

Frank Moore
Algebra 901 Notes
Professor: Tom Marley

Definition: Let R be a commutative ring with identity. Then R is a **field** provided every nonzero element of R is a unit.

Definition: R is a **domain** if whenever $ab = 0$, then $a = 0$ or $b = 0$.

Definition: If R is a domain then the **quotient field** or **field of fractions** of R is $Q(R) := \{\frac{a}{b} \mid a, b \in R, b \neq 0\}$. Note that $Q(R)$ is a field and is the smallest field containing R .

Definition: $R[x_1, \dots, x_n] :=$ the polynomial ring in n variables with coefficients from R . Note that we may think of $R[x_1, \dots, x_n]$ as $R[x_1, \dots, x_{n-1}][x_n]$.

Notation/Definition: Suppose $R \subseteq S$, where R, S are commutative rings with 1. Let $\alpha_1, \dots, \alpha_n \in S$. Then $R[\alpha_1, \dots, \alpha_n] := \bigcap T$ where $R \subset T \subset S$ and $\alpha_1, \dots, \alpha_n \in T$. In other words, it is the smallest ring containing R and $\alpha_1, \dots, \alpha_n$. Another way to describe it is as follows:

$$R[\alpha_1, \dots, \alpha_n] = \{p(\alpha_1, \dots, \alpha_n) \mid p(x_1, \dots, x_n) \in R[x_1, \dots, x_n]\}$$

Definition: Let $F \subset E$ be fields. We say that E/F is a field extension. Let $\alpha_1, \dots, \alpha_n \in E$. With the above notation, we note that $F[\alpha_1, \dots, \alpha_n]$ is the smallest ring containing F and the α_i and is in fact a domain. We also make the following definition:

$$F(\alpha_1, \dots, \alpha_n) := \bigcap L$$

where $F \subseteq L \subseteq E$ is a field and $\alpha_i \in L$ for all i . This is the quotient field of L and we may also describe $F(\alpha_1, \dots, \alpha_n)$ as follows:

$$F(\alpha_1, \dots, \alpha_n) := \left\{ \frac{p(\alpha_1, \dots, \alpha_n)}{q(\alpha_1, \dots, \alpha_n)} \mid p, q \in F[x_1, \dots, x_n], q(\alpha_1, \dots, \alpha_n) \neq 0 \right\}$$

Note that the above is the smallest field containing F and the α_i .

Definition: Let E/F be a field extension. Then E can be considered a vector space over F . The degree (E/F) is defined to be the dimension of E as an F -vector space. Notation: $[E : F] = \dim_F E$.

Lemma: Let E/F and F/L be field extensions. Then $[E : L] = [E : F][F : L]$.

Proof: Suppose $\{\alpha_1, \dots, \alpha_m\}$ is an F -basis for E and $\{\beta_1, \dots, \beta_l\}$ is an L -basis for F . Then $\{\alpha_i \beta_j\}$ where $1 \leq i \leq m$ and $1 \leq j \leq l$ is an L -basis for E .

Definition: Let E/F be a field extension and let $\alpha \in E$. Then α is **algebraic** over F if α is a root of a nonzero polynomial in $F[x]$. Otherwise, α is **transcendental** over F . In fact, we may choose the above polynomial to be monic by dividing by the leading coefficient.

Theorem: Let E/F be a field extension and $\alpha \in E$. Then TFAE:

1. α is algebraic over F .

2. $F[\alpha] = F(\alpha)$.
3. $[F(\alpha) : F]$ is finite.

Proof:

- 1) \Rightarrow 2): Note that $F[\alpha] = \text{span}_F\{1, \alpha, \alpha^2, \dots\}$. Consider the ring homomorphism: $\phi : F[x] \rightarrow F[\alpha]$ given by $f(x) \mapsto f(\alpha)$. Note by our remarks above, ϕ is surjective. As α is algebraic, we know that $\ker \phi \neq 0$. As $\ker \phi$ is an ideal, and $F[x]$ is a PID, we get that $\ker \phi = (h(x))$ for some $h \in F[x]$ where we may take h to be monic. Therefore, we have that $F[\alpha] \cong F[x]/(h(x))$. Note that $F[\alpha]$ has no zerodivisors as it is a subring of a field. Therefore, $F[x]/(h(x))$ has no ZD so that h is irreducible. Therefore, $(h(x))$ is a maximal ideal of $F[x]$ so $F[\alpha]$ is a field, hence $F[\alpha] = F(\alpha)$.
- 2) \Rightarrow 3): As $\frac{1}{\alpha} \in F(\alpha) = F[\alpha]$, $\frac{1}{\alpha} = c_0 + c_1\alpha + \dots + c_n\alpha^n$ for some n with $c_n \neq 0$. Therefore, we have that

$$c_n\alpha^{n+1} + c_{n-1}\alpha^n + \dots + c_1\alpha^2 + c_0\alpha - 1 = 0$$

and hence

$$\alpha^{n+1} = \left(-\frac{c_{n-1}}{c_n}\right)\alpha^n + \left(-\frac{c_{n-2}}{c_n}\right)\alpha^{n-1} + \dots + \frac{1}{c_n}$$

I claim that $F[\alpha] = \text{span}_F\{1, \dots, \alpha^n\}$. Indeed, it is enough to show that $\alpha^i \in \text{span}_F\{1, \alpha, \dots, \alpha^n\}$ for all i . We proceed by induction on i . If $i \leq n$ then the result follows. So, suppose we know that $\alpha_j \in \text{span}_F\{1, \alpha, \dots, \alpha^n\}$. Then α^{j+1} is just α times the expression for α^j in terms of our basis so using the above formula for α^{n+1} we get the desired result. Therefore, we have that $[F(\alpha) : F] = \dim_F F(\alpha) = \dim_F F[\alpha] \leq n + 1$ so that $[F(\alpha) : F] < \infty$ as desired.

- 3) \Rightarrow 1): Suppose that $[F(\alpha) : F] = n$. Consider $S = \{1, \alpha, \dots, \alpha^n\}$. Then S is linearly dependent over F . Then there exists c_0, \dots, c_n not all zero such that

$$c_0 + c_1\alpha + \dots + c_n\alpha^n = 0$$

Thus α is a root of $d(x) = c_0 + c_1x + \dots + c_nx^n$ which is nonzero because c_0, \dots, c_n were not all zero. So α is algebraic.

Definition: Let E/F be a field extension, $\alpha \in E$ algebraic over F . Consider the surjective ring homomorphism: $\phi : F[x] \rightarrow F[\alpha]$ defined $f(x) \mapsto f(\alpha)$. Let $\ker \phi = (h(x))$ where $h(x)$ is a monic irreducible polynomial in $F[x]$ such that $h(\alpha) = 0$. $h(x)$ is called the minimal polynomial of α over F , and is denoted $\text{Irr}(\alpha, F)$.

Remarks:

- h is uniquely defined, since if $(h_1) = (h_2)$ then $h_1 \mid h_2$ and $h_2 \mid h_1$ so $h_1 = h_2$ since they are monic.
- $F[\alpha] \cong F[x]/(h(x))$
- h is a nonzero polynomial of smallest degree of which α is a root.

Theorem: Let α be algebraic over F . Then $[F(\alpha) : F] = \deg \text{Irr}(\alpha, F)$.

Proof: Let $h(x) = x^n + c_{n-1}x^{n-1} + \dots + c_0 = \text{Irr}(\alpha, F)$. I claim that $\{1, \alpha, \dots, \alpha^{n-1}\}$ is an F -basis for $F(\alpha)$. Indeed, let us show linear independence first. Suppose that $d_0 \cdot 1 + d_1\alpha + \dots + d_{n-1}\alpha^{n-1} = 0$. Then α is a root of $g(x) = d_0 + d_1x + \dots + d_{n-1}x^{n-1} \in F[x]$. But $\deg g(x) < \deg(h(x))$, hence $g(x) = 0$. So $d_0 = d_1 = \dots = d_{n-1} = 0$. To show spanning, note that as α is algebraic, $F(\alpha) = F[\alpha]$. So, it is enough to show that $\alpha^i \in \text{span}_F\{1, \alpha, \dots, \alpha^{n-1}\}$. Induct on i with the cases $i \leq n-1$ being obvious. So, supposing that $\alpha^i \in \text{span}\{1, \alpha, \dots, \alpha_n\}$ and writing down the expression for α^i then multiplying by α^{j+1} give you the result.

Definition: Let E/F be a field extension. E/F is **finite** if $[E : F] < \infty$ and E/F is **finitely generated** if E is finitely generated as a field over F (i.e. $E = F(\alpha_1, \dots, \alpha_n)$). E/F is **algebraic** provided α is algebraic over F for all $\alpha \in E$.

Theorem: Let E/F be a field extension. Then E/F is finite $\Leftrightarrow E/F$ is finitely generated and algebraic.

Proof: " \Rightarrow ": Let $\alpha_1, \dots, \alpha_n$ be an F -basis for E . Then $E = F\alpha_1 + F\alpha_2 + \dots + F\alpha_n \subseteq F(\alpha_1, \dots, \alpha_n) \subset E$. Therefore, $E = F(\alpha_1, \dots, \alpha_n)$, hence we have that E/F is finitely generated. To show that E/F is algebraic, let $\alpha \in E$. Then $F \subseteq F(\alpha) \subseteq E$. So we have that $[E : F] = [E : F(\alpha)][F(\alpha) : F]$ where $[E : F]$ is finite. Therefore $[F(\alpha) : F] < \infty$, therefore by a previous theorem, α is algebraic over F .

" \Leftarrow ": Let $E = F(\alpha_1, \dots, \alpha_n)$, and in general, set $L_i = F(\alpha_1, \dots, \alpha_i)$. Then we have a tower of fields and we can use the fact about multiplicativity of field extensions to get that $[E : F] < \infty$.

Corollary: Suppose that $\alpha_1, \dots, \alpha_n$ are algebraic over F and let $p(x_1, \dots, x_n) \in F[x_1, \dots, x_n]$. Then $p(\alpha_1, \dots, \alpha_n)$ and $\frac{1}{p(\alpha_1, \dots, \alpha_n)}$ are algebraic, since both are in $F(\alpha_1, \dots, \alpha_n)$.

Theorem (recall from 817-818): Eisenstein's Criterion for Irreducibility: Let $f(x) = a_nx^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$ be a polynomial in $\mathbb{Z}[x]$. Suppose that there exists a prime p such that $p \mid a^i$ for $i \leq n-1$, $p \nmid a_n$, $p^2 \nmid a_0$. Then $f(x)$ is irreducible over \mathbb{Q} .

Gauss's Lemma: Let $f(x) \in \mathbb{Z}[x]$. Suppose that $f(x) = h(x)g(x)$ where $h(x), g(x) \in \mathbb{Q}[x]$, where $\deg h > 0$ and $\deg g > 0$. Then $\exists h_1(x), g_1(x) \in \mathbb{Z}[x]$ such that $f(x) = h_1(x)g_1(x)$, $h_1 = \alpha h$ and $g_1 = \beta g$ for some $\alpha, \beta \in \mathbb{Q}$.

