ is a field, and since the homomorphsim takes $1 \to 1$, it is 1–1. Then by the first isomorphsim theorem for ring homomorphsims these two fields are isomorphic. ∎

Corollary. *If $\deg p = n$, then $F(\alpha) = \{a_0 + a_1\alpha + \dots a_{n-1}\alpha^{n-1} : a_i \in F$ for all $1 \leq i \leq n-1\}$ and $[F(\alpha) : F] = n$.*

Example 1.4. (1) The polynomial $x^2 - 2$ over $\mathbb{Q}$ also has the root $-\sqrt{2}$ in $\mathbb{R}$, so that $\mathbb{Q}(-\sqrt{2})$ is of degree 2 over $\mathbb{Q}$ with elements of the form $a - b\sqrt{2}$. Notice however that $\mathbb{Q}(-\sqrt{2}) \simeq \mathbb{Q}(\sqrt{2})$ by taking $a - b\sqrt{2} \to a + b\sqrt{2}$.

(2) The polynomial $x^3 - 2$ only has the solution $\xi = \sqrt[3]{2}$ in $\mathbb{R}$. However, in $\mathbb{Q}$ it has the solutions given by

$$\sqrt[3]{2}\left(\frac{-1 \pm i\sqrt{3}}{2}\right)$$

So that the subfields generated by either of these three elements (over $\mathbb{C}$) are isomorphic.

Theorem 1.1.9. *Let $\phi : F \to L$ a field isomorphism and $p \in F[x]$, $q \in L[x]$ irreducible polynomials, where q is obtained by applying ϕ to the coefficients of p. Let α a root of p, and β a root of q. Then there exists an isomorphism $F(\alpha) \to L(\beta)$ taking $\alpha \to \beta$ and extending ϕ. That is, we have the following diagram*

$$\begin{tikzcd}
F(\alpha) \arrow[r] \arrow[d, dash] & L(\beta) \arrow[d, dash] \\
F \arrow[r, "\phi"'] & E
\end{tikzcd}$$

Proof. Notice that ϕ induces a ring homomorphism between $F[x]$ and $L[x]$, so that (p) is maximal. Since q is obtained from p, (q) is also maximal, so that $F[x]/(p)$ and $L[x]/(q)$ are fields. Then we have an isomorphsism

$$F[x]/(p) \simeq L[x]/(q)$$

Then, if α is a root of p, and β a root of q, we obtain the isomorphism

$$F(\alpha) \simeq L(\beta)$$

moreover, this isomorphism takes $\alpha \to \beta$. ■

1.2 Algebraic Extensions.

Definition. Let K/F be a field extension. We say that an element $\alpha \in K$ is **algebraic** over F, provided there exists a polynomial over F having α as a root. Otherwise we call α **transcendental**. If every $\alpha \in K$ is algebraic, we call K **algebraic** and K/F an **algebraic extension**.

Lemma 1.2.1. *Let α be algebraic over a field F. Then there exista a unique monic irreducible polynomial $m \in F[x]$ having α as a root. Moreover, if $f \in F[x]$ is a polynomial, then f has α as a root if, and only if $m|f$.*

Proof. Let m a polynomial of minimal degree having α as a root. Suppose, also that , is monic. Now, if m were reducible, then $m(x) = a(x)b(x)$ for some $a, b \in F[x]$ polynomials both of degree less than $\deg m$. Then we also have that $a(\alpha) = b(\alpha) = 0$, which contradicts that m is the polynomial of minimal degree satisfying that condition. Hence, m is irreducible.

Now, let $f \in F[x]$ have α as a root, then by the divison theorem, there exist $q, r \in F[x]$, with $q \neq 0$ for which

$$f(x) = q(x)m(x) + r(x) \text{ where } \deg r < \deg m$$

Now, since $f(\alpha) = q(\alpha)m(\alpha) + r(\alpha) = 0$, then $r(x) = 0$ for all x lest we contradict the minimality of m. Hence $m|f$. Conversely, if $m|f$, then f has α as a root.

