Field Theory and Galois Theory.

Alec Zabel-Mena

February 1, 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 $\{1, \theta, \ldots, \theta^{n-1}\}$ 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 $\{1, \theta, \ldots, \theta^{n-1}\}$ span K.

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

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

Then

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

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

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

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*

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

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 ${}^{F[x]}\!\diagup_{(p)} \to F(\alpha)$. Now, since p is irreducible, ${}^{F[x]}\!\diagup_{(p)}$ 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 $1 \le i \le n-1\}$ 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*

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

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 ${}^{F(\alpha)}\!/\!_{F}$ 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 ${}^{K}\!/\!_{F}$, 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 ${}^{K}\!/\!_{F}$ 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 $\operatorname{char} F \neq 2$, 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 ${}^{K}\!/\!_{F}$ 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 ${}^{K}\!/\!_{F}$ 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

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

$$\begin{tikzcd} \mathbb{Q}(\sqrt[6]{2}) \arrow[d, dash] \\ \mathbb{Q}(\sqrt{2}) \arrow[d, dash] \\ \mathbb{Q} \end{tikzcd}$$

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 $1 \leq i \leq \deg\alpha$ 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 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 $1 \leq i \leq n$. So each α_i is algebraic over F. Then K is generated by finitely many algebraic elements.

Conversely, let $K = F(\alpha_1, \dots, \alpha_k) = (F(\alpha_1, \dots a_{k-1}))(\alpha_k)$ 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 $1 \leq i \leq k$, 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 $\operatorname{cl}\mathbb{Q}$ the subfield of all elements of $\mathbb{C}$ which are algebraic over $\mathbb{Q}$. Then $\sqrt[n]{2} \in \operatorname{cl} Q$ for all $n \geq 1$, so that $[\operatorname{cl}\mathbb{Q} : \mathbb{Q}] \geq n$. 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.*

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

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 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 1.3.1. *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 ≥ 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.

$$\begin{tikzcd}
& \mathbb{Q}(\sqrt[3]{2},i\sqrt{3}) \arrow[ddl, dash] \arrow[dr, dash] \arrow[drr, dash] \arrow[drrr, dash] & & & \\
& & \mathbb{Q}(\sqrt[3]{2}) \arrow[ddl, dash] & \mathbb{Q}(\sqrt[3]{2}(-1+\xi)) \arrow[ddll, dash] & \mathbb{Q}(\sqrt[3]{2}(-1-\xi)) \arrow[ddlll, dash] \\
\mathbb{Q}(i\sqrt{3}) \arrow[dr, dash] & & & & \\
& \mathbb{Q} & & &
\end{tikzcd}$$

(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 1.3.2. *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 1.3.3. *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. ∎

1.4 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 1.4.1. *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 1.4.2. *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 1.4.3. *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

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

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

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

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

$$K_1 = {}^{F[\dots, x_n, \dots]}\!\diagup_{M}$$

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 1.4.4. *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, ${}^{\operatorname{cl} F}\!\diagup_{F}$ 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 1.4.5 (The Fundamental Theorem of Algebra)**.** $\mathbb{C}$ *is algebraically closed.*

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

1.5 Seperability.

Definition. Let f be a polynomial over a field F with factorization

$$f(x) = a_n (x - \alpha_1)^{n_1} \dots (x - \alpha_k)^{n_k}$$

where $\alpha_1, \dots, \alpha_k$ are roots of f, and a_n is the leading coefficient of f. If $n_i > 1$, we call α_i a **multiple root** of f, and if $n_i = 1$, we call α_i a **simple root**. We call n_i the **multiplicity** of α_i.

Definition. A polynomial over a field F is said to be **seperable** if it has only simple roots. Otherwise, we say it is **inseperable**.

Lemma 1.5.1. *Seperable polynomials have all their roots distinct.*

Definition. We say a field F is a **finite field** if it has a finite number of elements. If $|F| = n$, then we denote F as $\mathbb{F}_n$.

Lemma 1.5.2. *Every finite field has finite characteristic.*

Proof. Recall that the characteristic is just the additive order of the element 1 in the field. ∎

Example 1.14. (1) $x^2 - 2 = (x + \sqrt{2})(x - \sqrt{2})$ is seperable over $\mathbb{Q}$. However $(x^2 - 1)^n$ is inseperable.

(2) Consider $x^2 - t$ over the field $\mathbb{F}_2(t)$ of rational functions over t. $x^2 - t$ is irreducible, but inseperable. Let $\sqrt{t}$ a root, then $(x - \sqrt{t})^2 = x^2 - t$ since $\operatorname{char} \mathbb{F}_2 = 2$.

Definition. The **derivative** of a polynomial $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ over a field F is the polynomial

$$Df(x) = a_1 + 2a_2 x + \cdots + n a_n x^{n-1}$$

over F.

Lemma 1.5.3. *For any two polynomials f and g over a field, the following are true.*

(1) $D(f + g) = Df + D(g)$.

(2) $D(fg) = fDg + gDf$.

Lemma 1.5.4. *A polynomial f has a multiple root α if, and only if α is a root of Df. Moreover, the minimal polynomial of α, m_α divides (f, Df).*

Proof. Let α a multiple root of f. Then $f(x) = (x - \alpha)^n g(x)$ for some polynomial g. Hence

$$Df(x) = n(x - \alpha)^{n-1} g(x) + (x - \alpha)^n Dg(x)$$

so that α is a root of Df.

Conversly, suppose that α is a root of both f and Df. Then $f(x) = (x - \alpha)g(x)$ for some polynomial g, and $Df(x) = g(x) + (x - \alpha)Dg(x)$. Now, since $Df(\alpha) = 0$, we get $h(\alpha) = 0$, so that h has a linear factor $(x - \alpha)$. This makes α a multiple root of f. ∎

Corollary. *f is seperable if and only if $(f, Df) = 1$.*

Corollary. *Every irreducible polynomial ina field F of $\operatorname{char} F = 0$ is seperable. Moreover, a polynomial over such a field is irreducible if, and only if it is the product of distinct irreducible factors.*

Proof. Let p an irreducible polynomial over F of $\deg p = n$. Then $\deg Dp = n - 1$. Up to constant factors, the factors of p are 1 and itself, so that $(p, Dp) = 1$. This makes p seperable. Therefore every irreducible polynomial over F is seperable, and the rest follows. ∎

Example 1.15. (1) Let p prime and $f(x) = x^{p^n} - x$ over the finite field $\mathbb{F}_p$, of $\operatorname{char} \mathbb{F}_p = p$. Then $Df(x) = p^n x^{p^n - 1} - 1 \equiv -1 \mod p$. Then Df has no roots, which makes f seperable.

(2) $D(x^n - 1) = nx^{n-1}$ for any field of char coprime to p. Then $D(x^n - 1)$ has a root 0 of multiplicity $n > 1$, but 0 is not a root of $x^n - 1$ so that $x^n - 1$ is seperable. That is, $x^n - 1$ has n distinct roots of unity ξ.

(3) Let F a field of $\operatorname{char} F = p$, where $p|n$. Then there are fewew than n distinct n-th roots of unity over F, since $n \equiv 0 \mod p$. Then $D(x^n - 1) = 0$, and every root of $x^n - 1$ is a multiple root.