Corollary: Let E/F be a field extension. Set $L := \{\alpha \in E \mid \alpha \text{ is algebraic over } F\}$. Then L is a field by our previous work. L is often called the algebraic closure of F in E .

Example: $\bar{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \alpha \text{ is algebraic over } \mathbb{Q}\}$. Show that $\bar{\mathbb{Q}}$ is algebraic but not finite. Indeed, suppose that $[\bar{\mathbb{Q}} : \mathbb{Q}] = n$ and consider $\sqrt[n+1]{2}$. We know that $\text{Irr}(\sqrt[n+1]{2}, \mathbb{Q}) = x^{n+1} - 2$ since that polynomial is irreducible over \mathbb{Q} by Eisenstein. So the degree of the field extension is $n+1$ which we know has to divide n , a contradiction.

Proposition: Let $f(x) \in F[x]$ with degree f 2 or 3. Then $f(x)$ is reducible $\Leftrightarrow f(x)$ has a root in $F[x]$.

The Mod p technique: Let $f \in \mathbb{Z}[x]$, and suppose \exists a prime p such that p doesn't divide the leading coefficient of f and $f(x) \in \mathbb{Z}_p[x]$ is irreducible. Then f is irreducible in \mathbb{Q} .

Example: Let $f(x) = 3x^4 - 7x^3 + 6x^2 + 10x - 9 \in \mathbb{Q}[x]$. Show that $f(x)$ is irreducible. Let $\bar{f}(x)$ be the image of f in $\mathbb{Z}_2[x]$. Then $\text{bar}f(x) = x^4 + x^3 + 1$. \bar{f} has no roots in \mathbb{Z}_2 so it has no linear factors. The only irreducible quadratic in \mathbb{Z}_2 is $x^2 + x + 1$ and it does not divide \bar{f} . Therefore \bar{f} is irreducible in $\mathbb{Z}_2[x]$ and hence f is irreducible in $\mathbb{Q}[x]$.

Theorem: Let E/F and F/L be field extensions. Then E/L is algebraic if and only if E/F and F/L are algebraic.

Proof: For the forward direction, let $\alpha \in E$. Then α satisfies a polynomial over L , and hence over F . Similarly for $\alpha \in F$. Consider the reverse direction now. So, let $\alpha \in E$. Then there exists a monic polynomial $f(x) \in F[x]$ such that $f(\alpha) = 0$. Write $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1x + c_0$ where the $c_i \in F$. Let $K = L(c_{n-1}, \dots, c_0)$. Then K is a finite algebraic extension of L . Also, $f(x) \in K[x]$. Since $f(\alpha) = 0$, we see that α is algebraic over K . Therefore $[K(\alpha) : K] < \infty$. Therefore, we have that $[K(\alpha) : L] = [K(\alpha) : K][K : L] < \infty$. As $K(\alpha)/L$ is finite, it is algebraic, hence α is algebraic over L . Therefore, E/L is algebraic.

Definition: Let F be a field and $f \in F[x] \in F[x] \setminus F$. A field $L \supset F$ is called a splitting field for $f(x)$ over F if $f(x)$ factors into linear polynomials over $L[x]$, but not in any proper subfield of L containing F . We say that $f(x)$ “splits completely” in $L[x]$.

Remarks:

1. If $f(x) \in F[x]$ splits completely in a field E containing F , then a splitting field for $f(x)$ is F adjoin the roots of $f(x)$ in E . For example, if $f(x) = c(x - \alpha_1) \cdots (x - \alpha_n)$ in $E[x]$ then a splitting field for F is $F(\alpha_1, \dots, \alpha_n)$.
2. If $\deg f = n$ and L is a splitting field for f then $[L : F] \leq n!$.

Proof: Let $f(x) = c(x - \alpha_1) \cdots (x - \alpha_n)$, so that $L = F(\alpha_1, \dots, \alpha_n)$. We proceed by induction on n . If $n = 1$ then F is already the splitting field for f . If $n > 1$, let $\alpha \in L$ be a root of $f(x)$. Then, in $L[x]$, $f(x) = (x - \alpha)g(x)$. We first prove a claim:

Claim: Let E/F be a field extension, and let $g, h \in F[x]$. If $g \mid h$ in $E[x]$ then $g \mid h$ in $F[x]$.

Proof: Set $h = gq$ where $q \in E[x]$. Then use the division algorithm in $F[x]$ to get $h = gq_1 + r$ where $q_1, r \in F[x]$ and $\deg r < \deg g$. But this same equation holds in $E[x]$, so by the uniqueness of the division algorithm, we have that $q = q_1$ and hence $q \in F[x]$.

So, by the claim we have that $f(x) = (x - \alpha)g(x)$ in $F(\alpha)[x]$. Now $\deg g = n - 1$. Now we know that $[F(\alpha) : F] \leq n$ as α is a root of $f(x)$ and $\deg f = n$. Also, L is the splitting field of $g(x)$ over $F(\alpha)[x]$. By induction, we have that $[L : F(\alpha)] \leq n - 1!$, so that $[L : F] \leq n!$.

Examples:

1. Find the splitting field for $x^2 - 5$ over \mathbb{Q} . This is clearly $\mathbb{Q}(\sqrt{5})$.
2. Find the splitting field for $x^2 - 5$ over $\mathbb{Q}(\sqrt[3]{5})$. Set $L = \mathbb{Q}(\sqrt[3]{5})(\sqrt{5}) = \mathbb{Q}(\sqrt[3]{5}, \sqrt{5})$, and set $F = \mathbb{Q}(\sqrt[3]{5})$. We wish to find out $[L : F] = [F(\sqrt{5}) : F] = \text{degree of minimal polynomial} = \deg \text{Irr}(\sqrt{5}, \mathbb{Q}(\sqrt[3]{5}))$. Certainly if $f(x) = x^2 - 5 \in F[x]$ and $f(\sqrt{5}) = 0$. Therefore we have that $\text{Irr}(\sqrt{5}, \mathbb{Q}(\sqrt[3]{5})) \mid f(x)$. So, $\text{Irr}(\sqrt{5}, \mathbb{Q}(\sqrt[3]{5}))$ is either $x^2 - 5$ or $x - \sqrt{5}$. So the question now becomes is $\sqrt{5} \in \mathbb{Q}(\sqrt[3]{5})$? Note that $[\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 2$ as $x^2 - 5$ is irreducible over \mathbb{Q} by Eisenstein and similarly, we have that $[\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}] = 3$. Therefore, if $\sqrt{5} \in \mathbb{Q}(\sqrt[3]{5})$, we would have that $[\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] \mid [\mathbb{Q}(\sqrt[3]{5}, \mathbb{Q}) : \mathbb{Q}]$ and thus $2 \mid 3$, a contradiction. Therefore, we have that $[L : \mathbb{Q}(\sqrt[3]{5})] = 2$.
3. Let $f(x) = x^n - 1 \in \mathbb{Q}[x]$. The roots of $f(x)$ are called the n th roots of unity : $e^{2\pi ik/n}$ for $0 \leq k \leq n - 1$. The splitting field for $f(x)$ over \mathbb{Q} is $L = \mathbb{Q}(\{e^{2\pi ik/n} \mid 0 \leq k \leq n - 1\}) = \mathbb{Q}(e^{2\pi i/n})$.

Note also that $U_n = \{e^{2\pi ik/n} \mid k \in \{0, 1, \dots, n-1\}\}$ is a cyclic multiplicative group of order n . Any cyclic generator of U_n is called a primitive n th root of unity. I.e. $e^{2\pi ik/n}$ is primitive if and only if $(k, n) = 1$. So $L = \mathbb{Q}(\omega)$ where ω is a primitive n th root of unity. What is $[\mathbb{Q}(\omega) : \mathbb{Q}]$? We will see later that this is precisely $\phi(n)$.

Proposition: Let p be a prime and ω be a primitive p th root of unity over \mathbb{Q} . Then the irreducible polynomial of ω is as follows:

$$\text{Irr}(\omega, \mathbb{Q}) = x^{p-1} + x^{p-2} + \dots + x + 1$$

and therefore, we have that $[\mathbb{Q}(\omega) : \mathbb{Q}] = p - 1$.

Proof: ω is a root of $x^p - 1 = (x - 1)(x^{p-1} + x^{p-2} + \dots + x + 1)$ (let the second factor be $f(x)$). Hence ω is a root of $f(x)$. It is enough to show that $f(x)$ is irreducible over \mathbb{Q} . First we mention an important remark:

Remark: Let $f(x)$ be a polynomial in $F[x]$ where F is a field and let $a \in F$. Then $f(x)$ is irreducible over F if and only if $f(x + a)$ is irreducible over F .

So, consider $x^p - 1 = (x - 1)f(x)$. Then $(x + 1)^p - 1 = xf(x + 1)$. Expanding gives

$$x^p + \binom{p}{1}x^{p-1} + \dots + \binom{p}{i}x^i + \dots + \binom{p}{p-1}x = xf(x + 1)$$

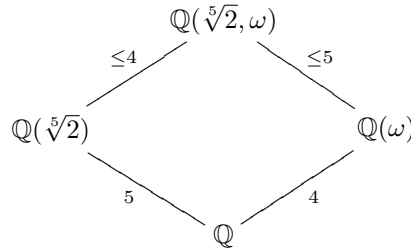
Cancelling x gives

$$x^{p-1} + \binom{p}{1}x^{p-2} + \dots + \binom{p}{i}x^{i-1} + \dots + \binom{p}{p-1} = f(x + 1)$$

Now by Eisenstein (take $p = p$) we have that $f(x + 1)$ is irreducible over \mathbb{Q} . Hence by the remark $f(x)$ is irreducible over \mathbb{Q} .

Example: Find the splitting field and its degree of $x^5 - 2$ over \mathbb{Q} .

Solution: The roots of $x^5 - 2$ are $\omega^i \sqrt[5]{2}$ for $i = 0, 1, 2, 3, 4$ and where ω is a primitive 5th root of unity. Let L be the splitting field of $x^5 - 2$ over \mathbb{Q} . Then $L = \mathbb{Q}(\sqrt[5]{2}, \omega^{\sqrt[5]{2}}, \dots, \omega^4 \sqrt[5]{2}) = \mathbb{Q}(\sqrt[5]{2}, \omega)$. We have the following tower of fields:



Where the numbers on the extensions denote either the degree or a bound on the degree. We know the bottom two degrees are what they are by a previous proposition or by Eisenstein. The others are bounded by that because we have a polynomial that is satisfied by the element we are adjoining. (I am not certain why the extensions also have to be at least that amount, perhaps the same trick from above applies as $4 \nmid 5$ and $5 \nmid 4$.) So the degree of $[\mathbb{Q}(\sqrt[5]{2}, \omega) : \mathbb{Q}] = 20$.

Example: Find the splitting field and its degree of $x^6 + 3$ over \mathbb{Q} .