Now, let g a polynomial of minimal degree for which $g(\alpha) = 0$. Then by above, we have that $\deg g = \deg m$, and that moreover, $m|g$ and $g|m$. therefore $g = m$ and uniqueness is established. ■

Corollary. *Let L/F be an extension, and α algebraic over F. Let $m_{\alpha,F}$ the unique monic irreducible polynomial over F having α as root, and $m_{\alpha,L}$ the unique monic irreducible polynomial over L having α as root. Then $m_{\alpha,L}|m_{\alpha,F}$ in $L[x]$.*

Definition. Let F be a field, and α algebraic over F. We define the **minimal polynomial** $m_{\alpha,F}$, to be the polynomial over F of minimal degree having α as a root. If the field is clear, we instead write m_α, or even just m when the root itself is also clear. We define the **degree** of α to be $\deg \alpha = \deg m_\alpha$.

Lemma 1.2.2. *Let α algebraic over F. Then*

$$F(\alpha) \simeq {}^{F[x]}\!\diagup_{(m_{\alpha,F})}$$

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

Example 1.5.

(1) The minimal polynomial for $\sqrt{2}$ over $\mathbb{Q}$ is $x^2 - 2$.

(3) The minimal polynomial for $\sqrt[3]{2}$ over $\mathbb{Q}$ is $x^3 - 2$.

(3) Let $n > 1$, then by the Eisenstein-Schömann criterion, $x^n - 2$ is irreducible over $\mathbb{Q}$. Moreover, $x^n - 2$ has as root in $\mathbb{R}$ $\sqrt[n]{2}$. Then $\mathbb{Q}(\sqrt[n]{2})$ is a field of degree $[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = 2$. Moreover $x^n - 2$ is the minimal polynomial of $\sqrt[n]{2}$. Notice, that over $\mathbb{R}$, $\deg [n]2 = 1$, and that $m_{\sqrt[n]{2},\mathbb{R}}(x) = x - \sqrt[n]{2}$.

(4) Consider $p(x) = x^3 - 3x - 1$ over $\mathbb{Q}$. Notice that p is irreducible over $\mathbb{Q}$ and let α a root of p. Then $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$.

Lemma 1.2.3. *An element α is algebraic over a field F if, and only if the simple extension ${}^{F(\alpha)}\!\diagup_{F}$ is finite.*

Proof. If α is algebraic over F then $[F(\alpha) : F] = \deg \alpha \leq n$ if α satisfies a polynomial of degree n. Conversely, if α is an element of the finite extenson ${}^{K}\!\diagup_{F}$, of degree n, then the set $\{1, \alpha, \ldots, \alpha^n\}$ is linearly dependent over F. Hence there exist $b_0, \ldots, b_n \in F$ not all 0 for which

$$b_0 + b_1\alpha + \cdots + a_n\alpha^n = 0$$

making α a root of a nonzero polynomial over F of degree $\deg \leq n$. ∎

Corollary. *If an extension ${}^{K}\!\diagup_{F}$ is finite, then it is algebraic.*

Proof. If $\alpha \in K$ is algebraic, then ${}^{K}\!\diagup_{F}$ implies that ${}^{F(\alpha)}\!\diagup_{F}$ is finite, since $F(\alpha) \subseteq K$. ∎

Example 1.6. Let F a field of $\operatorname{char} F \neq 2$, and let K an extension field of F of degree $[K : F] = 2$. Let $\alpha \in K$ not in F, then α satisfies an polynomial of at most degree 2 over F. Now, since $\alpha \notin F$, this polynomial must have degree greater than 1. Hence it satisfies a polynomial of degree 2. Then the minimal polynomial of α is a quadratic

$$m_\alpha(x) = x^2 + bx + c \text{ with } b, c \in F$$

Since $F \subseteq F(\alpha) \subseteq K$, and $F(\alpha)$ is a vector space over F of dimension 2, then we must have $K = F(\alpha)$; that is ${}^{K}\!\diagup_{F}$ is simple.

Now, the roots of m_α are

$$\alpha = \frac{-b \pm \sqrt{b^2 - 4c}}{2}$$

Since $\alpha \notin F$, $b^2 - 4c$ is not a square in F, and $\sqrt{b^2 - 4c}$ is a root of the equation $x^2 - (b^2 - 4c) = 0$ in K.