Lemma 1.5.5. *If f is a polynomial over a field F whose derivative is* 0*, then there exist a polynomial g for which $f(x) = g(x^p)$ where* $\operatorname{char} F = p$*.*

Proof. Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n$. Then $Df(x) = a_1 + \cdots + na_n x^{n-1} = 0$, so that every exponent $i \equiv 0 \mod p$. That is, $f(x) = a_0 + a_1 x^p + \cdots + a_m x^{mp}$. Then let

$$g(x) = a_0 + a_1 x + \cdots + a_m x^m$$

then $f(x) = g(x^p)$. ■

Lemma 1.5.6. *Let F a field of* $\operatorname{char} F = p$*. The for every $a, b \in F$, $(a + b)^p = a^p + b^p$ and $(ab^p) = a^p b^p$.*

Proof. The binomial theorem gives

$$(a + b)^p = a^p + \binom{p}{1} a^{p-1} b + \cdots + \binom{p}{p-1} ab^{p-1} + b^p$$

Now, since $\binom{p}{i} \in \mathbb{Z}$ for any $1 \leq i \leq p - 1$, and p is prime (the charateristic of a field has to be prime), then $p|\binom{p}{i}$. Hence $\binom{p}{i} \equiv 0 \mod p$, so that the binomial exapnsion above reduces to

$$(a + b)^p \equiv a^p + b^p \mod p$$

Now, let $\phi : a \to a^p$, then ϕ is an automorphism of fields taking $(ab)^p = a^p b^p$. ■

Corollary. *Let F be a finite field of* $\operatorname{char} F = p$*. Then every element of F is a $p^{th} powerinF$.*

Definition. Let F be a field. We call the automorphism $F \to F$ defined by $a \to a^p$ where $p \in \mathbb{Z}$ the **Forbenius automorphism**.

Lemma 1.5.7. *Every irreducible polynomial in a finite field F is seperable.*

Proof. Suppose otherwise. Since F has finite characteristic, there is a polynomial q over F for which $p(x) = q(x^l)$, where p is the irreducible polynomial in question, and $\operatorname{char} F = l$. Let

$$q(x) = a_0 + a_1 x + \cdots + a_n x^n$$

then $a_i = b_i^p$ for some $b_i \in F$, and

$$\begin{aligned} p(x) &= q(x^l) \\ &= a_0 + a_1 x^p + \cdots + a_n x^{pn} \\ &= b_0^p + b_1^p x^p + \cdots + b_n^p x^{np} \\ &= (b_0 + b_1 x + \cdots + b_n x^n)^p \end{aligned}$$

which is a contradiction. ■

Definition. A field K of characteristic $\operatorname{char} K = p$ is called **perfect** if for every $a \in K$, there exists a $b \in K$ for which $a = b^p$, or $p = 0$.

Example 1.16. Let $n > 0$ and consider the splitting field of the polynomial $x^{p^n} - x$ over the finite field $\mathbb{F}_p$. Then $x^{p^n} - x$ has precisely p^n roots.

Let α, β be roots. Then $\alpha^{p^n} = \alpha$, and $\beta^{p^n} = \beta$. Then $(\alpha\beta)^{p^n} = \alpha\beta$ and $(\alpha^{-1})^{p^n} = \alpha^{-1}$. Moreover, $(\alpha + \beta)^{p^n} = \alpha + \beta$. So the set of p^n disctinct roots of $x^{p^n} - x$ is closed under addition, multiplication, and inverses in its splitting field. Let F be that splitting field. Notice that $F \subseteq \mathbb{F}_{p^n}$, moreover, $[F : F_p] = n$ so that $|F| = p^n$. We also have that $\mathcal{U}(F)$ is a cyclic group of order $p^n - 1$, so that $F_{p^n} \subseteq F$, since $\alpha^{p^n - 1} = 1$. Therefore $\mathbb{F}_{p^n}$ is the splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$, and so contains all the roots of $x^{p^n} - x$. Hence finite fields of order p^n exist and are unique up to isomorphism.

Lemma 1.5.8. *Let f an irreducible polynomial over a field F of $\operatorname{char} F = p$. Then there exists a unique integer $k \geq 0$ and a unique seperable polynomial s such that $f(x) = s(x^{p^k})$.*

Proof. We have that since $\operatorname{char} F = p$, there exists a polynomial f_1 over F for which $f(x) = f_1(x^p)$. Now, if f_1 is seperable, take $k = 1$ and we are done. Otherwise, there is a polynomial f_2 over F for which $f_2(x) = f_2(x^p)$, so that $f(x) = f_1(x^p) = f_2(x^{p^2})$. Then proceeding in this fashion, we obtain a seperable polynomial s for which $f(x) = s(x^{p^k})$ where $k \geq 0$. ■

Definition. Let f an irreducible polynomial over a field of characteristic p, a prime. Let f_s the polynomial for which $f(x) = f_s(x^{p^k})$ for some unique integer $k \geq 0$. Then we call the degree of f_s the **seperable degree** of f and write $\deg_s f = \deg f_s$. We call the integer p^k the **inseperable degree** and write $\deg_i f = p^k$. We call f_s the **seperable part** of f.

Lemma 1.5.9. *A polynomial f is seperable if, and only if $\deg_i f = 1$ and $\deg_s f = \deg f$. Moreover,*

$$\deg f = \deg_s f \cdot \deg_i f$$

Example 1.17. (1) $x^p - t$ over $\mathbb{F}_p(t)$ is irreducible with derivative $D = 0$. Hence $x^p - t$ is inseperable. We call $x^p - t$ a **purely inseperable polynomial**. Notice that $x^p - t$ has seperable part $(x - t)$.

(2) $x^{p^n} - t$ over $\mathbb{F}_p(t)$ is irreducible with seperable part $(x - t)$, and $\deg_i = p^n$.

(3) Let $f(x) = (x^{p^n} - t)(x^p - t)$ over $\mathbb{F}_p(t)$. Then p has two inseperable irreducible factors, and so is inseperable.

Definition. An extension K over a field F is a called **seperable** if every $\alpha \in K$ is the root of a seperable polynomial over F. Otherwise, we call K **inseperable**.

Lemma 1.5.10. *Every fnite extension of a perfect field is seperable.*

Corollary. *Finite extension fields of $\mathbb{Q}$ and $\mathbb{F}_p$ are seperable.*

1.6 Cyclotomic Polynomials.

Definition. We define **Euler's totient** to be the map $\phi : \mathbb{Z} \to \mathbb{Z}$ defined by the rule $\phi(n) = |\{a \in \mathbb{Z} : (a, n) = 1\}|$. That is, ϕ of n is the number of all integers less than n, coprime to n.

Definition. We define Ξ_n to be the **group of all primitive n-th roots of unity**, ξ for which $\xi^n = 1$.

Lemma 1.6.1. $\Xi_n \simeq {}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$.

Proof. The map $a \to \xi^a$ defines the required isomorphism. ■

Corollary. $\operatorname{ord} \Xi_n = \phi(n)$ *where ϕ is Euler's totient.*

Proof. Since $\xi^n \equiv \xi^{0 \mod n} \equiv 1$, we have every non identity power of ξ has exponenct coprime to n. That is there are $\phi(n)$ such distinct powers ofξ. ■

Corollary. *If $d|n$, then $\Xi_d \leq \Xi_n$.*

Proof. Notice that if $d|n$, then $d = mn$ for some $m \in \mathbb{Z}^+$. Then $\xi^d = 1$ implies $(\xi^d) = \xi^{dm} = \xi^n = 1$. ■

Definition. We define the **n-th cyclotomic polynomial** to be the polynomial

$$\Phi_n(x) = \prod x - \xi$$

having as roots all n-primitive roots of unity.