Solution: Let $z = re^{i\theta}$ be a root of $x^6 + 3$. Then $r^6 e^{6i\theta} = -3 = 3e^{i\pi}$. So $r = \sqrt[6]{3}$ and $6\theta = \pi + 2\pi k$ or $\theta = \frac{\pi}{6} + \frac{\pi}{3}k$. Therefore, we have that

$$\begin{aligned} z &= \sqrt[6]{3}e^{i(\frac{\pi}{6} + \frac{\pi}{3}k)} \\ &= \sqrt[6]{3}e^{i\frac{\pi}{6}} \cdot (e^{i\frac{\pi}{3}})^k \end{aligned}$$

Hence, $L = \mathbb{Q}(\sqrt[6]{3}e^{i\pi/6}, e^{i\pi/3})$. Thus, we have the following tower of fields:

$$\begin{array}{ccc} & \mathbb{Q}(\sqrt[6]{3}e^{i\pi/6}, e^{i\pi/3}) & \\ \leq 2 \swarrow & & \searrow \leq 6 \\ \mathbb{Q}(\sqrt[6]{3}e^{i\pi/6}) & & \mathbb{Q}(e^{i\pi/3}) \\ \searrow 6 & & \swarrow 2 \\ & \mathbb{Q} & \end{array}$$

Where we know that $[\mathbb{Q}(\sqrt[6]{3}e^{i\pi/6}) : \mathbb{Q}] = 6$ since $x^6 + 3$ is irreducible by Eisenstein. Also, note that $e^{i\pi/3} = e^{i\pi} = -1$, so that it is a root of $x^3 + 1 = (x+1)(x^2 - x + 1)$. Therefore, $e^{i\pi/3}$ is a root of $x^2 - x + 1$ which is irreducible over \mathbb{Q} . Hence the question becomes is $e^{i\pi/3}$ in $\mathbb{Q}(\sqrt[6]{3}e^{i\pi/6})$. First, note that

$$e^{i\pi/3} = \cos(\pi/3) + i \sin(\pi/3) = \frac{1}{2} + i \frac{\sqrt{3}}{2}$$

but, $(\sqrt[6]{3}e^{i\pi/6})^3 = \sqrt{3}e^{i\pi/2} = i\sqrt{3} \in \mathbb{Q}(\sqrt[6]{3}e^{i\pi/6})$. Therefore we see that $e^{i\pi/3} \in \mathbb{Q}(\sqrt[6]{3}e^{i\pi/6})$, hence $L = \mathbb{Q}(\sqrt[6]{3}e^{i\pi/6})$, so that $[L : \mathbb{Q}] = 6$.

Theorem: Let F be a field and $f(x) \in F[x]$ be a non-constant polynomial. Then there exists a splitting field for $f(x)$ over F .

Proof: Induction on n , the degree of f . Let $g(x)$ be an irreducible factor of $f(x)$. So $g(t)$ is irreducible in $F[t]$. Therefore, $F[t]/(g(t))$ is a field, as $(g(t))$ is a maximal ideal in $F[t]$. Consider the field homomorphism $\phi : F \rightarrow F[t] \rightarrow F[t]/(g(t))$. Since $\phi(a) \neq \bar{0}$ in $F[t]/(g(t))$ for all $a \neq 0$, it is clear that ϕ is injective. Let $L = F[t]/(g(t)) = \{h(t) + (g(t)) \mid h \in F[t]\}$. Then $\phi : F \rightarrow L$ sends a to $a + (g(t)) = \bar{a}$. Since $F \cong \phi(F)$, we can identify F with its image in L , and assume that $F \subset L$. Let $\alpha = t + (g(t)) = \bar{t}$. Then

$$\begin{aligned} L &= \{a_0 + a_1t + \cdots + a_nt^n + (g(t)) \mid a_i \in F\} \\ &= \{(a_0 + (g)) + (a_1 + (g))(t + (g)) + \cdots + (a_n + (g))(t + (g))^n \mid a_i \in F\} \\ &= \{a_0 + a_1\alpha + \cdots + a_n\alpha^n \mid a_i \in F\} \end{aligned}$$

Note that $g(\alpha) = g(\bar{t}) = \bar{g(t)} = \bar{0}$, since $g(t) \in (g(t))$. Therefore, α is a root of $g(x)$. So $g(x)$ has a root in L , so $f(x)$ has a root also. Therefore, $f(x) = (x - \alpha)h(x)$ for some $h(x) \in L[x]$. Note that $\deg h(x) = n - 1$. By induction, $h(x) \in L[x]$ has a splitting field E containing L . Therefore $f(x)$ splits completely in E . So, let $\alpha_1, \dots, \alpha_n$ be the roots of $f(x)$ in E . Then $F(\alpha_1, \dots, \alpha_n)$ is a splitting field for $f(x)$ over F .

Example: Find a splitting field and its degree of $f(x) = x^3 + x + 1$ in $\mathbb{Z}_2[x]$.

Solution: As $\deg f = 3$ and has no roots in \mathbb{Z}_2 , it is irreducible in $\mathbb{Z}_2[x]$. We let $L = \mathbb{Z}_2[t]/(t^3 + t + 1) = \mathbb{Z}_2(\alpha)$ where $\alpha = t + (t^3 + t + 1)$, i.e. $\alpha^3 + \alpha + 1 = 0$. In L , $x^3 + x + 1 = (x - \alpha)h(x)$ for some $h(x) \in L[x]$ with $\deg h = 2$. Does h factor in L or is it irreducible? Lets try and find h . Using long division and the relation $\alpha^3 + \alpha + 1 = 0$, you get that $h(x) = x^2 + \alpha x + (1 + \alpha^2)$. Also, note that $h(\alpha^2) = 0$ so that h splits in L . Therefore L is the splitting field for $x^3 + x + 1$ and $[L : \mathbb{Z}_2] = 3$.

Definition: Let E/F and E'/F' be field extensions. Suppose that $\sigma : F \rightarrow F'$ is an injective field hom. Then a field map $\tau : E \rightarrow E'$ is said **to extend** σ if $\tau|_F = \sigma$. For the following important special case, take $F = F'$ and $\sigma = \text{Id}_F$. Then τ extends Id_F if and only if τ fixes F (i.e. $\tau(a) = a$ for all $a \in F$).

Remark: Suppose $\sigma : F \rightarrow F'$ is a field isomorphism. Define

$$\begin{aligned}\tilde{\sigma} : F[x] &\rightarrow F'[x] \\ a_0 + a_1x + \cdots + a_nx^n &\mapsto \sigma(a_0) + \sigma(a_1)x + \cdots + \sigma(a_n)x^n \\ f(x) &\mapsto f^\sigma(x)\end{aligned}$$

Then $\tilde{\sigma}$ is a ring isomorphism, which is clear since σ is a field isomorphism.

Let $f(x) \in F[x]$. Then f is irreducible in $F[x] \Leftrightarrow f^\sigma$ is irreducible in $F'[x]$. Also, $\tilde{\sigma}((f(x))) = (f^\sigma(x))$. Therefore, we have that

$$\begin{aligned}\bar{\sigma} : F[x]/(f(x)) &\rightarrow F'[x]/(f^\sigma(x)) \\ g(x) + (f(x)) &\mapsto g^\sigma + (f^\sigma(x))\end{aligned}$$

is a field isomorphism and furthermore, $\bar{\sigma}$ extends σ , as is clear by the definition of $\bar{\sigma}$.

Theorem: Let $\sigma : F \rightarrow F'$ be a field isomorphism, and let $f(x) \in F[x]$ be a nonconstant polynomial. Let E and E' be splitting fields for f and f^σ . Then there exists a $\tau : E \rightarrow E'$ which is an isomorphism of fields extending σ .

Proof: Let $n = \deg f$. If $n = 1$ then $E = F$ and $E' = F'$ so let $\tau = \sigma$. Suppose that $n > 1$. If $f(x)$ splits in F , then as above, $\tau = \sigma$. Let $p(x)$ be a monic nonlinear irreducible factor of $f(x)$. Then p^σ is a monic nonlinear irreducible factor of $f^\sigma(x)$. So, as f splits in E , p splits in E , so let α be a root of $p(x)$ in E and let $\beta \in E'$ be a root of $p^\sigma(x)$. Therefore, we have that $p(x) = \text{Irr}(\alpha, F)$ and $p^\sigma(x) = \text{Irr}(\beta, F')$. So, $F(\alpha) \cong F[x]/(p(x))$ and $F'(\beta) \cong F'[x]/(p^\sigma(x))$.

$$\begin{aligned}\phi : F[x]/(p(x)) &\rightarrow F'[x]/(p^\sigma(x)) \\ g + (p) &\mapsto g^\sigma + (p^\sigma)\end{aligned}$$

be the field isomorphism of the remark. Let π be the composition of the following maps (π is an isomorphism as each piece is):

$$F(\alpha) \rightarrow F[x]/(p(x)) \rightarrow F'[x]/(p^\sigma(x)) \rightarrow F'(\beta)$$

Then for $a \in F$, we have

$$a \mapsto a + (p) \mapsto \sigma(a) + (p^\sigma) \mapsto \sigma(a)$$

so that π extends σ . Now we have an isomorphism $\pi : F(\alpha) \rightarrow F'(\beta)$ which extends σ . Now we have the following diagram:

$$\begin{array}{ccc}
E & \xrightarrow{\tau} & E' \\
| & & | \\
F(\alpha) & \xrightarrow{\pi} & F'(\beta) \\
| & & | \\
F & \xrightarrow{\sigma} & F'
\end{array}$$

Write $f(x) = (x - \alpha)h(x)$, $h(x) \in F(\alpha)[x]$. Note that $\deg h = n - 1$. Notice that E is the splitting field for $h(x)$ over $F(\alpha)$ so by induction, we have that there exists a $\tau : E \rightarrow E'$ extending π , and hence extending σ also.

Corollary: Let E, E' be splitting fields for $f(x)$ in $F[x]$. Then there exists an isomorphism $\tau : E \rightarrow E'$ fixing F . For the proof, take $\sigma = \text{Id}_F$ and extend it to $\tau : E \rightarrow E'$.

Definition: Let S be a set. A relation \leq is called a partial order if for all $r, s, t \in S$ we have

1. $r \leq r$ (reflexive)
2. $r \leq s$ and $s \leq t$ implies that $r \leq t$ (transitive)
3. $r \leq s$ and $s \leq r$ implies that $r = s$ (antisymmetric)

We say that \leq is a total order on S if it is a partial order and for all $s, t \in S$ we have that $s \leq t$ or $t \leq s$. For example, \leq in the usual sense is a total ordering on \mathbb{R} . As another example, let S be a nonempty set and $\mathcal{P}(S)$ be the powerset of S . Then inclusion is a partial order on $\mathcal{P}(S)$.

Definition: Let S be a poset and let $A \subset S$. Then an element $b \in S$ is said to be an upper bound for A if $a \leq b$ for all $a \in A$. An element $m \in S$ is called **maximal** if whenever $m \leq s$ for $s \in S$, we have that $m = s$.