Conversely, $\sqrt{b^2 - 4c} = \pm(b + 2\alpha)$ which puts $\sqrt{b^2 - 4c} \in F(\alpha)$. That is $F(\sqrt{b^2 - 4c}) = \mathbb{F}(\alpha)$. Moreover, $x^2 - (b^2 - 4c)$ does not have solutions in K.

We call field extensions ${}^{K}\!\diagup_{F}$ of degree 2 **quadratic field extension**, where $K = F(\sqrt{D})$, and D is a squarefree element of F.

Theorem 1.2.4. *Let $F \subseteq K \subseteq L$. Then $[L : F] = [L : K][K : F]$.*

Proof. Let $[L : K] = m$ and $[K : F] = n$. Let $\{\alpha_1, \dots, \alpha_m\}$ and $\{\beta_1, \dots, \beta_n\}$ be bases for the extensions ${}^{L}\!/_{K}$ and ${}^{K}\!/_{F}$. Now, the elements of L over K are of the form

$$a_1\alpha_1 + \cdots + a_m\alpha_m \text{ where } a_i \in K \text{ for all } 1 \leq i \leq m$$

Since each $a_i \in K$, which is an extension over F, they have the form

$$a_i = b_{i1}\beta_{i1} + \cdots + b_{in}\beta_{in} \text{ where } b_{ij} \in F \text{ for all } 1 \leq j \leq n$$

That is, every element of L, as a vector space over F are of the form

$$\sum b_{ij}\alpha_i\beta_j$$

So the set $\{\alpha_1\beta_1, \dots \alpha_m\beta_n\}$ spans L. It remains to show that this set is linearly in dependent.

Suppose that

$$\sum b_{ij}\alpha_i\beta_j = 0$$

for some $b_{ij} \in F$. Since $\{\alpha_1, \dots, \alpha_m\}$ are linearly indpendent in L over K, we have that the coefficients $a_1 = \cdots = a_n = 0$ which makes

$$a_i = b_{i1}\beta_{i1} + \cdots + b_{in}\beta_{in} = 0$$

Now, since $\{\beta_1, \dots, \beta_n\}$ is linearly independent in K over F, this implies that $b_{i1} = \cdots = b_{in} = 0$ which makes the collection $\{\alpha_1\beta_1, \dots \alpha_m\beta_n\}$ linearly independent, and hence, a basis. Moreover, notice that this basis has size mn. ■

Example 1.7. (1) The element $\sqrt{2} \notin \mathbb{Q}(\alpha)$, where α is the root of $x^3 - 3x - 1$; since $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, and $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$.

(2) We have $[\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}] = 6$, and since $(\sqrt[6]{2})^3 = \sqrt{2}$, we observe that $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[6]{2})$. Moreover, notice that by theorem 1.2.4 $[\mathbb{Q}(\sqrt[6]{2}) : Q(\sqrt{2})] = 3$. Then we have the following tower of fields for

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[6]{2})$$

$$\begin{array}{c} \mathbb{Q}(\sqrt[6]{2}) \\ | \\ \mathbb{Q}(\sqrt{2}) \\ | \\ \mathbb{Q} \end{array}$$

Lemma 1.2.5. *Let α, β be algebraic over a field F. Then $F(\alpha, \beta) = (F(\alpha))(\beta)$.*

Proof. By definition, $F(\alpha, \beta)$ contains F, and α, and hence contains $F(\alpha)$. It also contains β so that $(F(\alpha))(\beta) \subseteq F(\alpha, \beta)$. By the same argument, $(F(\alpha))(\beta)$ contains F, α and β so that $F(\alpha, \beta) \subseteq (F(\alpha))(b)$. ■

Corollary. *The elements of $F(\alpha,\beta)$ are of the form $\sum a_{ij}\alpha^i b^j$, where $1 \le i \le \deg\alpha$ and $1 \le j \le \deg\beta$.*

Example 1.8. Consider $\mathbb{Q}(\sqrt{2},\sqrt{3})$ generated by $\sqrt{2}$ and $\sqrt{3}$. Notice that $\deg\sqrt{3} = 2$ over $\mathbb{Q}$ so that $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2})] \le 2$. Now $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$ if, and only if the polynomial $x^2 - 3$ is irreducible over $\mathbb{Q}(\sqrt{2})$. Then it is irreducible if, and onyl if $\sqrt{2} \in \mathbb{Q}(\sqrt{3})$. It can be shown that this is not the case by trying to find $a, b \in \mathbb{Q}$ for which $\sqrt{3} = a + b\sqrt{2}$. Moreover we have

$$[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}] = 4$$

Theorem 1.2.6. *An extension field K/F is finite if, and only if it is generated by finitely many algebraic elements over F.*