Lemma 1.6.2. *The n-th cyclotomic polynomial Φ_n has degree* $\deg \Phi_n = \phi(n)$*, where ϕ is Euler's totient.*

Proof. Recall that $\operatorname{ord} \Xi_n = \phi(n)$, and since the elements of Ξ_n are the roots of Φ_n, there are $\phi(n)$ such roots. This puts $\deg \Phi_n = \phi(n)$. ■

Example 1.18 (Computing Cyclotomic Polynomials)**.** Recall that the polynomial $x^n - 1$ has as roots precisely all n-th roots of unity ξ, that is $\xi^n = 1$. If $x^n - 1 \in F[x]$, F a field, the the splitting field of $x^n - 1$ is $F(\xi)$. Then we have

$$x^n - 1 = \prod_{\xi \in \Xi_n} (x - \xi)$$

Now, grouping those factors where $\xi^d = 1$ for some $d|n$, then we have

$$x^n - 1 = \prod_{\xi \in \Xi_d} (x - \xi) \prod_{\xi \in \Xi_n} (x - \xi) = \prod d|n \prod_{\xi \in \Xi_n} (x - \xi) = \prod_{d|n} \Phi_n(x)$$

that is,

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

which gives a method for computing Φ_n recursively.

We have $\Phi_1(x) = x - 1$ and $\Phi_2(x) = x + 1$. Now, $\Phi_3(x) = \Phi_1(x)\Phi_3(x) = (x - 1)\Phi_3(x)$, so that

$$Phi_n(x) = x^2 + x + 1$$

We have $\Phi_4(x) = \Phi_1(x)\Phi_2(x)\Phi_4(x) = (x - 1)(x + 1)\Phi_4(x) = (x^2 - 1)\Phi_4(x)$. So

$$\Phi_4(x) = x^2 + 1$$

Similarly,

$$\begin{aligned}
\Phi_5(x) &= x^4 + x^3 + x + 1 \\
\Phi_6(x) &= x^2 - x + 1 \\
\Phi_7(x) &= x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \\
\Phi_8(x) &= x^4 + 1 \\
\Phi_9(x) &= x^6 + x^x + 1 \\
\Phi_{10}(x) &= x^4 - x^3 + x^2 - x + 1 \\
\Phi_{11}(x) &= x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \\
\Phi_{12}(x) &= x^4 - x^2 + 1
\end{aligned}$$

Also observe that if p is prime, then

$$\Phi_p(x) = \sum_{i=0}^{p-1} x^i = x^{p-1} + x^p + \cdots + x + 1$$

Lemma 1.6.3. *$\Phi_n(x)$ is monic over $\mathbb{Z}$.*

Proof. Notice that since $x^n - 1 = \prod \Phi_d(x)$, is monic, then each Φ_d must also be monic for all $d|n$.

Now, by induction on n, for $n = 1$, it is clear that $x - 1$ has coefficiencts in $\mathbb{Z}$ (if $x^n - 1 \in \mathbb{Z}[x]$ we are done, if not, just take $1_F \to 1_{\mathbb{Z}}$, whre F is the underlying field of $x^n - 1$). Now, suppose that $\Phi_d(x) \in \mathbb{Z}[x]$ for all $1 \leq d < n$, and $d|n$. Then $x^n - 1 = f(x)\Phi_n(x)$, where $f(x) = \prod \Phi_d(x)$ is monic over $\mathbb{Z}$. Moreover, $f|x^n - 1$, in the splitting field $\mathbb{Q}(\xi)$ (since we take $1_F \to F_{\mathbb{Z}}$), where $\xi^n = 1$. Then $f|x^n - 1$ over $\mathbb{Q}$ by the division theorem, and by Gauss' lemma, $f|x^n - 1$ in $\mathbb{Z}$. So $\Phi_n \in \mathbb{Z}[x]$. ■

Theorem 1.6.4. *Φ_n is irreducible over $\mathbb{Z}$.*

Proof. Again, if $x^n - 1 \in F[x]$ for some field F, take $1_F \to 1_{\mathbb{Z}}$ so that $x^n - 1 \in \mathbb{Z}[x]$. Suppose then that $\Phi_n(x) = f(x)g(x)$ where f and g are monic, and f is irreducible. Let $\xi^n = 1$, a primitive n-th root, so that ξ is a root of f. Then f is the minimal polynomial for ξ over $\mathbb{Q}$. Now, let p a prime such that $p \nmid n$. Then ξ^p is a n-th root, of f or g. If $f(\xi^p) = 0$, then for all a with $(a, n) = 1$, we have ξ^a is a root of f. Moreover, $a = p_1 \dots p_k$ where each $p_i \nmid n$ is prime. That means tht ξ^{p_1}, $(\xi^{p_1})^{p_2}, \dots, \xi^n$ are all roots of f making $f = \Phi_n$ and we are done.

Suppose then that $g(\xi^p) = 0$. Then ξ is root of $g(x^p)$, and since f is minimal, $f | g(x^p)$ in $\mathbb{Z}[x]$. Then we have $g(x^p) = f(x)h(x)$ for $f, h \in \mathbb{Z}[x]$. reducing mod p, we get $g(x^p) \equiv f(x)h(x) \mod p$ in $\mathbb{F}_p[x]$; but $g(x^p) \equiv (g(x))^p \mod p$. Since $\mathbb{F}_p[x]$ is a unique factorization domain, we get that $f \mod p$ and $g \mod p$ have a common factor. Then $\Phi_n(x) \equiv f(x)g(x) \mod p$ has a multiple root in $\mathbb{F}_p[x]$; implying that $x^n - 1$ has a multiple root, which is impossible; since $x^n - 1$ has n distinct roots. Therefore ξ^p is a root of f. ■

Corollary. $[\mathbb{Q}(\xi) : \mathbb{Q}] = \phi(n)$.

Proof. We have by above that Φ_n is the minimal polynomial for ξ over $\mathbb{Q}$. ■

Example 1.19. Let $\xi^8 = 1$ an 8-th root of unity. Then $[\mathbb{Q}(\xi) : \mathbb{Q}] = 4$ and $\mathbb{Q}(\xi)$ has minimal polynomial $\Phi_8(x) = x^4 + 1$. Moreover, $\mathbb{Q}(\xi)$ contains a primitive 4-th root of unity $i^4 = 1$ (over $\mathbb{C}$, $i^2 = -1$). So that $\mathbb{Q}(i) \subseteq \mathbb{Q}(\xi)$. We als get that $\xi + \xi^7 = \sqrt{2}$ (since $\xi = e^{\frac{2i\pi}{8}}$ over $\mathbb{C}$), and $\mathbb{Q}(\xi) = \mathbb{Q}(i, \sqrt{2})$.

Chapter 2

Galois Theory

2.1 Definitions and Examples.

Definition. An isomorphism of a field K onto itself is called an **automorphism**. We denote the set of all automorphisms of K $\operatorname{Aut} K$, and for $\sigma \in \operatorname{Aut} K$, we write $\sigma\alpha$ to mean $\sigma(\alpha)$. We say an automorphism σ of K **fixes** an element $\alpha \in K$ if $\sigma\alpha = \alpha$. We say σ **fixes** a subset $F \subseteq K$ if $\sigma\alpha = \alpha$ for all $\alpha \in F$. We denote $\operatorname{Aut} {}^{K}\!/_{F}$ to be the set of all automorphisms of K that fix F, where ${}^{K}\!/_{F}$ is a field extension.

