

Field Theory and Galois Theory.

Alec Zabel-Mena

January 12, 2023

Contents

1	Fields.	5
1.1	Field Extensions.	5
1.2	Algebraic Extensions.	9

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 $\text{char } F = p$, and if no such p exists, then we write $\text{char } F = 0$.

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

Proof. Let $\text{char } F = p$. 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 $\text{char } F = p$, 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 $\text{char} = 0$. Similarly, $\text{char } \mathbb{Z} = 0$, even though \mathbb{Z} is just an integral domain.

(2) $\text{char } \mathbb{Z}/p\mathbb{Z} = p$ and $\text{char } \mathbb{Z}/p\mathbb{Z}[x] = p$ 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 an element $\alpha \in R$ a **root** (or **zero**) of f if $f(\alpha) = 0$.

Lemma 1.1.4. *Let $\phi : F \rightarrow L$ 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 $K = F[x]/(p)$. Since p is irreducible in a principle ideal domain, (p) is a maximal ideal, and hence K is a field. Now consider the canonical map $\pi : F[x] \rightarrow K$ taking $f \rightarrow f \bmod (p)$ and let $\phi = \pi|_F$. Then $\phi \neq 0$, since $\pi : 1 \rightarrow 1$. Then ϕ is 1-1. And so $\phi(F) \simeq F$.

Now, consider F as a subfield of K . Then $p(x \bmod (p)) \equiv p(x) \bmod (p) \equiv 0 \bmod (p)$, so that $x \bmod (p)$ 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 $\theta = x \bmod (p)$. 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 $pq \in (p)$, $a(x) \equiv r(x) \bmod (p)$, 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

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

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

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

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

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

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

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

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

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

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

of degree $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, 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 $\sqrt{2} \rightarrow i$.

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

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

of degree $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ over \mathbb{Q} . 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

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

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 precisely, 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 α, β, \dots over F to be the unique minimal subfield containing all α, β, \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 $K = (F\alpha_1, \dots, \alpha_n)$ for $\alpha_1, \dots, \alpha_n \in K$, 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 $F[x] \rightarrow F(\alpha)$ taking $a(x) \rightarrow a(\alpha)$. Since $p(\alpha) = 0$, p is in the kernel of this homomorphism, and we get an induced homomorphism from $F[x]_{(p)} \rightarrow F(\alpha)$. Now, since p is irreducible, $F[x]_{(p)}$ is a field, and since the homomorphism takes $1 \rightarrow 1$, it is 1–1. Then by the first isomorphism theorem for ring homomorphisms these two fields are isomorphic. ■

Corollary. *If $\deg p = n$, then $F(\alpha) = \{a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1} : a_i \in F \text{ for all } 1 \leq i \leq n-1\}$ 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 $a - b\sqrt{2} \rightarrow a + b\sqrt{2}$.

(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 $\phi : F \rightarrow L$ 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 $F(\alpha) \rightarrow L(\beta)$ taking $\alpha \rightarrow \beta$ and extending ϕ . That is, we have the following diagram*

$$\begin{array}{ccc} F(\alpha) & \longrightarrow & L(\beta) \\ \downarrow & & \downarrow \\ F & \xrightarrow{\phi} & L \end{array}$$

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 isomorphism

$$F[x]_{(p)} \simeq L[x]_{(q)}$$

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 $\alpha \rightarrow \beta$. ■

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 exists 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 m 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 division 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 $r(\alpha) = 0$ for all α 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*

$$F(\alpha) \simeq F[x]/(m_{\alpha,F})$$

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 $[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$. 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 $F(\alpha)/F$ 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 extension K/F , of degree n , then the set $\{1, \alpha, \dots, \alpha^n\}$ is linearly dependent over F . Hence there exist $b_0, \dots, b_n \in F$ not all 0 for which

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

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

Corollary. *If an extension K/F is finite, then it is algebraic.*

Proof. If $\alpha \in K$ is algebraic, then K/F implies that $F(\alpha)/F$ is finite, since $F(\alpha) \subseteq K$. ■

Example 1.6. Let F a field of 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/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 $F(\sqrt{b^2 - 4c}) = F(\alpha)$. Moreover, $x^2 - (b^2 - 4c)$ does not have solutions in K .