Proof. Let K/F finite of degree n, and $\{\alpha_1,\dots,\alpha_n\}$ a basis. Then by theorem 1.2.4, $[F(\alpha_i) : F] | [K : F]$ for all $1 \le i \le n$. So each α_i is algebraic over F. Then K is generated by finitely many algebraic elements.

Conversely, let $K = F(\alpha_1,\dots,\alpha_k) = (F(\alpha_1,\dots a_{k-1}))(\alpha_k)$ We obtain K by taking the extensions F_{i+1}/F_i iteratively, where $F_{i+1} = F_i(\alpha_{i+1})$, and obtain the sequence

$$F = F_0 \subseteq \cdots \subseteq F_k = K$$

Now, if the elements $\alpha_1,\dots,\alpha_k$ are algebraic over F, each of $\deg\alpha_i = n_i$ for $1 \le i \le k$, then the extension F_{i+1}/F_i is a simple extension, and $[F_{i+1} : F_i] = \deg m_{\alpha_{i+1}} \le \deg\alpha_{i+1} = n_{i+1}$. Then we have

$$[K : F] = [F_k : F_{k-1}]\dots[F_1, F] \le n_1 \dots n_k$$

which makes K/F a finite extension. ■

Corollary. *If α,β are algebraic over F, then so are $\alpha \pm \beta$, $\alpha\beta$, and $\alpha\beta^{-1}$ (for $\beta \ne 0$).*

Corollary. *If L/F is an extension, then the collection of elements of L which are algebraic over F forms a subfield of L.*

Example 1.9. (1) Consider the extension $\mathbb{C}/\mathbb{Q}$, and let $\operatorname{cl}\mathbb{Q}$ the subfield of all elements of $\mathbb{C}$ which are algebraic over $\mathbb{Q}$. Then $\sqrt[n]{2} \in \operatorname{cl} Q$ for all $n \ge 1$, so that $[\operatorname{cl}\mathbb{Q} : \mathbb{Q}] \ge n$. This makes $\operatorname{cl}\mathbb{Q}$ an infinite algebraic extension, and we call $\operatorname{cl}\mathbb{Q}$ the **field of algebraic numbers**.

(2) Consider $\operatorname{cl}\mathbb{Q} \cap \mathbb{R}$ as a subfield of $\mathbb{R}$ (i.e. the subfield of all algebraic elements of $\mathbb{Q}$). Since $\mathbb{Q}$ is countable, so is the field $\mathbb{Q}[x]$, and each polynomial in $\mathbb{Q}[x]$ has at most n roots in $\mathbb{R}$, hence the number of all algebraic elements of $\mathbb{R}$ over $\mathbb{Q}$ is also countable. This means that $\operatorname{cl}\mathbb{Q}$ must also be countable. Now, since $\mathbb{R}$ is uncountable, then there exist uncountably transcendental numbers of $\mathbb{R}$ over $\mathbb{Q}$. Most notably the irrational numbers π and e are transcendental.

Theorem 1.2.7. *If K is algebraic over F, and L algebraic over K, then L is algebraic over F.*

Proof. Let $\alpha \in L$, since L is algebraic over K, there exists a $p \in K[x]$ having α as root. Let $p(x) = a_0 + a_1x + \cdots + a_nx^n$. Consider then $F(\alpha, a_0, \ldots, a_n)$. Since ${}^{K}\!/_{F}$ is algebraic, $a_0, \ldots, a_n$ are algebraic over F, and so $F(\alpha, a_0, \ldots, a_n)$ is a finite extension over F. Then α generates an extension field of degree less than n, and we get

$$[F(\alpha, a_0, \ldots, a_n) : F] = [F(\alpha, a_0, \ldots, a_n) : F(a_0, \ldots, a_n)][F(a_0, \ldots, a_n) : F]$$

is finite, and $F(\alpha, a_0, \ldots, a_n)$ is algebraic over F. That is, α is algebraic over F, and so L is algbraic over F. ■

Definition. Let K_1 and K_2 subfields of a field K. The **composite field** K_1K_2 is the smallest subfield of K containing both K_1 and K_2.