Lemma 2.1.1. *Let K be a field. Then $\operatorname{Aut} K$ is a group. Moreover, if K is an extension of a field F, then $\operatorname{Aut} {}^{K}\!/_{F} \leq \operatorname{Aut} K$.*

Lemma 2.1.2. *Let K be an extension of F, and let $\alpha \in K$ algebraic over F. Then for every $\sigma \in \operatorname{Aut} {}^{K}\!/_{F}$, $\sigma\alpha$ is a root of the minimal polynomial of α over F; that is, $\operatorname{Aut} {}^{K}\!/_{F}$ permutes the roots of irreducible polynomials.*

Proof. Suppose that $a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} + \alpha^n = 0$, where $a_i \in F$ for all $1 \leq i \leq n$, and $a_n = 1$. Notice that if σ is an automorphism of K, then it is a homomorphism, moreover, since σ fixes F, and $a_i \in F$, we get $\sigma(a_i\alpha^i) = a_i\sigma\alpha^i$. Therefore,

$$\begin{aligned}
\sigma(a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} + \alpha^n) &= \sigma 0 = 0 \\
\sigma(a_0) + \sigma(a_1\alpha) + \cdots + \sigma(a_{n-1}\alpha^{n-1}) + \sigma(\alpha^n) &= 0 \\
a_0 + a_1\sigma\alpha + \cdots + a_{n-1}\sigma\alpha^{n-1} + \sigma\alpha^n &= 0
\end{aligned}$$

which makes $\sigma\alpha$ a root. ■

Example 2.1. (1) The identity map is an automorphism called the **trivial automorphsim**, and just maps elements of a field onto themselves. We denote this automorphism by ι. Notice additionally, that if σ is an automorphism of a field, then $\sigma : 1 \to 1$ and $\sigma : 0 \to 0$, so that $\sigma a = a$ for any element a in the prime subfield. That is, the automorphism group of a field fixes its prime subfield. In partucular, notice that $\mathbb{Q}$ and $\mathbb{F}_p$ have only the trivial automorphism, so that $\operatorname{Aut} \mathbb{Q} = \langle \iota \rangle$ and $\operatorname{Aut} \mathbb{F}_p = \langle \iota \rangle$.

(2) If $\tau \in \operatorname{Aut}\mathbb{Q}(\sqrt{2}) = \operatorname{Aut} {}^{\mathbb{Q}(\sqrt{2})}\!/_{\mathbb{Q}}$, then $\tau\sqrt{2} = \pm\sqrt{2}$. Then τ fixes $\mathbb{Q}$, and we have that it sends elements $\tau : a + b\sqrt{2} \to a \pm b\sqrt{2}$. In the case of addition, we have that $\tau = \iota$ the identity. The latter case of subtraction gives $\tau = a + b\sqrt{2} \to a - b\sqrt{2}$, so that $\operatorname{Aut}\mathbb{Q}(\sqrt{2}) = \langle \tau \rangle$ a cyclic group of order 2 generated by τ.

Lemma 2.1.3. *Let $H \leq \operatorname{Aut} K$ for some field K. Then the collection F of elements of K fixed by H is a subfield of K.*

Proof. LEt $h \in H$, and $a, b \in F$. Then $ha = a$, $hb = b$, so that $h(a \pm b) = a \pm b$, and $h(ab) = ab$, and $h(a^{-1}) = (ha)^{-1} = a^{-1}$. ■

Definition. Let K be a field. If $H \leq \operatorname{Aut} K$, we define the **fixed field** of H to be the subfield of K fixed by H, and we denote it $\mathcal{F}(H)$.

Lemma 2.1.4. *If $F_1 \subseteq F_2 \subseteq K$ are subfields of a field K, then $\operatorname{Aut} {}^{K}\!/_{F_2} \subseteq \operatorname{Aut} {}^{K}\!/_{F_1}$. Moreover, if $H_1 \leq H_2 \leq \operatorname{Aut} K$, then $\mathcal{F}(H_2) \subseteq \mathcal{F}(H_1)$.*

Example 2.2. (1) The fixed field of $\operatorname{Aut}\mathbb{Q}(\sqrt{2})$ is the field

$$F = \{a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2}) : \sigma(a + b\sqrt{2}) = a + b\sqrt{2}\}$$

by definition. Then $a - b\sqrt{2} = a + b\sqrt{2}$ so that $b = 0$. Therefore $F = \mathbb{Q}$ and $\mathbb{Q}$ is the fixed field.

(2) Consider $\operatorname{Aut}\mathbb{Q}(\sqrt[3]{2}) = \langle \iota \rangle$. Then the fixed field of $\operatorname{Aut} {}^{\mathbb{Q}(\sqrt[3]{2})}\!/_{\mathbb{Q}}$ is $\mathbb{Q}(\sqrt[3]{2})$.

Lemma 2.1.5. *Let E be the splitting field over a field F of a polynomial $f(x)$ over F. Then*

$$\operatorname{ord}\operatorname{Aut} {}^{E}\!/_{F} \leq [E : F]$$

Proof. By induction on $[E : F]$. If $[E : F] = 1$, then $E = F$, and we are done. Now, for $[E : F] \geq 1$, $f(x)$ has atleast one irreducible factor $p(x)$ of degree $\deg p > 1$. Now, let F' be the corresponding field to F with splitting field E', corresponding to E. Let $f'(x)$ be the polynomial over F' the polynomial corresponding to f over F, with irreducible factor $p'(x)$ corresponding to the irreducible factor p. Now, let α be a root of p. IF σ is an extension of an isomorphism ϕ to E, then the restriction $\tau = \sigma|_{F(\alpha)}$ is an isomorphism of $F(\alpha)$ onto a subfield of E'. Since α generates $F(\alpha)$, τ is completely determined by its action on α; i.e. $\tau\alpha$, so that $\tau\alpha$ is a root of p'. We then get the following diagram:

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

COnversly, let β be a root of p'. Then there exist extensions τ and σ of the isomorphism ϕ giving the above diagram (replace $\tau\alpha$ with β). Now, the number of extensions of ϕ to τ is equal to the number of distinct roots of p'. Since $\deg p = \deg p' = [F(\alpha) : F]$, the number of extensions to τ is at most $[F(\alpha) : F]$.

Now, notice that $[E : F(\alpha)] < [E : F]$. Therefore, by the induction hypothesis, the number of extensions of τ to σ is at most $[E : F(\alpha)]$. Therefore, the number of extensions of ϕ to σ is at most $[E : F(\alpha)][F(\alpha) : F] = [E : F]$.

Finally, if $F = F'$, we have $f = f'$ (and $p = p'$), and so ϕ is the identity map and $E = E'$. THis makes σ an automorphism of E which fixes F. The proof is complete. ■

Corollary. *If K is the splitting field of a seperable polynomial $f(x)$ over a field F, then* $\operatorname{ord}\operatorname{Aut} {}^{K}\!/_{F} = [K : F]$.