Zorn's Lemma: Let $S \neq \emptyset$ be a poset and suppose every totally ordered subset of S has an upper bound in S . Then S has a maximal element. Note that this statement is equivalent to the axiom of choice. As an example of how to use this lemma, consider the following:

Proposition: Let V be a vector space over a field F and let S be a linearly independent subset of V . Then there exists a basis β of V containing S .

Proof: Let $\Lambda = \{T \mid S \subseteq T \subseteq V \text{ and } T \text{ is linearly independent}\}$. Note that $\Lambda \neq \emptyset$ since $S \in \Lambda$, and Λ is a poset when ordered by inclusion. Let C be a totally ordered subset of Λ , and let $T_0 = \bigcup_{T \in C} T$. Clearly $T \subset T_0$ for all $T \in C$, so we claim that $T_0 \in \Lambda$, i.e. T_0 is linearly independent. Suppose that $c_1v_1 + \dots + c_nv_n = 0$ where $v_1, \dots, v_n \in T_0$ and then c_i come from F . As C is totally ordered, there exist a T_n such that all the v_i are in T_n . So, since T_n is linearly independent, we have that $c_i = 0$ for all i . Therefore $T_0 \in \Lambda$. Thus by Zorn's Lemma, Λ has a maximal element, say β . Since $\beta \in \Lambda$, β is linearly independent, and $S \subset \beta$. Now we must show that β spans V . If not, choose $v \in V \setminus \text{span}_F \beta$. Then $\beta \cup \{v\}$ is linearly independent and containing S , contradicting the maximality of β . Hence β spans and is therefore a basis of V .

Corollary: Every vector space has a basis. To prove this, apply the above proposition to $S = \emptyset$.

Proposition: Let R be a commutative ring with identity. Assume that $1 \neq 0$. Let I be an ideal of R , with $I \neq R$. Then there exists a maximal ideal of R containing I .

Proof: Let $\Lambda = \{J \mid I \subseteq J \subset R \text{ where } J \text{ is a proper ideal of } R\}$. Note that $\Lambda \neq \emptyset$ as $I \in \Lambda$. Let C be a totally ordered subset of Λ . Now, let $J_0 = \bigcup_{J \in C} J$. Note that J_0 is not usually an ideal but it is if and only if we have an increasing chain of ideals, which is the case here. So, J_0 is an ideal containing I . If $J_0 = R$, then $1 \in J_0$, thus $1 \in J$ for some $J \in C$, and thus $J = R$, a contradiction. Therefore $J_0 \in \Lambda$ and is an upper bound for C . Thus, by Zorn's Lemma, Λ has a maximal element, say \mathfrak{m} . So \mathfrak{m} is a maximal ideal of R containing I .

Corollary: Every commutative ring with identity has a maximal ideal (by applying the above to (0)).

Theorem/Definition: Let F be a field. Then TFAE:

1. If E/F is an algebraic field extension, then $E = F$.
2. Every nonconstant polynomial in F splits completely in $F[x]$.
3. Every nonconstant polynomial in $F[x]$ has a root in F .

If F satisfies any of the three equivalent definitions above, then F is said to be **algebraically closed**.

Proof: (1) \Rightarrow (2): Let $f(x) \in F[x]$ and let E be the splitting field of $f(x)$ over F . Then E/F is algebraic, so by (1), $E = F$ hence $f(x)$ splits completely in $F[x]$.

(2) \Rightarrow (3) is trivial.

(3) \Rightarrow (1) Let E/F be an algebraic field extension. Let $\alpha \in E$. Let $f(x) = \text{Irr}(\alpha, F)$. By (3), $f(x)$ has a root in F , so $\deg f = 1$ and therefore $f(x) = x - \alpha$. Therefore, $\alpha \in F$ and so $E = F$.

Definition: Let F be a field. A field E containing F is an algebraic closure of F if E/F is algebraic and E is algebraically closed.

Proposition: Suppose L/F is a field extension and L is algebraically closed. Let $E = \{\alpha \in L \mid \alpha \text{ is algebraic over } F\}$. Then E is an algebraic closure of F in L .

Proof: We have show that E is a field and that E/F is algebraic. It is hence enough to show that E is algebraically closed. Suppose $f(x)$ in $E[x]$ is a nonconstant polynomial. Then $f(x) \in L[x]$, so $f(x)$ has a root $\alpha \in L$. Therefore α is algebraic over E , as $f(\alpha) = 0$. So, $E(\alpha)/E$ is an algebraic extension, but E/F is algebraic, so that $E(\alpha)/F$ is algebraic. Thus α is algebraic over F , so $\alpha \in E$, by definition of E . So E is algebraically closed since we proved condition (3) of the above definition.

Lemma: Let K be a field. Then \exists a field L containing K such that every nonconstant polynomial in $K[x]$ has a root in L .

Proof: For each nonconstant polynomial $f(x) \in K[x]$ let x_f be a new variable. Let $R = K[\{x_f \mid f \in K[x] \setminus K\}]$. Let I be the ideal generated by $\{f(x_f)\}$.

Claim: $I \neq R$. If $I = R$, then $1 \in I$ which means $1 = \sum_{i=1}^n r_i f_i(x_{f_i})$ for some $r_i \in R$. So, the r_i 's involve only finitely many of the variables. Let $x_i = x_{f_i}$, and let x_{n+1}, \dots, x_m be all the other variables appearing in the r_i . Therefore, we have that

$$1 = \sum_{i=1}^n r_i(x_1, \dots, x_m) f_i(x_i).$$

Now, let F be a splitting field for $f_1(x)f_2(x)\cdots f_n(x)$ over K , i.e. in F , every $f_i(x)$ has a root α_i . Certainly the above equation still holds in $F[\{x_f\}]$. Now, let $x_i = \alpha_i$ for $i = 1, \dots, n$. ; Then the above equation after substituting reads $1 = 0$, a contradiction. So, I is a proper ideal. Then by the previous proposition, there exists a maximal ideal \mathfrak{m} of R that contains I . Let $L = R/\mathfrak{m}$, which is a field. Note that the composition of maps, call it δ , below:

$$K \hookrightarrow K[\{x_f\}] \rightarrow K[\{x_f\}]/\mathfrak{m}$$

is 1-1 as \mathfrak{m} has no units. So, we identify K with $\delta(K)$ in L and consider $K \subset L$. Let $f(x) \in K[x] \setminus K$. Let $\alpha_f = x_f + \mathfrak{m}$. Then $f(\alpha_f) = f(x_f + \mathfrak{m}) = f(x_f) + \mathfrak{m}$. But $f(x_f) \in I \subseteq \mathfrak{m}$ so $f(\alpha_f) = \bar{0}$, as desired.

Theorem: Let F be a field. Then there exists an algebraic closure of F .

Proof: We can construct by the previous lemma a chain of fields:

$$F = L_0 \subseteq L_1 \subseteq L_2 \subseteq \cdots$$

where every nonconstant polynomial in $L_n[x]$ has a root in L_{n+1} . Let $L = \bigcup_{n \geq 0} L_n$. Note that L is a field. I claim that L is algebraically closed. Indeed, let $f(x) \in L[x] \setminus L$. Then there exists an n such that $f(x) \in L_n[x]$. Then f has a root in L_{n+1} with is also in L . So, by the theorem, $\{\alpha \in L \mid \alpha \text{ is algebraic over } F\}$ is an algebraic closure of F and this completes the proof.

Theorem: Let E/F be an algebraic extension and L/K an extension in which L is an algebraic closure of K . Let $\sigma : F \rightarrow K$ be a nonzero field homomorphism. Then there exists a field map $\tau : E \rightarrow L$ that extends σ .

Proof: We will use Zorn's Lemma. Let $\Lambda = \{(T, \phi) \mid F \subset T \subset E \text{ and } \phi : T \rightarrow L \text{ extends } \sigma\}$. Partially order Λ as follows: $(T_1, \phi_1) \leq (T_2, \phi_2) \Leftrightarrow T_1 \subset T_2$ and $\phi_2|_{T_1} = \phi_1$. First, note that $\Lambda \neq \emptyset$ as $(F, \sigma) \in \Lambda$. Let C be a totally ordered subset of Λ . Let $T_0 = \bigcup_{(T, \phi) \in C} T$ and define $\psi : T_0 \rightarrow L$ as follows. Let $t \in T_0$. Then $t \in (T_1, \phi_1) \in C$. Define $\psi(t) = \phi_1(t)$. By the extension part of the condition of being in Λ this is well-defined. It is easy to check that ψ is a field homomorphism.

Then $(T_0, \psi) \in \Lambda$ and is an upper bound for C . By Zorn's Lemma, Λ has a maximal element, call it (M, δ) . It is enough to show that $M = E$. Suppose that $M \subsetneq E$. Let $N = \delta(M)$. Then $\delta : M \rightarrow N$ is a field isomorphism. So, let $\alpha \in E \setminus M$. Then α is algebraic over M as E is algebraic over F . Let $f(x) = \text{Irr}(\alpha, M)$. Then $M(\alpha) \cong M[x]/(f(x)) \cong N[x]/(f^\delta(x))$. But $f^\delta(x) \in N[x] \subset L[x]$ has a root $\beta \in L$ as L is algebraically closed. So, $N[x]/(f^\delta(x)) \cong N(\beta)$, since $f^\delta(x)$ is irreducible over N . Nut $N(\beta) \subset L$. Let $\delta' : M(\alpha) \hookrightarrow L$ be the composition of the maps above. By construction, $\delta'|_M = \delta$. Hence, $(M(\alpha), \delta') \supsetneq (M, \delta)$, a contradiction. Therefore, $M = E$.

Corollary: Let F be a field and E_1, E_2 two algebraic closures of F . Then there exists an isomorphism $\tau : E_1 \rightarrow E_2$ such that τ fixes F .

Proof: Let $\sigma : F \rightarrow F$ be the identity map. Then there exists $\tau : E_1 \rightarrow E_2$ such that $\tau|_F = \text{Id}_F$. As E_1 is algebraically closed, so is $\tau(E_1)$. But $E_2/\tau(E_1)$ is algebraic, so $E_2 = \tau(E_1)$, so the map is surjective, hence an isomorphism.

Definition: Let F be a field and S a set of polynomials in $F[x]$. The splitting field L for S over F is the smallest subfield of \bar{F} (the algebraic closure of F), such that every polynomial in S splits completely in this field. I.e. $L = F(\text{all roots in } \bar{F} \text{ of all polynomials in } S)$.

Remark: Let E/F and L/F be field extensions and $\sigma : E \rightarrow L$ a field map that fixes F . Suppose that $p(x) \in F[x]$ has a root $\alpha \in E$. Then $\sigma(\alpha)$ is also a root of $p(x)$.

Proof: Let $p(x) = c_n x^n + \cdots + c_1 x + c_0 \in F[x]$. So, we know that $0 = c_n \alpha^n + \cdots + c_1 \alpha + c_0$. Applying σ to both sides gives $0 = c_n \sigma(\alpha)^n + \cdots + c_1 \sigma(\alpha) + c_0$ since σ is a homomorphism and also fixes F . Therefore $\sigma(\alpha)$ is a root of $p(x)$.