Example 1.10. The composite field of $\mathbb{Q}(\sqrt[3]{2})$ and $\mathbb{Q}(\sqrt{2})$ is $\mathbb{Q}(\sqrt[6]{2})$.

Lemma 1.2.8. *Let K_1 and K_2 be extensions of a field F contained in a field K. Then $[K_1K_2 : F] \leq [K_1 : F][K_2 : F]$ with equality holding if, and only if a basis of F in the other field is linearly independent. Moreover if $\{\alpha_1, \ldots, \alpha_m\}$ and $\{\beta_1, \ldots, \beta_n\}$ are bases for K_1 and K_2, then $\{\alpha_1, \beta_1, \ldots, \alpha_m\beta_n\}$ span K_1 and K_2.*

$$\begin{tikzcd}
 & K_1K_2 & \\
K_1 \arrow[ur, dash, "\leq m"] & & K_2 \arrow[ul, dash, "\leq n"'] \\
 & F \arrow[ul, dash, "n"] \arrow[ur, dash, "m"'] &
\end{tikzcd}$$

Corollary. *If $[K_1 : F] = m$, and $[K_2 : F] = n$ with m and n coprime, then $[K_1K_2 : F] = [K_1 : F][K_2 : F]$.*

Proof. We have that $m, n | [K_1K_2 : F]$ and since $K_1, K_2 \subseteq K_1K_2$ are subfields of K_1K_2, we get the least common multiple $[m, n] | [K_1K_2 : F]$. Now, since $(m, n) = 1$, we get $[m, n] = mn$ so that $mn \leq= [K_1K_2 : F]$. ■

1.3 Ruler and Compass Constructions.

1.4 Splitting Fields

Definition. Let K be an extension of a field F. We say a polynomial f over F **splits completely** over K if f factors into linear factors over K. If f splits completely over K, and in no other proper subfield, then we say K is the **splitting field** of f over F.

Theorem 1.4.1. *If f is a polynomial over a field F, then there exists a splitting field K of f over F.*

Proof. Let E an extension of F with $[E : F] = n$. By induction on n, for $n = 1$, we take $E = F$ and we are done. Now, for $n \geq 1$, suppose the irreducible factors of f are of $\deg = 1$. Then f has all its roots in F, and hence splits completely over F. Then take $E = F$. On the other hand, if f has at least one irreducible factor of $\deg \geq 2$, then there is an extension E_1 of F for which f has the factor $(x - \alpha)$ for some root α. Then $f(x) = (x - \alpha) f_1(x)$ where $\deg f_1 = n - 1$. Therefore by the induction hypothesis, there is an extension E of E_1 containing all the roots of f_1. Hence, it contains all the roots of f and f splits completely over E.

Now, let K be the intersection of all subfields of E for which f splite; i.e. all subfields containing the roots of f. Then by definition, K is the splitting field of f over F. ■

Definition. If K is an algebraic extesnion of F such that it is the splitting field for a collection of polynomials over F, then we say that K is a **normal extension** of F.

Example 1.11. (1) The splitting field of $x^2 - 2$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{2})$, since $x^2 - 2 = (x + \sqrt{2})(x - \sqrt{2})$ and $\pm\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ and $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, so there is no other subfield in between.