Definition. We call a finite field extension ${}^{K}\!/_{F}$ a **Galois extension** if $\operatorname{ord}\operatorname{Aut} {}^{K}\!/_{F} = [K : F]$. We call $\operatorname{Aut} {}^{K}\!/_{F}$ the **Galois group** of ${}^{K}\!/_{F}$, and write $\operatorname{Gal} {}^{K}\!/_{F}$.

Example 2.3. (1) ${}^{\mathbb{Q}(\sqrt{2})}\!/_{\mathbb{Q}}$ is Galois, and $\operatorname{Gal} {}^{\mathbb{Q}(\sqrt{2})}\!/_{\mathbb{Q}} = \langle \sigma \rangle \simeq {}^{\mathbb{Z}}\!/_{2\mathbb{Z}}$, where $\sigma : a + b\sqrt{2} \to a - b\sqrt{2}$.

(2) Any quadratic extension field K over F is Galois over F, provided $\operatorname{char} F \neq 2$. Then any quadratic extension K of F, of degree $[K : F] = 2$ is of the form $F(\sqrt{D})$, where $D \in \mathbb{Z}^+$ is squarefree. Hence $K = F(\sqrt{D})$ is the splitting field of the polynomial $x^2 - D$.

(3) $\mathbb{Q}(\sqrt[3]{2})$ is not Galois over $\mathbb{Q}$, since $\operatorname{ord}\operatorname{Aut} {}^{\mathbb{Q}(\sqrt[3]{2})}\!/_{\mathbb{Q}} = 1$, but $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.

(4) $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is the splitting field of the seperable polynomial $(x^2 - 2)(x^2 - 3)$ over $\mathbb{Q}$. Hence $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is Galois over $\mathbb{Q}$, and has Galois group $\operatorname{Gal} {}^{\mathbb{Q}(\sqrt{2},\sqrt{3})}\!/_{\mathbb{Q}}$ of order 6. Moreover, since the automorphisms of this group are completely determined by the roots $\sqrt{2}$ and $\sqrt{3}$, we get the possible automorphisms are given by the maps

$$\begin{array}{ll} \sqrt{2} \to \sqrt{2} & \sqrt{3} \to -\sqrt{3} \\ \sqrt{2} \to -\sqrt{2} & \sqrt{3} \to \sqrt{3} \\ \sqrt{2} \to \sqrt{2} & \sqrt{3} \to -\sqrt{3} \\ \sqrt{2} \to -\sqrt{2} & \sqrt{3} \to -\sqrt{3} \end{array}$$

Now, let $\sigma : \sqrt{2} \to -\sqrt{2}, \sqrt{3} \to \sqrt{3}$ and $\tau : \sqrt{2} \to \sqrt{2}, \sqrt{3} \to -\sqrt{3}$. Then $\sigma\tau : \sqrt{2} \to -\sqrt{2}, \sqrt{3} \to -\sqrt{3}$. Therefore we have

$$\operatorname{Gal} {}^{\mathbb{Q}(\sqrt{2},\sqrt{3})}\!/_{\mathbb{Q}} = \langle \sigma, \tau \rangle \simeq V_4$$

where V_4 is the Klein 4-group.

We can also determine the fixed fields correspongidng to each subgroup of $\langle \sigma\tau \rangle$. That is, $\mathcal{F}(\langle \sigma\tau \rangle)$ is the set of all elements fixed by $\sigma\tau$ and has elements of the form $a+b\sqrt{6}$. So

$\mathcal{F}(\langle\sigma\tau\rangle) = \mathbb{Q}(\sqrt{6})$. The table below lists the fixed fields of the Galois group considered.

subgroup	fixed field
$\langle\iota\rangle$	$\mathbb{Q}(\sqrt{2},\sqrt{3})$
$\langle\sigma\rangle$	$\mathbb{Q}(\sqrt{3})$
$\langle\sigma\tau\rangle$	$\mathbb{Q}(\sqrt{6})$
$\langle\tau\rangle$	$\mathbb{Q}(\sqrt{2})$
$\langle\sigma,\tau\rangle$	$\mathbb{Q}$

(5) The roots of x^3-2 over $\mathbb{Q}$ are given by

$$\sqrt[3]{2} \qquad \xi\sqrt[3]{2} \qquad \xi^2\sqrt[3]{2}$$

where $\xi^3 = 1$ is the 3-rd root of unity. Additionally, the splitting field of x^3-2 over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt[3]{2},\xi\sqrt[3]{2})$ of degree 6. Now, x^3-2 is irreducible over $\mathbb{Q}$, and hence seperable over $\mathbb{Q}$. This makes $\mathbb{Q}(\sqrt[3]{2},\xi\sqrt[3]{2})$ Galois over $\mathbb{Q}$, of order 6.

Consider now the set of generators $\sqrt[3]{2}$ and ξ. Then an automorphism σ takes $\sqrt[3]{2}\to\sqrt[3]{2},\xi\sqrt[3]{2}$, or $\xi^2\sqrt[3]{2}$, and takes $\xi\to\xi$ or ξ^2. Since these are the roots of the cyclotomic polynomial $\Phi_3(x) = x^2+x+12+x+1$, σ is completely determined by the actions on $\sqrt[3]{2}$ and ξ. Hence there are 6 possible automorphisms.

Let

$$\begin{array}{ll} \sigma : \sqrt[3]{2}\to\xi\sqrt[3]{2} & \xi\to\xi \\ \tau : \sqrt[3]{2}\to\sqrt[3]{2} & \xi\to\xi^2 \end{array}$$

We obtain then the elements

$$\iota \qquad \sigma^2 \qquad \tau\sigma^2 = \sigma\tau$$

and we get the additional relations

$$\sigma^2 = \tau^2 = \iota$$

so that

$$\operatorname{Gal}{}^{\mathbb{Q}(\sqrt[3]{2},\xi\sqrt[3]{2})}\!\big/_{\mathbb{Q}} = \langle\sigma,\tau\rangle \simeq S_3$$

The fixed field of $\langle\sigma^2\rangle$ is $\mathbb{Q}(\xi)$.

(6) $\mathbb{Q}(\sqrt[4]{2})$ is not Galois over $\mathbb{Q}$. We have $[\mathbb{Q}(\sqrt[4]{2}):\mathbb{Q}] = 4$ but that any automorphism takes $\sqrt[4]{2}$ onto $\pm\sqrt[4]{2}$, or $\pm i\sqrt[4]{2}$. But $\pm i\sqrt[4]{2}\notin\mathbb{Q}(\sqrt[4]{2})$. Notice however that $\mathbb{Q}(\sqrt[4]{2})$ is Galois over $\mathbb{Q}(\sqrt{2})$, and $\mathbb{Q}(\sqrt{2})$ is Galois over $\mathbb{Q}$.

(7) The extension field $\mathbb{F}_{p^n}$ is Galois over $\mathbb{F}_p$. Recall that $\mathbb{F}_{p^n}$ is the splitting field of the seperable polynomial $x^{p^n}-x$ over $\mathbb{F}_p$. Then $\operatorname{ord}\operatorname{Gal}{}^{\mathbb{F}_{p^n}}\!\big/_{\mathbb{F}_p} = n$ and the Frobenius automorphism given by

$$\sigma : \alpha\to\alpha^p$$

generates the Galois group, making it $\langle\sigma\rangle$, a cyclic group of order n.