Proposition: Let E/F be an algebraic extension and $\sigma : E \rightarrow E$ a field map which fixes F . Then σ is surjective and hence an automorphism of E .

Proof: Let $\beta \in E$. Let $p(x) = \text{Irr}(\beta, E)$. Let $\{\beta_1, \dots, \beta_t\}$ be the roots of $p(x)$ which lie in E , and wlog, let $\beta_1 = \beta$. By the remark, $\sigma(\beta_i)$ is also a root for all i and hence in E . Therefore $\sigma : \{\beta_1, \dots, \beta_t\} \rightarrow \{\beta_1, \dots, \beta_t\}$ is an injective set map, and hence is also onto. In particular, $\sigma(\beta_i) = \beta_i = \beta$ for some β_i above. Hence $\beta \in \text{im}(\sigma)$.

Theorem/Definition: Let E/F be an algebraic extension. Then TFAE:

1. E is the splitting field for some set of nonconstant polynomials in $F[x]$
2. Every irreducible polynomial in $F[x]$ which has a root in E splits in E .
3. If $\sigma : E \rightarrow \bar{F}$ is a field map that fixes F , then $\sigma(E) = E$ (i.e. σ is really an automorphism of E).

If E/F satisfies (1),(2),or (3) then E/F is called a **normal** extension.

Proof: (2) \Rightarrow (1): Let $\alpha \in E$, and let $p_\alpha(x) = \text{Irr}(\alpha, F)$. By (2), $p_\alpha(x)$ splits in E . Let $S = \{p_\alpha(x) \mid \alpha \in E\}$. Then E is the splitting field for S .

(1) \Rightarrow (3): Let $\sigma : E \rightarrow \bar{F}$ be an embedding fixing F . We need to show that $\sigma(E) = E$. As E/F is algebraic, and by the proposition, we need only show that $\sigma(E) \subseteq E$. By (1), E is the splitting field for a set $S \subseteq F[x] \setminus F$. Therefore, $E = F(\text{all roots of all polynomials in } S)$. Let β be a root of $p(x) \in S$. Since σ fixes F , $\sigma(\beta)$ is also a root of $p(x)$. But $p(x)$ splits in E , therefore $\sigma(\beta) \in E$, hence $\sigma(E) \subseteq E$.

(3) \Rightarrow (2): Let $p(x)$ be an irreducible polynomial in $F[x]$ which has a root $\alpha \in E$. Let $\beta \in \bar{F}$ be any root of $p(x)$. Let τ the composition of the maps:

$$\begin{aligned} F(\alpha) &\rightarrow F[x]/(p(x)) \rightarrow F(\beta) \\ \alpha &\rightarrow x + (p) \rightarrow \beta \end{aligned}$$

Therefore, $\tau : F(\alpha) \rightarrow F(\beta)$ is an isomorphism that sends α to β and fixes F . By an old theorem, we can extend $\tau : E \rightarrow \bar{F}$. By (3), $\sigma(E) = E$, therefore $\beta = \sigma(\alpha) \in E$. Therefore $p(x)$ splits in E .

Remarks/Examples:

1. If $[E : F] = 2$, then E/F is normal. Indeed, pick $\alpha \in E \setminus F$. Certainly $E = F(\alpha)$. Let $f(x) = \text{Irr}(\alpha, F)$. Then $(x - \alpha)$ is a factor of $f(x)$, so $f(x) = (x - \alpha)(x - \beta)$ for some $\beta \in E$. Then E is the splitting field for $f(x)$.
2. Take $E = \mathbb{Q}(\sqrt[3]{2})$. Then $x^3 - 2$ has a root in E , but $x^3 - 2$ doesn't split in E because its other roots are not real, and $E \subset \mathbb{R}$. So E/\mathbb{Q} is not normal.
3. Recall that if $K \subseteq F \subseteq E$, then E/K is algebraic $\Leftrightarrow E/F$ and F/K is algebraic. The same does not occur in the normal case. Suppose that $K \subseteq F \subseteq E$ and E/K is normal. Then E/F is normal, but F/K need not necessarily normal. For a counterexample, let L be the splitting field for $x^3 - 2$ over \mathbb{Q} , and take E to be in the above example. Then L/\mathbb{Q} is normal by definition, and hence L/E is normal. However, E/\mathbb{Q} is not normal.

4. Suppose that E/K is finite. Then E/K is normal $\Leftrightarrow E$ is the splitting field over K of a single polynomial. For the forward direction, suppose that $E = K(\alpha_1, \dots, \alpha_n)$, let $f_i(x) = \text{Irr}(\alpha_i, K)$. Then E is the splitting field for $f(x) = f_1(x) \cdots f_n(x)$. The reverse direction is by definition.
5. Let $\{L_i\}$ be a collection of fields, all of which are normal over F a field. Then $\bigcap L_i$ is normal over F .

Definition: Let E/F be an algebraic extension. Then the **normal closure** of E/F is the smallest field $L \supseteq E$ such that L/F is normal. Just let $L = \bigcap K$ where $E \subseteq K \subseteq \bar{F}$ and K/F is normal. Clearly L is normal over F by the previous remark and is contained in any normal extension of F containing E by definition.

Example: Let $E = \mathbb{Q}(\sqrt[3]{2})$, and $F = \mathbb{Q}$. We saw last time that E/F is not normal. The normal closure of E/F is $\mathbb{Q}(\sqrt[3]{2}, \omega)$ where $\omega = e^{2\pi i/3}$. It is normal as it is the splitting field for $x^3 - 2$. It is the closure because suppose that L/\mathbb{Q} is normal and $L \subseteq \mathbb{Q}(\sqrt[3]{2})$. Then $x^3 - 2$ has a root in L and L is normal, so $x^3 - 2$ splits in L , therefore L contains ω . So, $L \supseteq \mathbb{Q}(\sqrt[3]{2}, \omega)$ and therefore $\mathbb{Q}(\sqrt[3]{2}, \omega)$ is the normal closure of E/F . Along these lines, we have the following useful proposition:

Proposition: Suppose that $E = F(\alpha_1, \dots, \alpha_n)$, and suppose that E/F is algebraic. Let $f_i(x) = \text{Irr}(\alpha_i, F)$. Let L be the splitting field for $f(x) = f_1(x) \cdots f_n(x)$ over F . Then L is the normal closure of E/F .

Proof: L/F is normal as it is the splitting field of $f(x)$. If $T \supseteq E$ and T/F is normal, then $f_i(x)$ has a root in T and hence splits in T for all i . Therefore, $T \subseteq L$. So, L is the smallest normal extension of F containing E . For another example, let $E = \mathbb{Q}(\sqrt[5]{2}, \sqrt[3]{3})$. Then the normal closure of E/\mathbb{Q} is $\mathbb{Q}(\sqrt[5]{2}, e^{2\pi i/5}, \sqrt[3]{3}, e^{2\pi i/3})$.

Let R be a commutative ring with 1_R . Since $(R, +)$ is an abelian group, we can let \mathbb{Z} act on R as follows: for $m \in \mathbb{Z}$, $r \in R$, define

$$mr = \begin{cases} \sum_{i=1}^m r & m > 0 \\ \sum_{i=1}^m (-r) & m < 0 \\ 0 & m = 0 \end{cases}$$

Note that the above turns $(R, +)$ into a \mathbb{Z} module, and that the above definition in fact works for any abelian group. Let $P = \langle 1_R \rangle = \{m \cdot 1_R \mid m \in \mathbb{Z}\}$ where $\langle 1_R \rangle$ is the \mathbb{Z} -submodule generated by 1_R in $(R, +)$. Of course, P is a cyclic group under $+$ but it is in fact a subring of R since $(m \cdot 1_R)(n \cdot 1_R) = (mn) \cdot 1_R \in P$.

Definition: $P = \langle 1_R \rangle$ is called the **prime subring** of R and P is clearly the smallest subring of R containing 1_R . For some examples, the prime subring of \mathbb{Q} is \mathbb{Z} and the prime subring of \mathbb{Z}_n is \mathbb{Z}_n .

Now, consider the ring map $\phi : \mathbb{Z} \rightarrow R$ sending $m \mapsto m \cdot 1_R$. By definition, $P = \mathfrak{I}(\phi)$, and we also have that $\ker(\phi) = (n)$ where $n \geq 0$.

Definition: If $\ker \phi = (n)$, $n \geq 0$, then R is said to have **characteristic** n . Since $P \cong \mathbb{Z}/\ker \phi = \mathbb{Z}/(n)$, we have that if R has characteristic n then $P \cong \mathbb{Z}_n$ and if R has characteristic zero, then $P \cong \mathbb{Z}$.

Examples: The characteristic of $\mathbb{Q}, \mathbb{Z}, \mathbb{R}$, or \mathbb{C} are all zero. $\text{Char } \mathbb{Z}_n[x]/(x^2 - 3) = n$. $\text{Char } \mathbb{Z}_6 \times \mathbb{Z}_8 = 24 = \text{lcd}(6, 8)$. As a remark, if R is a domain, then the characteristic of $R = 0$ or p , p a prime (else we

would have zerodivisors in R).

Definition: If F is a field, then the prime subfield of F is the smallest subfield of F containing 1_F . Certainly the prime subfield contains the prime subring. Also the characteristic of $F = 0$ or p , p a prime. If the characteristic of the field is p , then $P = \mathbb{Z}_p$ and P is already a field, so the prime subring equals the prime subfield. If $\text{Char } F = 0$, then $P \cong \mathbb{Z}$ and so the prime subfield has to be \mathbb{Q} .

Definition: Let $f(x) \in F[x]$ be a polynomial and $\alpha \in \bar{F}$ be a root of $f(x)$. Then α is called a multiple root of $f(x)$ if $(x - \alpha) \mid f(x)$ in $\bar{F}[x]$.

Definition: Let $f(x) \in F[x]$, $f(x) = c_n x^n + \cdots + c_1 x + c_0$. Define the derivative of $f(x)$ by

$$f'(x) = (n c_n) x^{n-1} + ((n-1) c_{n-1}) x^{n-2} + \cdots + c_1 \in F[x]$$

Check that the normal rules for derivative like linearity, product rule and chain rule still work (they do).

Proposition: Let $f(x) \in F[x]$ and $\alpha \in \bar{F}$ be a root of $f(x)$. Then α is a multiple root of $f(x) \Leftrightarrow f'(\alpha) = 0$.

Proof: If α is a multiple root, then $f(x) = (x - \alpha)^2 g(x)$. Then $f'(x) = 2(x - \alpha)g(x) + (x - \alpha)^2 g'(x)$, so that $f'(\alpha) = 0$. Conversely, suppose that $f'(\alpha) = 0$ and write $f(x) = (x - \alpha)h(x)$. Then $f'(x) = h(x) + (x - \alpha)h'(x)$, hence $0 = f'(\alpha) = h(\alpha)$. By the root theorem, $(x - \alpha)$ is a factor of $h(x)$, so write $h(x) = (x - \alpha)g(x)$, hence $f(x) = (x - \alpha)^2 g(x)$ as desired.