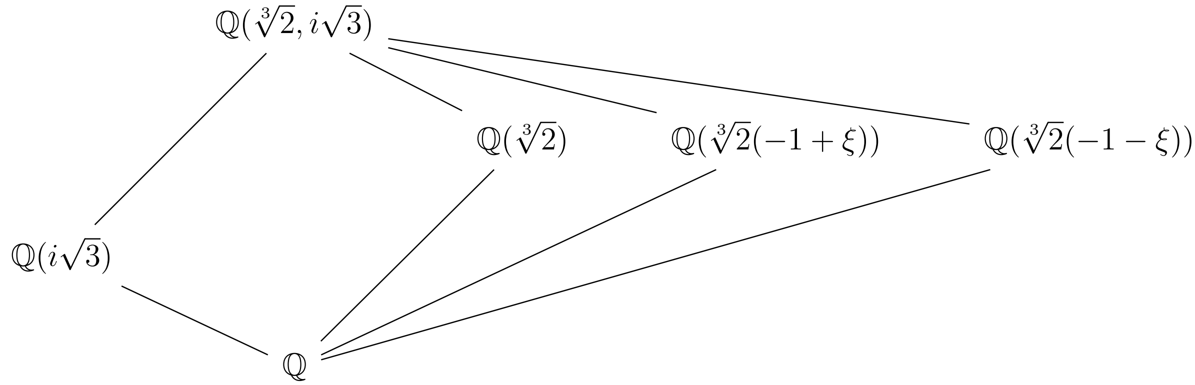
(2) The splitting field for $(x^2 - 2)(x^2 - 3) = (x + \sqrt{2})(x - \sqrt{2})(x + \sqrt{3})(x - \sqrt{3})$ is $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. Now, $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : Q] = 4$ and the lattice of fields is

$$\begin{tikzcd}
 & \mathbb{Q}(\sqrt{2},\sqrt{3}) \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] & \\
\mathbb{Q}(\sqrt{2}) \arrow[dr, dash, "2"'] & \mathbb{Q}(\sqrt{6}) \arrow[d, dash, "2"] & \mathbb{Q}(\sqrt{3}) \arrow[dl, dash, "2"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

(3) Let $\xi = i\frac{\sqrt{3}}{2}$. Notice that $x^3 - 2$ factors into $x^3 - 2 = (x - \sqrt[3]{2})(x + \sqrt[3]{2}(-1 + \xi))(x + \sqrt[3]{2}(-1 - \xi))$. Now, $-1 + \xi, -1 - \xi \notin \mathbb{Q}(\sqrt[3]{2})$, so $\mathbb{Q}(\sqrt[3]{2})$ is not the splitting field for $x^3 - 2$. Let K be the splitting field of $x^3 - 2$. Then K conmtains $-1 \pm \xi$, so that $i\sqrt{3} \in K$. Thus

$$K = \mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$$

Moreover, $[\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}) : \mathbb{Q}(\sqrt[3]{2})] \geq 2$ and since $\mathbb{Q}(\sqrt[3]{2})$ is not the splitting field, $[\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}) : \mathbb{Q}(\sqrt[3]{2})] = 2$. Hence $[\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}) : \mathbb{Q}] = 6$. We have the following lattice.



(4) Notice that $x^4+4 = (x^2+2x+2)(x^2-2x+2)$ over $\mathbb{Q}$ which is irreducible by Eisenstein's criterion. Using the quadratic formula, we get ± 1 and $\pm i$ as the roots, moreover, notice that $\pm 1, \pm i \in \mathbb{Q}(i)$ and since $[\mathbb{Q}(i) : \mathbb{Q}] = 2$ there are no subfields between $\mathbb{Q}$ and $\mathbb{Q}(i)$ so that $\mathbb{Q}(i)$ is the splitting field of x^4+4 over $\mathbb{Q}$.

Lemma 1.4.2. *A splitting field of a polynomial of degree n over a field F is of degree at most $n!$ over F.*

Proof. Let $f \in F[x]$ a polynomial of $\deg f = n$. Adjoining one root of f to F, we have an extension ${}^{F_1}\!/_{F}$ of degree $[F_1 : F] = n$. Now,f over F_1 has at leas one linear factor, and so any root of f satisfies a polynomial of degree $n-1$. Hence proceeding inductively gives the result. ∎

Example 1.12. Consider the polynomial $x^n - 1$ over $\mathbb{Q}$. Then the roots of x^n-1 are of the form ξ where $\xi^n = 1$. Notice, that in $\mathbb{C}$, $\xi = e^{\frac{2i\pi}{n}}$, so that $\mathbb{C}$ contains a splitting field of $x^n - 1$. Hence $\mathbb{Q}(\xi) \subseteq \mathbb{C}$ is a splitting field of x^n-1 over $\mathbb{Q}$. Notice that the set of all roots ξ of $x^n - 1$ forms a cyclic group generated by ξ.