(8) The extension $\mathbb{F}_2(x)$ is not Galois over $\mathbb{F}_2(t)$, since $x^2 - t$ is not seperable. Moreover, any automorphism of $\mathrm{Aut}\,{}^{\mathbb{F}_2(x)}\!/_{\mathbb{F}_2(t)}$ sends x to the only root of $x^2 - t$, making it the trivial group.

2.2 The Fundamental Theorem of Galois Theory.

Definition. A **linear character** of a group G with values in a field L is a homomorphism $\chi : G \to \mathcal{U}(L)$. We say that distinct linear characters $\chi_1, \dots, \chi_n$ of G are **linearly independent** over L if they are linearly independent, as functions, over G.

Theorem 2.2.1. *If $\chi_1, \dots, \chi_n$ are distinct linear characters of a group G with values in a field L, then they are linearly independent over L.*

Proof. Suppose that $\chi_1, \dots, \chi_n$ are linearly dependent, and choose a dependence relation with minimum of m nonzero coefficients $a_1, \dots, a_m \in L$, so that

$$a_1\chi_1 + \cdots + a_n\chi_m = 0$$

Then for any $g \in G$, we have

$$a_1\chi_1(g) + \cdots + a_n\chi_m(g) = 0$$

Now, let $g_0 \in G$, with $\chi_1(g_0) \neq \chi_m(g_0)$. Then

$$a_1\chi_1(g_0g) + \cdots + a_n\chi_n(g_0g) = a_1\chi(g_0)\chi(g) + \cdots + a_m\chi_m(g_0)\chi_m(g) = 0$$

multiplying the preceeding equation with the above by $\chi_m(g_0)$ and subtracting from the above equation, we get

$$a_1(\chi_1(g_0) - \chi_m(g_0))\chi_1(g) + \cdots + a_m(\chi_1(g_0) - \chi_m(g_0))\chi_m(g) = 0$$

which gives a linear dependence relation with fewer than m nonzero coefficients; which contradicts our choice of m. Therefore $\chi_1, \dots, \chi_n$ must be linearly independent. ■

Corollary. *If $\sigma_1, \dots, \sigma_n$ are distinct embeddings of a field K into a field L, then they are linearlyy independent as functions.*

Theorem 2.2.2. *Let $G = \{\sigma_1, \dots, s_n\}$ where $\sigma_1 = \iota$ a subgroup of automorphisms of a field K, and let F be the corresponding fixed field. THen*

$$[K : F] = \operatorname{ord} G = n$$

Proof. Suppose that $n > [K : F]$, and consider the basis $\{\omega_1, \dots, \omega_m\}$ of ${}^{K}\!/_{F}$ as a vector space so that $[K : F] = m$. Then the matrix equation

$$\begin{pmatrix} \sigma_1\omega_1 & \dots & \sigma_n\omega_m \\ \vdots & \ddots & \vdots \\ \sigma_n\omega_1 & \dots & \sigma_n\omega_m \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} = 0 \tag{2.1}$$

has nontrivial solution $\begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix}$. Let $a_1, \dots, a_m \in F$, so that $\sigma_i \alpha_j = \alpha_j$ for each $1 \le i \le n$ and $1 \le j \le m$. Multyplying by $\begin{pmatrix} \sigma_1 a_1 \\ \vdots \\ \sigma_m a_1 \end{pmatrix}$, we obtain

$$\begin{pmatrix} a_1\sigma_1\omega_1 & \dots & a_1\sigma_1\omega_1 \\ \vdots & \ddots & \vdots \\ a_m\sigma_m\omega_1 & \dots & a_m\sigma_n\omega_m \end{pmatrix} \begin{pmatrix} \beta_1 \\ \vdots \\ b_n \end{pmatrix} = 0$$

so that we can obtain the equation

$$\sigma_1(a_1\omega_1 + \cdots + a_m\omega_m)\beta_1 + \cdots + \sigma_n(a_1\omega_1 + \cdots + a_m\omega_m)\beta_n = 0$$

Where $\beta_1, \dots, \beta_n$ are not all 0. Now, since $\{\omega_1, \dots, \omega_m\}$ is an F-basis for K, for all $\alpha \in K$, we get that $\alpha = a_1\omega_1 + \cdots + a_m\omega_m$. So we have from the above equation

$$(\sigma_1\alpha)\beta_1 + \dots (\sigma_n\alpha)\beta_n = 0$$

so that $\{\sigma_1, \dots, \sigma_n\}$ are linearly dependent over K; which contradicts the above corollary. No $n \le [K : F]$.

Now, suppose that $n < [K : F]$, and thte tere are more than n F-linearly independent elements $\alpha_1, \dots, \alpha_{n+1} \in K$. Then

$$\begin{pmatrix} \sigma_1\alpha_1 & \dots & \sigma_1\alpha_{n+1} \\ \vdots & \ddots & \vdots \\ \sigma_n\alpha_1 & \dots & \sigma_n\alpha_{n+1} \end{pmatrix} \begin{pmatrix} x_1 \\ \dots \\ x_{n+1} \end{pmatrix} = 0$$

has nontrivial solution with entries $\beta_1, \dots, \beta_{n+1} \in K$. Now, if $\beta_i \in F$ for all $1 \le i \le n+1$, we get an immediate contradiction of the linear independence of $\{\alpha_1, \dots, \alpha_{n+1}\}$ over F. So at least one $\beta_i \notin F$.

Now, choose a nontrivial solution with minimum of r nonzero entries β_i. Suppose also that $\beta_r = 1$, then at least one $\beta_i \notin F$, for $1 \le i \le r-1$, and so $r > 1$. SUppose then that $\beta_1 \notin F$. Then the matrix equation

$$\begin{pmatrix} \sigma_1\alpha_1 & \dots & \sigma_1\alpha_{r-1} & \sigma_1\alpha_r \\ \vdots & \ddots & \vdots & \\ \sigma_n\alpha_n & \dots & \sigma_n\alpha_{r-1} & \sigma_n\alpha_r \end{pmatrix} \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_{r-1} \\ 1 \end{pmatrix} = 0$$

Now, since $\beta_1 \notin F$, there exists an automorphsim σ_{k_0} of K with $\sigma_{k_0}\beta_1 \ne \beta_1$ for $1 \le k_0 \le n$. Applying σ_{k_0} to each row of the above equation yields a row of the form

$$\sigma_{k_0}(\sigma_j\alpha_1)(\sigma_{k_0}\beta_1) + \cdots + \sigma_{k_0}(\sigma_j\alpha_{r-1})(\sigma_{k_0}\beta_{r-1}) + \sigma_j\alpha_r = 0$$

However, since G is a group, $\sigma_{k_0}\sigma_j = \sigma_i$ for $1 \leq i, j \leq n$, so we get

$$(\sigma_i\alpha_1)(\sigma_{k_0}\beta_1) + \cdots + (\sigma_i\alpha_{r-1})(\sigma_{k_0}\beta_{r-1}) + \sigma_i\alpha_r = 0$$

Subtracting this equation from the one preceeding it, we obtain

$$(\sigma_i\alpha_1)(\beta_1 - \sigma_{k_0}\beta_1) + \cdots + (\sigma_i\alpha_{r-1})(\beta_{r-1} - \sigma_{k_0}\beta_{r-1}) = 0$$

with $x_1 = \beta_1 - \sigma_{k_0}\beta_1 \neq 0$. This choice of k_0 gives fewer than r nonzero coefficients of a nontrivial solutions, which contradicts the choice of r. Therefore $n = [K : F]$. ■

Corollary. *If K is a finite extension over a field F, then*

$$\operatorname{ord}\operatorname{Aut} {}^{K}\!/_{F} \leq [K : F]$$

with equality holding if, and only if F is the fixed field of $\operatorname{Aut} {}^{K}\!/_{F}$.