Theorem: Let $f(x) \in F[x] \setminus F$. Then $f(x)$ has multiple roots $\Leftrightarrow \gcd(f, f') = 1$.

Proof: If $f(x)$ has no multiple roots then f and f' have no common root in F . Therefore, $\gcd_{\bar{F}}(f, f') = 1 = \gcd_F(f, f')$. For the reverse direction, if $\gcd_F(f, f') = 1$ then f and f' have no common factors in \bar{F} . Therefore f and f' have no common roots, hence f has no multiple roots.

Theorem: Let $f(x)$ be an irreducible polynomial in $F[x]$.

1. If $\text{Char } F = 0$ then $f(x)$ has no multiple roots.
2. If $\text{Char } F = p$ then $f(x)$ has multiple roots $\Leftrightarrow f(x) = g(x^p)$ for some $g(x) \in F[x]$, i.e. $f(x) = a_n x^{pn} + a_{n-1} x^{p(n-1)} + \cdots + a_1 x^p + a_0$.

Proof: Certainly, $\deg f'(x) < \deg f$. Since $f(x)$ is irreducible, $\gcd(f', f) = 1$ or cf for some $c \in F$. If $f'(x) \neq 0$, then $cf \nmid f'$ so $\gcd(f, f') = 1$. Therefore, $\gcd(f, f') \neq 1 \Leftrightarrow f'(x) = 0$. So, in case 1) this cannot happen since we are in characteristic zero. If the $\text{Char } F = p$, then $f'(x) = 0 \Leftrightarrow$ the only nonzero coefficients occur in front of powers of x to a multiple of p , i.e. $f(x) = g(x^p)$ for some $g \in F[x]$.

Note that if $|F| < \infty$ then $\text{Char } F = p$ where p is a prime. In fact, $\mathbb{Z}_p \subseteq F$.

Proposition: If $|F| < \infty$ then $|F| = p^n$ where $p = \text{Char } F$.

Proof: $F \supseteq \mathbb{Z}_p$ and as $|F| < \infty$, F/\mathbb{Z}_p is algebraic, with $[F : \mathbb{Z}_p] = n$. So, as a \mathbb{Z}_p vector space, $F \cong (\mathbb{Z}_p)^n$ and hence $|F| = p^n$.

Remark: If $\text{Char } R = p$, where p is a prime, then $(a + b)^p = a^p + b^p$ by the binomial theorem. In fact, we get that $(a + b)^{p^n} = a^{p^n} + b^{p^n}$ for any $n \geq 1$. The function

$$\phi : R \rightarrow R$$

$$a \mapsto a^p$$

is a ring homomorphism for this reason and is called the **Frobenius endomorphism**.

Theorem: Let p be a prime and $n \geq 1$. Then there exists a field of order p^n . Moreover, any field of order p^n is a splitting field of $x^{p^n} - x$ over \mathbb{Z}_p . Hence, any two finite fields of the same order are isomorphic.

Proof: Let p, n be given. Let F be a splitting field for $f(x) = x^{p^n} - x$ over \mathbb{Z}_p . Let $S = \{\alpha \in F \mid f(\alpha) = 0\}$. Since $f'(x) = -1$, $f(x)$ has p^n distinct roots in F , and hence $|S| = p^n$. We claim that $S = F$. It is enough to show that S is a field, since F was the splitting field for $x^{p^n} - x$ and certainly has to contain all its roots. By a HW exercise (If E/F is an algebraic field extension and R a subring of E that contains F , then R is a field), it is enough to show that S is a ring, so it is enough to check that S is closed under $+$ and $*$. $*$ is easily checked, and for $+$, note that if $\alpha, \beta \in S$, we have that $(\alpha + \beta)^{p^n} - (\alpha + \beta) = \alpha^{p^n} + \beta^{p^n} - \alpha - \beta = 0$, so $\alpha + \beta \in S$. Therefore $S = F$ and $|F| = p^n$.

Now let E be a field of order p^n , p a prime. So $\text{Char } E = \text{Char } F = p$. Therefore $\mathbb{Z}_p \subseteq E$. Note that $|E^\times| = p^n - 1$, where E^\times denotes the group of units of E . By Lagrange's Theorem, we have that $\alpha^{p^n-1} = 1$ for all $\alpha \in E^\times$, and this $\alpha^{p^n} = \alpha$ for all $\alpha \in E$. So, every element in E is a root of $x^{p^n} - x \in \mathbb{Z}_p[x]$. Certainly E is a splitting field of $x^{p^n} - x$, and hence $E \cong F$.

Proposition: Let F be a field of order p^n . Then F is the splitting field of an irreducible polynomial in $\mathbb{Z}_p[x]$ of deg n .

Proof: As F is a finite field, F^\times is cyclic. Let $F^\times = \langle \alpha \rangle$. Certainly, $F = \mathbb{Z}_p(\alpha)$. Since $[\mathbb{Z}_p(\alpha) : \mathbb{Z}_p] = n$, we have that $f(x) = \text{Irr}(\alpha, \mathbb{Z}_p)$ has degree n . Now, note that F/\mathbb{Z}_p is normal since it is the splitting field of $x^{p^n} - x$. Hence $f(x)$ splits in F since it has a root in F . Therefore F is the splitting field for $f(x)$.

Example/Remark: Let $f(x) \in K[x]$ be an irreducible polynomial. We know that f has multiple roots $\Leftrightarrow (f, f') = 1 \Leftrightarrow f \nmid f'$, as f is irreducible $\Leftrightarrow f' = 0$. So, if $\text{Char } K = 0$ then every irreducible polynomial has only simple roots. If $\text{Char } K = p > 0$, then there may exist $f(x)$ irreducible such that $f'(x) = 0$.

Indeed, assume that $K^p \neq K$ (i.e K is not perfect), and take $a \in K^p \setminus K$. Then $x^p - a$ is irreducible and has multiple roots. To see that $x^p - a$ is irreducible, then there would exist g irreducible in $K[x]$ such that $\deg g < \deg f = p$ and $g \mid f$. Note that $g' \neq 0$ as the leading term of the polynomial is not a power of p . If $g = x^i + \dots + \beta_1 x + \beta_0$ where $i < p$, then $g' = ix^{i-1} + \dots + \beta_1 \neq 0$ so g has no multiple roots. Note that this is true for every irreducible factor of f . However, f itself has multiple roots, and hence $f = (x - b)^p$ (since different irreducible polynomials do not share roots???) where $b^p = a \in K^p$, a contradiction.

Definition: An irreducible polynomial is called **separable** if it has no multiple roots. (i.e. $\gcd(f, f') = 1$). This is the case $\Leftrightarrow f$ has precisely as many roots as its degree. The example show that in characteristic zero, every polynomial is separable but in $\text{Char } p > 0$, there exist irreducible polynomials f that have a unique root.

Remark: Let α be a root of an irreducible polynomial $f \in K[x]$. Then there is an embedding

$$K(\alpha) \rightarrow \bar{K}$$

that fixes K . For each root of f , we get such an embedding, and distinct roots give distinct embeddings. So, the number of embeddings is the number of distinct roots.

Proposition: Let $K \subseteq F \subseteq E$ be a sequence of algebraic field extensions, and let $\sigma, \tau : F \rightarrow \bar{F}$ be embeddings over K . Set $S_\sigma = \{\pi : E \rightarrow \bar{F} \mid \pi|_F = \sigma\}$ and $S_\tau = \{\pi : E \rightarrow \bar{F} \mid \pi|_F = \tau\}$. Then the sets

S_σ and S_τ have the same cardinality.

Proof: Since \bar{F} is algebraic over $\sigma(F)$, there exists a $\lambda : \bar{F} \rightarrow \bar{F}$ so that $\lambda|_{\sigma(F)} = \tau\sigma^{-1}$ by the lifting theorem we did a while ago. So, for every $\chi \in S_\sigma$, consider the composition $\lambda\chi : E \rightarrow \bar{F}$. Then for $a \in A$, note that

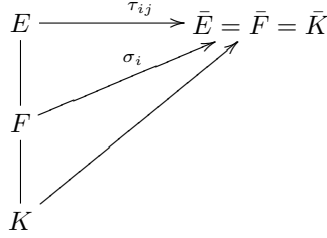
$$\lambda\chi(a) = \lambda\sigma(a) = (\tau\sigma^{-1})(\sigma(a)) = \tau(a)$$

so that $\lambda\chi \in S_\tau$. Switching σ and τ and using the map λ^{-1} we get a similar correspondence in which the composition is the identity on both sets. Therefore $|S_\sigma| = |S_\tau|$.

Definition: The cardinality of the set of extensions of any embedding $\sigma : F \rightarrow \bar{F}$ is called to **separability degree** of E/F and is denoted $[E : F]_s$. This is well defined in view of the above proposition.

Theorem: Let $K \subseteq F \subseteq E$ and E/K be algebraic. Then $[E : K]_s = [E : F]_s[F : K]_s$.

Proof: Let $\{\sigma_i : F \rightarrow \bar{E}\}$ be the set of all embeddings of F into $\bar{E}(= \bar{F})$ fixing K . For each $i \in I$, choose, by the proposition, $[E : F]_s$ extensions $\tau_{ij} : E \rightarrow \bar{E}$ such that $\tau_{ij}|_F = \sigma_i$. In this way, we get $[E : F]_s[F : K]_s$ distinct embeddings of E/K . We have the picture:



Since for every embedding $\tau : E \rightarrow \bar{E}$ over K , we have that $\tau|_F = \sigma_i$ for some i , we have obtained all embeddings of $E \rightarrow \bar{E}$ over K .

Lemma: If $F = K(\alpha)$ is an algebraic extension, then $[F : K]_s =$ number of distinct roots of $\text{Irr}(\alpha, F) \leq [F : K]$. For the proof, this is the initial example that we computed.

Proposition: For every finite extension $K \subset F$ there is an inequality $[F : K]_s \leq [F : K]$.

Proof: F is finitely generated by algebraic elements, so $F = K(\alpha_1, \dots, \alpha_n)$. Then we have a chain of field extensions

$$K \subseteq K(\alpha_1) = K_1 \subseteq K(\alpha_1, \alpha_2) = K_2 \subseteq \dots \subseteq K(\alpha_1, \dots, \alpha_n) = K_n = F$$

So we have $[K_{i+1} : K_i]_s \leq [K_{i+1} : K_i]$ and multiplying these inequalities we get $[F : K]_s \leq [F : K]$.

Definition: An element $\alpha \in F$ is called **separable over K** if its irreducible polynomial over K is separable. An algebraic extension F/K is called separable if every element $\alpha \in F$ is separable over K .

Remark: Let $K \subseteq F \subseteq E$, and let $\alpha \in E$. Suppose that α is separable over K . Then α is separable over F . Indeed, we know that $\text{Irr}(\alpha, K)$ has distinct roots. However, $\text{Irr}(\alpha, F) \mid \text{Irr}(\alpha, K)$ so $\text{Irr}(\alpha, F)$ has distinct roots.