Definition. Consider a field F and the polynomial $x^n - 1$ over F. We call the roots ξ of x^n-1, where $\xi^n = 1$ the **primitive n-th roots of unity** over F. We call $F(\xi)$ the **cyclotomic field** over F.

Example 1.13. Let p be a prime, and consider the splitting field $x^p - 2$ over $\mathbb{Q}$. If α is a root, then $\alpha^p = 2$ so that $(\xi\alpha)^p = 2$ where ξ is a primitive p-th root of unity over $\mathbb{Q}$. So the roots of x^2-2 are

$$\sqrt[p]{2} \text{ and } \xi\sqrt[p]{2}$$

Notice that $\frac{\xi\sqrt[p]{2}}{\sqrt[p]{2}} = \xi$ so the splitting field contains $\mathbb{Q}(\xi, \sqrt[p]{2})$, Moreover, $\mathbb{Q}(\xi, \sqrt[p]{2})$ contains all the roots of x^p-2 so that $\mathbb{Q}(\xi, \sqrt[p]{2})$ is the splitting field of x^p-2 over $\mathbb{Q}$.

Notice, that $\mathbb{Q}(\xi) \subseteq \mathbb{Q}(\xi, \sqrt[p]{2})$ so that $[\mathbb{Q}(\xi, \sqrt[p]{2}) : \mathbb{Q}(\xi)] \leq p$. not, since $\mathbb{Q}(\sqrt[p]{2})$ is also a subfield, we get $[\mathbb{Q}(\xi, \sqrt[p]{2}) : Q] \leq p(p-1)$. Since $(p, p-1) = 1$ (i.e. they are coprime), we have $p(p-1)|[\mathbb{Q}(\xi, \sqrt[p]{2}) : \mathbb{Q}]$ so that $[p]2) : \mathbb{Q}] = p(p-1)$. We have the follwing lattice.

$$\begin{tikzcd}
& \mathbb{Q}(\xi, \sqrt[p]{2}) \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\xi) \arrow[dr, dash] & & \mathbb{Q}(\sqrt[p]{2}) \arrow[dl, dash] \\
& \mathbb{Q} &
\end{tikzcd}$$

Theorem 1.4.3. *Let $\phi : F \to F'$ a field isomorphism. Let f and f' polynomials over F and F', where f' is obtained by applying ϕ to the coefficients of f. Let E and E' be splitting fields of f and f' over F and F', respectively. Then ϕ extends to an isomorphism betweenn E and E'; i.e. $E \simeq E'$.*

$$\begin{tikzcd}
E \arrow[r] \arrow[d, dash] & E' \arrow[d, dash] \\
F \arrow[r, "\phi"] & F'
\end{tikzcd}$$

Proof. Let $\deg f = n$. By induction on n. If f has all its roots in F, f splits completely over F, and f' over F'. Then take $E = F$ and $E' = F'$ and we are done for $n = 1$.

Now, for $n \geq 1$, suppose the theorem is true. Let p an irreducible factor of f, and p' an irreducible factor of f'. If α and α' are roots of p and p', respectively, then extend ϕ to $F(\alpha)$ and $F'(\alpha')$. Then $f(x) = (x-\alpha)f_1(x)$ and $f'(x) = (x-\alpha')f_1'(x)$; with $\deg f_1 = \deg f_1' = n-1$. Then let E the splitting field of f_1 over $F(\alpha)$, and E' the splitting field of f_1' over $F'(\alpha')$

$$\begin{tikzcd}
E \arrow[r] \arrow[d, dash] & E' \arrow[d, dash] \\
F(\alpha') \arrow[r] \arrow[d, dash] & F'(\alpha') \arrow[d, dash] \\
F \arrow[r, "\phi"'] & F'
\end{tikzcd}$$

The the roots of f_1 and f_1' are in E and E', respectively, and hence so are the roots of f and f'. Then by the induction hypothesis, we can extend ϕ to E and E' so that $E \simeq E'$. ■

Corollary. *Any two splitting fields of a given polynomial over a field are isomorphic.*

Proof. Take ϕ to be the identity map. ■

1.5 Algebraic Closures.

Definition. We define the **algebraic closure** of a field F to be the algebraic extension, $\operatorname{cl} F$, over F for which every polynomial over F splits. We call a field K **algebraically closed** if every polynomial over K has at least one root in K.