Proof. Let F_1 be the fixed field of $\operatorname{Aut} {}^{K}\!/_{F}$, so that $F \subseteq F_1 \subseteq K$. TYhen $[K : F_1] = \operatorname{ord}\operatorname{Aut} {}^{K}\!/_{F}$, hence

$$[K : F] = (\operatorname{ord}\operatorname{Aut} {}^{K}\!/_{F})[F_1 : F]$$

■

Corollary. *If G is a finite subgroup of automorphisms of a field K, and F is its fixed field, then* $\operatorname{Aut} {}^{K}\!/_{F} = G$ *so that K is Galois over F with Galois group G.*

Proof. By definition, we have that since G fixes the elements of F, then $G \leq \operatorname{Aut} {}^{K}\!/_{F}$. THen $\operatorname{ord} G = [K : F]$ and by the above corollary, we get

$$\operatorname{ord}\operatorname{Aut} {}^{K}\!/_{F} \leq [K : F]$$

so that

$$[K : F] = \operatorname{ord} G \leq \operatorname{ord}\operatorname{Aut} {}^{K}\!/_{F} \leq [K : F]$$

and equality holds. ■

Corollary. *If G and H are distinct finite subgroups of* $\operatorname{Aut} K$*, then their fixed fields are also distinct.*

Proof. Let F_G the fixed field of G, and F_H the fixed field of H. I f $F_G = F_H$, then we have that H fixes F_G, and since any automorphism fixing F_G is in G, we have $H \leq G$. By similar reasoning, we get $G \leq H$ so that $G = H$. ■

Theorem 2.2.3. *The extension K over a field F is Galois if, and only if K is the splitting field of some seperable polynomial in F. Moreover, every irreducible polynomial over F having at least one root in K splits over K.*

Proof. By lemma 2.1.5, the splitting field of a seperable polynomial over a field is Galois.

Now, suppose that K is Galois over F, and let $p(x) \in F[x]$ an irreducible polynomial with a root $\alpha \in K$. Consider, for each $\sigma_i \in \operatorname{Gal} {}^{K}\!/_{F}$ the elements

$$\alpha \qquad \sigma_2\alpha \qquad \dots \qquad \sigma_n\alpha$$

where $\sigma_1 = \iota$, and let

$$\alpha \qquad \alpha_2 \qquad \dots \qquad \alpha_n$$

be the distinct elements taken on by these permutations (in no particular order). If $\tau \in \operatorname{Gal} {}^{K}\!/_{F}$, by the group law, we get $\tau\sigma_i = \sigma_j$ for all $1 \leq i, j \leq n$. APplying τ to α_i we het permutations of the elements $\alpha, \alpha_2, \dots, \alpha_n$. Then the polynomial $f(x) = (x - \alpha)(x - \alpha_2) \dots (x - \alpha_n)$ has coefficients fixed by the elements of $\operatorname{Gal} {}^{K}\!/_{F}$. That is, the coefficients lie in the fixed field F. Hence $f \in F[x]$.

Now, since p is irreducible with root α, it is the minimal polynomial for α over F, and hence $p|f$. Moreover, we can pbserve that $f|p$, so that $p(x) = f(x)$, which makes $p(x)$ seperable with all its roots in K.

Now, let $\{\omega_1, \dots, \omega_n\}$ be a basis for ${}^{K}\!/_{F}$ as a vector space, and let $p_i(x)$ the minimal polynomial for ω_i over F for all $1 \leq i \leq n$. Then p_i is seperable, with roots in K. Let $g(x) = p_1(x) \dots p_n(x)$ (where this product is squarefree). Then if E is the splitting field of g over F, then $\omega_i \in E$ for all $1 \leq i \leq n$, so that $K \subseteq E$. On the otherhand, since g splits over K, we get $E \subseteq K$, and so $K = E$ is the splitting field of g over F. ■

Definition. LEt K be an extension of a field F. If $\alpha \in K$, and $\sigma \in \operatorname{Gal} {}^{K}\!/_{F}$, we call the permutations $\sigma\alpha$ **Galois conjugates** (or simply **conjugates**) of α over F. If E is a sbufield of K containing F, then we call σE the **conjugate field** of Eover F.

Theorem 2.2.4 (The Fundamental Theorem of Galois Theory)**.** *Let K be Galois over a field F. Then there is a 1–1 correspondence of the subfields E of K, each containing F, onto the subgroups of* $\operatorname{Gal} {}^{F}\!/_{K}$. *This correspondence is given by taking each E to elements of* $\operatorname{Gal} {}^{K}\!/_{F}$ *fixing E, and by taking subgroups of* $\operatorname{Gal} {}^{K}\!/_{F}$ *to thier fixed fields. Moreover, this correspondence gives the following*

(1) If E_1 and E_2 correspond to H_1 and H_2, then $E_1 \subseteq E_2$ if, and only if $H_2 \leq H_1$.

(2) $[K : E] = \operatorname{ord} H$ *and* $[E : F] = [\operatorname{Gal} {}^{K}\!/_{F} : H]$.

(3) K is Galois over E with Galois group $H = \operatorname{Gal} {}^{K}\!/_{E}$.

(4) E is Galois over F if, and only if $H \trianglelefteq \operatorname{Gal} {}^{K}\!/_{F}$, *and* $\operatorname{Gal} {}^{E}\!/_{F}$ *is isomorphic to the quotient group of* $\operatorname{Gal} {}^{K}\!/_{F}$ *by H.*

(5) *If E_1 and E_2 correspond to H_1 and H_2, then $E_1 \cap E_2$ corresponds to $\langle H_1, H_2\rangle$, and E_1E_2 corresponds to $H_1 \cap H_2$. Moreover, the lattice of subfields of K containing F is dual to the lattice of subgroups of* $\operatorname{Gal} {}^{K}\!/_{F}$

Proof. Take $G = \operatorname{Gal} {}^{K}\!/_{F}$, and $H \leq G$. Obtain a unique fixed field of E, of H. Since fixed fields of distinct subgroups of G are distinct, we get that the correspondence is 1–1.a Now, let K be the splitting field of a seperable polynomial $f(x)$ over F. Consider $f(x)$ as a polynomial over E, for any subfield E of K containing F. Then K is the splitting field of f over E, and by theorem 2.2.3, K is Galois over E. Then E is the fixed field of the automorphism group $\operatorname{Aut} {}^{K}\!/_{E}$ which is a subgroup of G. Hence every subfield of K containing F is the fixed field of a subgroup of G, and we have proved that the correspondence is onto and we get the required bijection. We also have by lemma 2.1.4, that this correspondence is inclusion reversing.

Now, notice that for any automorphism $\sigma \in G$, $\sigma|_E$ is an embedding of E onto σE and $\sigma E \subseteq K$ is a subfield. Conversely, let $\tau : E \to \tau E \subseteq \operatorname{cl} F$ be an embedding of E. If $\alpha \in E$, and m_α is the minimum polynomial of α over F, then $\tau\alpha$ is alos a root of m_α, and K contains all the roots of m_α. Now, K is the splitting field of f, and hence, also the splitting field of $\tau f(x)$. Then if we extend τ to an isomorphism σ, we get the diagram

$$\begin{array}{lccc} \sigma : & K & \longrightarrow & K \\ & | & & | \\ \tau : & E & \longrightarrow & \tau E \end{array}$$

and since σ fixes F, then every embedding τ of E fixing F is the restriction of some automorphism σ of K.