Theorem: If F/K is an algebraic extension, then it is separable if and only if $[F : K]_s = [F : K]$.

Proof: Induct on $[E : F]$. If $[E : F] = 1$ then $E = F$ hence E/F is separable. If $[E : F] > 1$, pick $\alpha \in E \setminus F$, and consider the diagram

$$\begin{array}{c}
E \\
| \\
F(\alpha) \\
| \\
F
\end{array}
>1$$

As α is separable over F and since $\alpha \in E \setminus F$, we have that $[F(\alpha) : F]_s = [F(\alpha) : F] > 1$. By induction, we have that $[E : F(\alpha)]_s = [E : F(\alpha)]$. Therefore, using the multiplicative law for separable extensions, we have that $[E : F]$ is separable. For the reverse direction, note that $[E : F]_s = [E : F]$ means that $[F(\alpha) : F]_s = [F(\alpha) : F]$ for all $\alpha \in E$ and hence α is separable for all $\alpha \in E$.

Corollary: Let $E = F(\alpha_1, \dots, \alpha_n)$ be an algebraic extension. Then E/F is separable \Leftrightarrow each α_i is separable over F .

Proof: The forward direction is trivial. For the reverse, consider the chain of fields:

$$F \subseteq F(\alpha_1) = F_1 \subseteq F(\alpha_1, \alpha_2) = F_2 \subseteq \dots \subseteq F(\alpha_1, \dots, \alpha_n) = F_n = E$$

Then consider also F_i/F_{i-1} . As α_i is separable over F , α_i is separable over F_{i-1} . Therefore, we have that $[F_i : F_{i-1}]_s = [F_i : F_{i-1}]$. Therefore, by multiplicativity of the separability degree, we get that $[E : F]_s = [E : F]$.

Theorem: Let E/F be an algebraic field extension. If $\text{Char } F = 0$ then E/F is separable.

Proof: Let $\alpha \in E$ and $f(x) = \text{Irr}(\alpha, F)$. Then $\gcd(f, f') = 1$ and hence $f(x)$ has distinct roots, so α is separable.

Definition: A field F is called **perfect** if every algebraic extension of F is separable (hence if $\text{Char } F = 0$ then F is perfect).

Theorem: Let F be a field of characteristic $p > 0$. Then F is perfect $\Leftrightarrow F = F^p = \{\alpha^p \mid \alpha \in F\}$ (i.e. every element of F has a p th root). Note also that F^p is a subfield of F in this case.

Proof: " \Rightarrow ": Let $a \in F$. Consider $f(x) = x^p - a \in F[x]$. Let E be a splitting field for f and let α be a root of $f(x)$ in E . So $\alpha^p = a$, so we wish to show that $\alpha \in F$. In $E[x]$, $f(x) = x^p - \alpha^p = (x - \alpha)^p$. Let $h(x) = \text{Irr}(\alpha, F)$. Then $h(x) \mid f(x)$. So, in $E[x]$, we have that $h(x) \mid (x - \alpha)^p$. But E/F is separable, so α is separable over F , hence $h(x)$ has no multiple roots. Therefore $h(x) = (x - \alpha)$. Therefore $\alpha \in F$ and we have that a is a p th power of α .

" \Leftarrow ": Let E/F be an algebraic extension. Let $\alpha \in E$ and suppose α is not separable over F . Let $f(x) = \text{Irr}(\alpha, F)$. Then $f(x)$ has multiple roots and by a previous result, we have that $f(x) = g(x^p)$ for some $g \in F[x]$, say $g(x) = a_n x^n + \dots + a_1 x + a_0 \in F[x]$. For each i , let $a_i = b_i^p$, since $F = F^p$. Then we have that $f(x) = g(x^p) = b_n^p (x^n)^p + \dots + b_1 x^p + b_0^p = (b_n x^n + \dots + b_1 x + b_0)^p$, a contradiction to the fact that $f(x)$ was irreducible. Therefore, α is separable.

Corollary: Every finite field is perfect.

Proof: Let F be a finite field, $\text{Char } F = p$. Consider the Frobenius endomorphism

$$\phi : F \rightarrow F$$

$$a \mapsto a^p$$

Note that $\ker \phi = \{0\}$, so as F is finite, ϕ is surjective as well, so $F = F^p$. Therefore, F is perfect.

Example: Let t be an indeterminate over \mathbb{Z}_p . Let $F = \mathbb{Z}_p(t)$. Then $F \neq F^p$ as t is not a p th power. Therefore, F is not perfect. An inseparable element would be α where α is a root of $f(x) = x^p - t$.

Major Proposition on Separability: Let K be a field of Char P , $\alpha \in \bar{K}$.

1. α is separable over $K \Leftrightarrow K(\alpha) = K(\alpha^p)$.
2. If α is inseparable over K , then $[K(\alpha) : K(\alpha^p)] = p$ and $\text{Irr}(\alpha, K(\alpha^p)) = x^p - \alpha^p$.
3. $[K(\alpha) : K]_s = [K(\alpha^{p^n}) : K]_s$ for all $n \geq 1$.
4. α^{p^n} is separable over K for all large n .
5. $[K(\alpha) : K] = p^n [K(\alpha) : K]_s$ where n is the largest nonnegative integer such that α^{p^n} is separable.

Proof:

1. “ \Rightarrow ”: Suppose α is separable over K . So α is separable over $K(\alpha^p)$. Let $f(x) = \text{Irr}(\alpha, K(\alpha^p))$. Then $f(x) \mid x^p - \alpha^p \in K(\alpha^p)[x]$. Therefore, in $K(\alpha)[x]$, $f(x) \mid (x - \alpha)^p$. As $f(x)$ has no multiple roots $f(x) = x - \alpha$. Therefore $\alpha \in K(\alpha^p)$ and hence $K(\alpha) = K(\alpha^p)$.
“ \Leftarrow ”: Suppose $K(\alpha) = K(\alpha^p)$. Let $h(x) = \text{Irr}(\alpha, K)$. Suppose $h(x)$ has multiple roots. Then $h(x) = g(x^p)$ for some $g(x) \in K[x]$. But $h(\alpha) = g(\alpha^p) = 0$. Thus, $[K(\alpha^p) : K] \leq \deg g(x) < \deg h$. On the other hand, $[K(\alpha^p) : K] = [K(\alpha) : K] = \deg h$, a contradiction. Thus $h(x)$ does not have multiple roots.
2. Let $f(x) = \text{Irr}(\alpha, K(\alpha^p))$. We know $f(x) \mid x^p - \alpha^p = (x - \alpha)^p$. Therefore, we have that $f(x) = (x - \alpha)^m$ for some $1 \leq m \leq p$. Note that $m > 1$ as α is inseparable. So, expanding $f(x)$ gives $f(x) = x^m + (m\alpha)x^{m-1} + \dots$, so $m\alpha \in K(\alpha^p) \Rightarrow \alpha \in K(\alpha^p)$ unless $m = p$, so we must have that $m = p$, again, since α is inseparable. Therefore, $\text{Irr}(\alpha, K(\alpha^p)) = x^p - \alpha^p$ and hence $[K(\alpha) : K(\alpha^p)] = p$.
3. $[K(\alpha) : K(\alpha^p)]_s = [K(\alpha^p)(\alpha) : K(\alpha^p)]_s =$ the number of distinct roots of $\text{Irr}(\alpha, K(\alpha^p)) = 1$ since the only root of $\text{Irr}(\alpha, K(\alpha^p))$ is α . So, as $[\cdot, \cdot]_s$ is multiplicative, $[K(\alpha) : K]_s = [K(\alpha^p) : K]_s$ and by induction we see that $[K(\alpha) : K]_s = [K(\alpha^{p^n}) : K]_s$ for all $n \geq 1$.
4. Consider the chain of fields

$$K(\alpha) \subseteq K(\alpha^p) \subseteq K(\alpha^{p^2}) \subseteq \dots \subseteq K$$

This is a descending chain of finite dimensional vector K vector spaces (as α is algebraic over K , $[K(\alpha) : K] < \infty$). Therefore, for some n , we have that $K(\alpha^{p^n}) = K(\alpha^{p^{n+1}})$. Therefore, α^{p^n} is separable over K . Thus $K(\alpha^{p^n})/K$ is separable and hence α^{p^l} is separable for all $l \geq n$.

5. By the above propositions, we have the following tower of fields and their degrees

$$\begin{array}{c}
 K(\alpha) \\
 \left| \begin{array}{c} p \\ \vdots \\ p \end{array} \right. \\
 K(\alpha^p) \\
 \left| \begin{array}{c} p \\ \vdots \\ p \end{array} \right. \\
 \vdots \\
 \left| \begin{array}{c} p \\ \vdots \\ p \end{array} \right. \\
 K(\alpha^{p^n}) \\
 \left| \begin{array}{c} \text{sep} \end{array} \right. \\
 K
 \end{array}$$

Therefore, we have that $[K(\alpha) : K] = p^n [K(\alpha^{p^n}) : K] = p^n [K(\alpha^{p^n}) : K]_s = p^n [K(\alpha) : K]_s$, as desired.

Theorem: Let $E = K(\alpha_1, \dots, \alpha_n)$ be a finite extension. Then $[E : K] = p^m [E : K]_s$ for some $m \geq 0$.

Proof: Prove by induction on n . For the case $n = 1$, this is part 5 of the above major proposition. For $n > 1$, let $F = K(\alpha_1, \dots, \alpha_{n-1})$. By induction, $[F : K] = p^l [F : K]_s$. As $E = F(\alpha_n)$, $[E : F] = p^k [E : F]_s$, and hence $[E : K] = p^{k+l} [E : K]_s$.

Corollary: If $[E : K] < \infty$ then $[E : K]_s \mid [E : K]$.

Definition: Let E/K be a finite field extension. Then define the inseparable degree of E/K by $[E : K]_i = \frac{[E : K]}{[E : K]_s}$. By the theorem, $[E : K]_i = 1$ or a power of the characteristic. As a remark, we also have that the inseparability degree is multiplicative since both the usual degree and the separable degree are multiplicative.

Definition: Let K be a field of characteristic p and α an algebraic element of \bar{K} . Then α is **purely inseparable** over K if $\alpha^{p^n} \in K$ for some $n \geq 0$. An algebraic extension E/K is called **purely inseparable** if each $\alpha \in E$ is purely inseparable.

Lemma: An element $\alpha \in \bar{K}$ is purely inseparable over $K \Leftrightarrow [K(\alpha) : K] = [K(\alpha) : K]_i \Leftrightarrow [K(\alpha) : K]_s = 1$.

Proof: Suppose that α is purely inseparable over K . Then $\alpha^{p^n} \in K$ for some n . Then $[K(\alpha) : K]_s = [K(\alpha^{p^n}) : K]_s = [K : K]_s = 1$, by part 3) of the proposition. Suppose that $[K(\alpha) : K]_s = 1$. By part 4), α^{p^n} is separable over K for some $n \geq 0$. Then $[K(\alpha^{p^n}) : K] = [K(\alpha^{p^n}) : K]_s = [K(\alpha) : K]_s = 1$ and hence $\alpha^{p^n} \in K$.