Lemma 1.5.1. *A field K is algebraically closed if, and only if every polynomial over K has all of its roots in K.*

Proof. Certainly, if a polynomial f over K contains all of its roots in K, then K is algebraically closed, by definition.

Now, suppose that K is algebraically closed, and let f a polynomial over K. Then f contains at least one root in K. Hence $f(x) = (x - \alpha)f_1(x)$ for some root α of f, and where $f_1 \in K[x]$. But then by definition again, f_1 contains at least one root in K. Hence, we proceed until we exhaust all the roots of f, and obtain that every root of f lies in K. ■

Corollary. *K is algebraically closed if, and only if* $\operatorname{cl} K = K$.

Lemma 1.5.2. *Let F be a field, and* $\operatorname{cl} F$ *its algebraic closure. Then* $\operatorname{cl} F$ *is algebraically closed; i.e.* $\operatorname{cl}(\operatorname{cl} F) = \operatorname{cl} F$.

Proof. Let $f \in \operatorname{cl} F[x]$, and α a root of f. Then α generates all of $\operatorname{cl} F(\alpha)$, making $\operatorname{cl} F$ algebraic over F. Hence α is algebraic over F, but $\alpha \in \operatorname{cl} F$, so that $\operatorname{cl}(\operatorname{cl} F) = \operatorname{cl} F$. ■

Lemma 1.5.3. *For every field F, there exists an algebraically closed set containing F.*

Proof. Consider the polynomial ring $F[\dots, x_n, \dots]$ where $f(x_n)$ is a nonconstant polynomial over f. Consider the ideal (f). Then, if $(f) = (1)$, then

$$g_1 f_1(x_1) + \cdots + g_n f_n(x_n) = 1$$

where $g_i \in F[x_i]$. Then we get

$$g_1(x_1, \dots, x_m) f_1(x_1) + \cdots + g_n(x_1, \dots, x_m) f_n(x_n) = 1$$

Now, let F' an extension of F containing a root α_i of f_i. Then we observe that $0 = 1$ in the above equation which is a blatant contradiciton. S o (f) must be a proper ideal.

Now, by Zorn's lemma, there exists a maximal ideal M containing I. Then the quotient

$$K_1 = {}^{F[\dots, x_n, \dots]}\!\big/_{M}$$

is a field containing an imbedding of F. Moreover, f has a root in K_1, so that $f(x_n) \in (f) \subseteq M$. Then K_1 is a field in which every polynomial over F has a root. Proceeding as before with K_1, we obtain K_2 in which every polynomial over K_1 has a root. Hence, proceeding recursively, we obtain the sequence

$$F = K_0 \subseteq K_1 \subseteq K_n \subseteq \dots$$

in which everypolynomial over K_n has all its roots in K_{n+1}. Now, let

$$K = \bigcup K_n$$

Then $F \subseteq K$, and every polynomial over K has a root in K_N, for N large enough; but $K_N \subseteq K$, so that K is algebraically closed. ■

Lemma 1.5.4. *Let K be algebraically closed, and let $F \subseteq K$. Then the collection of elements of the algbraic closure* $\operatorname{cl} F$ *of K that are algebraic over F is an algebraic closure of F.*

Proof. By definition, ${}^{\operatorname{cl} F}\!\big/_{F}$ is algebraic. Then every polynomial f over F splits over K into linear factors $(x - \alpha)$, where α is a root of f. So α is algebraic over F, and hence $\alpha \in \operatorname{cl} F$. then all linear factors have a coefficient in $\operatorname{cl} F$, so that f splits completely over $\operatorname{cl} F$. ∎

Corollary. *Algebraic closures are unique up to isomorphism.*

Theorem 1.5.5 (The Fundamental Theorem of Algebra)**.** $\mathbb{C}$ *is algebraically closed.*

Corollary. $\mathbb{C}$ *contains the an algebraic closuder of any of its subfields.*

Bibliography

[1] D. Dummit, *Abstract algebra.* Hoboken, NJ: John Wiley & Sons, Inc, 2004.

[2] I. N. Herstein, *Topics in algebra.* New York: Wiley, 1975.