We call field extensions K/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

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

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

$$a_i = b_{i1}\beta_1 + \dots + b_{in}\beta_n \text{ where } b_{ij} \in F \text{ for all } 1 \leq j \leq n$$

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 independent.

Suppose that

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

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

$$a_i = b_{i1}\beta_1 + \dots + b_{in}\beta_n = 0$$

Now, since $\{\beta_1, \dots, \beta_n\}$ is linearly independent in K over F , this implies that $b_{i1} = \dots = b_{in} = 0$ 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 $[\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}(\sqrt{2})] = 3$. Then we have the following tower of fields for

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

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 $F(\alpha, \beta) \subseteq (F(\alpha))(\beta)$. ■

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

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 $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] \leq 2$. 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 only 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, $[F(\alpha_i) : F][K : F(\alpha_i)]$ for all $1 \leq i \leq n$. So each α_i is algebraic over F . Then K is generated by finitely many algebraic elements.

Conversely, let $K = F(\alpha_1, \dots, \alpha_k) = (F(\alpha_1, \dots, \alpha_{k-1}))(\alpha_k)$. 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

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

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

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

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 $\beta \neq 0$).*

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 $\text{cl } \mathbb{Q}$ the subfield of all elements of \mathbb{C} which are algebraic over \mathbb{Q} . Then $\sqrt[n]{2} \in \text{cl } \mathbb{Q}$ for all $n \geq 1$, so that $[\text{cl } \mathbb{Q} : \mathbb{Q}] \geq n$. This makes $\text{cl } \mathbb{Q}$ an infinite algebraic extension, and we call $\text{cl } \mathbb{Q}$ the **field of algebraic numbers**.

(2) Consider $\text{cl } \mathbb{Q} \cap \mathbb{R}$ 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 $\text{cl } \mathbb{Q}$ 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 $F(\alpha, a_0, \dots, a_n)$. Since K/F is algebraic, a_0, \dots, a_n are algebraic over F , and so $F(\alpha, a_0, \dots, a_n)$ is a finite extension over F . Then α generates an extension field of degree less than n , and we get

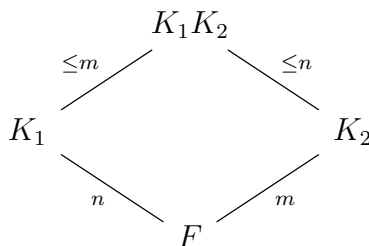
$$[F(\alpha, a_0, \dots, a_n) : F] = [F(\alpha, a_0, \dots, a_n) : F(a_0, \dots, a_n)][F(a_0, \dots, a_n) : F]$$

is finite, and $F(\alpha, a_0, \dots, a_n)$ is algebraic over F . That is, α is algebraic over F , and so L is algebraic 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 $\{\alpha_1, \dots, \alpha_m\}$ and $\{\beta_1, \dots, \beta_n\}$ are bases for K_1 and K_2 , then $\{\alpha_1\beta_1, \dots, \alpha_m\beta_n\}$ span K_1K_2 .



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 $m, n \mid [K_1K_2 : F]$ and since $K_1, K_2 \subseteq K_1K_2$ are subfields of K_1K_2 , we get the least common multiple $[m, n] \mid [K_1K_2 : F]$. 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 and Algebraic Closures.

Bibliography

- [1] D. Dummit, *Abstract algebra*. Hoboken, NJ: John Wiley & Sons, Inc, 2004.
- [2] I. N. Herstein, *Topics in algebra*. New York: Wiley, 1975.