Now, two autmorphisms $\sigma, \sigma' \in G$ restrict to the same embedding if, and only if $\sigma^{-1}\sigma' = \iota$, the identity map on E. This makes $\sigma^{-1}\sigma' \in H$; i.e. $\sigma' \in \sigma H$. Since $\operatorname{Gal} {}^{K}\!/_{E} = H$, and letting $\operatorname{Emb} {}^{E}\!/_{F}$ be the set of all embeddings of E into $\operatorname{cl} F$, we get

$$|\operatorname{Emb} {}^{E}\!/_{F}| = [G : H] = [E : F].$$

Also notice that since automorphisms are also embeddings, $\operatorname{Aut} {}^{E}\!/_{F} \subseteq \operatorname{Emb} {}^{E}\!/_{F}$. Now, E is Galois over F if, and only if $\operatorname{ord} \operatorname{Aut} {}^{E}\!/_{F} = [E : F]$. Hence E is Galois over F if, and only if $\operatorname{Aut} {}^{E}\!/_{F} = \operatorname{Emb} {}^{E}\!/_{F}$; that is, each embedding of E is an automorphism of E which makes $\sigma E = E$.

Notice, now, that if $\sigma\alpha \in \sigma E$, then $(\sigma h s^{-1})(\sigma\alpha) = \sigma(h\alpha) = \sigma\alpha$, since $h\alpha = \alpha$ for all H in H. So $\sigma H \sigma^{-1}$ fixes σE. Moreover, we have $\operatorname{ord} \sigma H \sigma^{-1} = [K : \sigma E] = [K : E]$, so that $\operatorname{ord} \sigma H \sigma^{-1} = \operatorname{ord} H$. This makes $\sigma H \sigma^{-1}$ the group fixing σE.

Now, $\sigma E = E$ for all $\sigma \in G$ if, and only if $\sigma H s^{-1} = H$. That is, E is Galois over F if, and only if $H \trianglelefteq \operatorname{Gal} {}^{K}\!/_{F}$. Since the embedding of E over F are cosets of H in G, and $H \trianglelefteq G$, the correspondence gives that

$${}^{G}\!/_{H} \simeq \operatorname{Gal} {}^{E}\!/_{F}$$

Lastly, let $E_1, E_2 \subseteq K$ subfields contain ing F, and let $H_1, H_2 \leq G$ subgroups fixing E_1 and E_2. Then $H_1 \cap H_2$ fixes both E_1 and E_2, and so fixes E_1E_2. Conversely, if $h \in H_1$ such that h fixes E_2, then $h \in H_1 \cap H_2$. So that $H_1 \cap H_2$ corresponds to E_1E_2. By similar reasoning, we get that $\langle H_1, H_2 \rangle$ corresponds to $E_1 \cap E_2$. ■

Example 2.4. (1) The lattices of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ and $\mathbb{Q}(\sqrt[3]{2}, \xi)$ (where $\xi^3 = 1$) indicate all of the subfields of these fields. We have that the lattice of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is isomorphic to the lattice of the Klein 4-group V_4, which has all its subgroups normal. Thus we get every subfield of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is Galoix over $\mathbb{Q}$.

$$\begin{tikzcd}[column sep=small]
 & \mathbb{Q}(\sqrt{2},\sqrt{3}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{2}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{6}) \arrow[d, dash] & \mathbb{Q}(\sqrt{3}) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}
\qquad
\begin{tikzcd}[column sep=small]
 & \langle \sigma, \tau, \eta \rangle \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\langle \sigma \rangle \arrow[dr, dash] & \langle \tau \rangle \arrow[d, dash] & \langle \eta \rangle \arrow[dl, dash] \\
 & \langle \iota \rangle &
\end{tikzcd}$$

Figure 2.1: The lattice of subfields of $\mathbb{Q}(\sqrt{2, \sqrt{3}})$ and the lattice of subgroups of $\mathrm{Gal}\,{}^{\mathbb{Q}(\sqrt{2,\sqrt{3}})}\big/_{\mathbb{Q}}$.

On the other hand, the lattice for $\mathbb{Q}(\sqrt[3]{2}, \xi)$ is isomorphic to the lattice of S^3 where the only normal subgroup is the nontrivial subgroup of order 3; moreover, only $\mathbb{Q}(\xi)$ is Galois over $\mathbb{Q}$ with $\mathrm{Gal}\,{}^{\mathbb{Q}(\xi)}\big/_{\mathbb{Q}} \simeq {}^{S_3}\big/_{\langle\sigma\rangle}$, where $\langle \sigma \rangle$ is the cyclic subgroup of order 2.

(2) Consider $\mathbb{Q}(\sqrt{2} + \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$. If $m(x)$ is the minimal polynomial of $\sqrt{2} + \sqrt{3}$, then observe that is has as roots the distinct conjugates

$$\pm\sqrt{2} \pm \sqrt{3}$$

so that

$$m(x) = (x+(\sqrt{2}+\sqrt{3}))(x-(\sqrt{2}+\sqrt{3}))(x+(\sqrt{2}-\sqrt{3}))(x-(\sqrt{2}-\sqrt{3})) = x^4+10x+1$$

Moreover, $x^4 + 10x + 1$ is irreducible. Then only the automorphism ι of $\{\iota, \sigma, \tau, \sigma\tau\}$ fixes $\sqrt{2} + \sqrt{3}$ so that the fixing group of $\mathbb{Q}(\sqrt{2} + \sqrt{3})$ is preciesly that of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. So $\mathbb{Q}(\sqrt{} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

(3) Consider the splitting field of x^8+1 over $\mathbb{Q}$, generated by the elements $\sqrt[8]{2}$ and ξ, where $\xi^8 = 1$ (i.e. a primitive 8-th root of unity). Let $\zeta = \sqrt[8]{2}$, and notice that $\zeta^4 = \sqrt{2}$, and the splitting field of $x^8 - 2$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt[8]{2}, i)$ of degree $[\mathbb{Q}(\sqrt[8]{2}, i) : \mathbb{Q}] = 16 = 4^2$. Consider then all possible maps on ζ and i given by $\zeta \to \xi^a\zeta, i \to \pm i$. Define then the automorphisms

$$\sigma : \zeta \to \xi\zeta, i \to i \text{ and } \tau : \zeta \to \zeta, i \to -i$$

Since $\xi = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2} = \frac{1+i}{2}\zeta^4$, we compute that $\sigma : \xi \to \xi^5$, and $\tau : \xi \to \xi^7$. We can then compute the Galois group by noting that $\sigma^8 = \tau^2 = \iota$, and $\sigma\tau = \tau\sigma^3$, so that

$$\operatorname{Gal} {}^{\mathbb{Q}(\sqrt[8]{2}, i)}\!\diagup_{\mathbb{Q}} = \langle \sigma, \tau : \sigma^8 = \tau^2 = \iota \text{ and } \sigma\tau = \tau\sigma^3 \rangle$$

which describes the quasidihedral group of order 16.

Bibliography

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

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