Theorem: Let E/K be a finite extension. Write $E = K(\alpha_1, \dots, \alpha_n)$. Then TFAE:

1. E/K is purely inseparable.

2. Each α_i is purely inseparable.
3. $[E : K]_s = 1$
4. $[E : K]_i = [E : K]$

Proof: Induction on n (Exercise).

Let n be a positive integer and let ω be a primitive n th root of unity over \mathbb{Q} . Then $\{\omega^i \mid \gcd(i, n) = 1\}$ is the set of all the primitive n th roots of unity.

Definition: The n th cyclotomic polynomial is

$$\Phi_n = \prod_i (x - \omega_i)$$

Where the product is taken over all $i \in \{0, 1, \dots, n-1\}$ such that $\gcd(i, n) = 1$. For example, we have that

1. $\Phi_1(x) = x - 1$
2. $\Phi_2(x) = x + 1$
3. $\Phi_3(x) = x^2 + x + 1$
4. $\Phi_4(x) = x^2 + 1$
5. $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$.

Remark: Note that $x^n - 1 = \prod_{d|n} \phi_d(x)$. Furthermore, $\deg \Phi_n(x) = \phi(n)$ (the Euler phi function). To see this, note that $x^n - 1 = \prod_{i=0}^{n-1} (x - \omega^i)$. Then group the factors $x - \omega^i$ according to the order of ω^i in the group of units. If ω^i has order d then $d \mid n$ and ω^i is a primitive d th root of unity. The statement about the degree is clear from the definition of the cyclotomic polynomial.

Example: Find $\Phi_9(x)$. Note that $x^9 - 1 = \Phi_1(x)\Phi_3(x)\Phi_9(x) = (x^3 - 1)(x^6 + x^3 + 1)$. Therefore, we have that $\Phi_9(x) = x^6 + x^3 + 1$.

Lemma: $\Phi_n(x) \in \mathbb{Z}[x]$.

Proof: We induce on n , with the statement being true for the cases computed above. Assume that it is true for $1 \leq d < n$. Then $x^n - 1 = f(x)\Phi_n(x)$, where $f(x) \in \mathbb{Z}[x]$ by induction (since $f(x)$ is the product of all the cyclotomic polynomials of integers that divide n). We have $x^n - 1 = f(x)\Phi_n(x)$ in $\mathbb{Q}(\omega)[x]$. But $f(x)$ is monic, and the division algorithm works in any polynomial ring $R[x]$ with R commutative as long as the leading coefficient of $f(x)$ is a unit. So, in $\mathbb{Z}[x]$, we have $x^n - 1 = f(x)q(x) + r(x)$ where $q, r \in \mathbb{Z}[x]$ and $\deg r < \deg f$. This equation also holds true in $\mathbb{Q}(\omega)[x]$. Hence $r(x) = 0$ and $q(x) = \Phi_n(x)$. Thus $\Phi_n(x) \in \mathbb{Z}[x]$.

Theorem: $\Phi_n(x)$ is irreducible for all $n \geq 1$.

Proof: Let $f(x) \in \mathbb{Q}[x]$ be an irreducible factor of $\Phi_n(x)$. By Gauss' Lemma, we may choose $f(x) \in \mathbb{Z}[x]$. We'll show that $f(x) = \Phi_n(x)$. Write $\Phi_n(x) = f(x)g(x)$, where $g(x) \in \mathbb{Z}[x]$. Let ω be a root of $f(x)$. Then ω is a primitive n th root of unity. Assuming the below claim, we inductively have that ω^i is a root

of f for any $i > 0$ such that $\gcd(i, n) = 1$. Hence all the primitive n th roots of unity are roots of $f(x)$ and hence $\Phi_n(x) = f(x)$.

Claim: If p is a prime not dividing n , then ω^p is also a root of $f(x)$.

Proof of Claim: Certainly ω^p is another primitive n th root of unity, hence a root of $\Phi_n(x)$. Suppose that $f(\omega^p) \neq 0$. Then $g(\omega^p) = 0$. Therefore ω is a root of $g(x^p)$. As $f(x)$ is irreducible, and $f(\omega) = 0$, we have that $f(x) \mid g(x^p)$. So $g(x^p) = f(x)h(x)$ with $h(x) \in \mathbb{Z}[x]$. In $\mathbb{Z}_p[x]$, we get that $(\bar{g}(x))^p = \bar{g}(x^p) = \bar{f}(x)\bar{h}(x)$, since we have that $a^p = a$ for any $a \in \mathbb{Z}_p$. Therefore, $\bar{f}(x)$ and $\bar{g}(x)$ must share some common root in some algebraic closure of \mathbb{Z}_p . But since $\bar{\Phi}_n(x) = \bar{f}(x)\bar{g}(x)$, $\Phi_n(x)$ has multiple roots. Therefore $\bar{x}^n - \bar{1}$ has multiple roots. But $\gcd(\bar{x}^n - 1, n\bar{x}^{n-1}) = 1$ as $p \nmid n$, a contradiction. Therefore, ω^p is also a root of $f(x)$.

Corollary: Let ω be a primitive n th root of unity over \mathbb{Q} . Then $[\mathbb{Q}(\omega) : \mathbb{Q}] = \phi(n)$. The above extension is called a cyclotomic extension.

Definition: Let E/F be a finite extension. If $E = F(\alpha)$ for some $\alpha \in E$, then α is called a primitive element for E/F . We have a couple theorems giving criterion for when a primitive element exists.

Primitive Element Theorem I: Let E/F be a finite extension. Then $E = F(\alpha)$ for some $\alpha \in E \Leftrightarrow$ there exist only finitely many intermediate fields between E and F .

Proof: " \Leftarrow ": We break the argument into cases. If $|F| < \infty$, then $|E| < \infty$ also. Then $E^\times = \langle \alpha \rangle$ for some $\alpha \in E$. Then we immediately have that $E = F(\alpha)$. For the case when $|F| = \infty$, as E is finite, we have that $E = F(\alpha_1, \dots, \alpha_n)$. By induction, it is enough to consider the case where $n = 2$. Let $E = F(\alpha, \beta)$. Consider the set of fields $\Lambda = \{F(\alpha + c\beta) \mid c \in F\}$. Since F is infinite and by our hypothesis, there exists $c_1 \neq c_2 \in F$ such that $L = F(\alpha + c_1\beta) = F(\alpha + c_2\beta)$. Therefore, we have that $(c_1 - c_2)\beta \in L$ and hence $\beta \in L$ and $\alpha \in L$. Thus, we have that $F(\alpha, \beta) = L = F(\alpha + c_1\beta)$.

" \Rightarrow ": Let $\Lambda = \{L \mid L \text{ is a field and } F \subset L \subset E\}$. For each $L \in \Lambda$, let $g_L = \text{Irr}(\alpha, L)$. Recall that $g_L(x) \mid g_F(x)$ since $F \subseteq L$. As g_L is monic, there are only finitely many possible g_L 's. So we have reduced the problem to the following claim:

Claim: L is uniquely determined by $g_L(x)$.

Proof of Claim: Let $g_L(x) = x^m + c_{m+1}x^{m+1} + \dots + c_1x + c_0 \in L[x]$, with $g_L(x)$ irreducible and α a root of $g_L(x)$. Note that $g_L(x) \in F(c_{m-1}, \dots, c_1, c_0)[x] \subseteq L[x]$. Certainly $g_L(x)$ is irreducible in $F(c_{m-1}, \dots, c_1, c_0)[x]$. Consider the degrees of these field extensions to E . Note that $[E : L] = [F(\alpha) : L] = \deg g_L$. Also, $[E : F(c_{m-1}, \dots, c_1, c_0)] = \deg g_L$. So, we have that $L = F(c_{m-1}, \dots, c_1, c_0)[x]$, since $F(c_{m-1}, \dots, c_1, c_0)[x] \subseteq L$. Therefore, we there are only finitely many g_L 's, there are only finitely many elements in Λ , as desired.

Primitive Element Theorem II: If E/F is a finite separable extension then $E = F(\alpha)$ for some $\alpha \in E$ (and hence there are only finitely many intermediate fields between E and F by the last theorem).

Proof: By induction again, we may assume that $E = F(\alpha, \beta)$. Let $\{\sigma_1, \dots, \sigma_n\}$ be the distinct embeddings of $E \hookrightarrow \bar{F}$, which fix F . As E/F is separable, $n = [E : F]$. Also, by the previous theorem, we may assume that $|F| = \infty$, and that $[E : F] > 1$. Set

$$p(x) = \prod_{i \neq j}^n \left[(\sigma_i(\beta) - \sigma_j(\beta))x - (\sigma_j(\alpha) - \sigma_i(\alpha)) \right] \in \bar{F}[x]$$

First note that $p(x) \neq 0$ as $\sigma_i \neq \sigma_j$ and hence $\sigma_i(\alpha) \neq \sigma_j(\alpha)$ or $\sigma_i(\beta) \neq \sigma_j(\beta)$. Since F is infinite, $\exists c \in F$

such that $p(c) \neq 0$. So,

$$\begin{aligned} 0 \neq p(c) &= \prod_{i \neq j}^n \left[\left(\sigma_i(\beta) - \sigma_j(\beta) \right) c - \left(\sigma_j(\alpha) - \sigma_i(\alpha) \right) \right] \\ &= \prod_{i \neq j}^n \left[\sigma_i(\alpha + c\beta) - \sigma_j(\alpha + c\beta) \right] \end{aligned}$$

So, $\sigma_i(\alpha + c\beta) \neq \sigma_j(\alpha + c\beta)$ for all $i \neq j$. Then $\sigma_i|_{F(\alpha+c\beta)} : F(\alpha+c\beta) \hookrightarrow \bar{F}$ are distinct embeddings that fix F . So $[F(\alpha+c\beta) : F]_s \geq n$ and $[F(\alpha+c\beta) : F] \geq n$ implies that $F(\alpha+c\beta) = E$ as $F(\alpha+c\beta) \subseteq E$. Note that the above works for all but finitely many of the $c \in F$, namely at most $\binom{n}{2}$ of them.

Definition: Let E/F be a field extension. Then denote the set of automorphisms of E that fix F by

$$\text{Aut}(E/F) := \{ \phi : E \rightarrow E \mid \phi|_F = \text{Id}_F \}$$

Clearly the above is a group.

Examples:

1. $E = \mathbb{Q}(\sqrt[3]{2})$. What is $\text{Aut}(E/\mathbb{Q})$? We know that $\text{Irr}(\sqrt[3]{2}, \mathbb{Q}) = x^3 - 2$, and the roots of this polynomial are $\sqrt[3]{2}, \omega\sqrt[3]{2}$, and $\omega^2\sqrt[3]{2}$. If $\phi : E \rightarrow E$ fixes \mathbb{Q} then $\phi(\sqrt[3]{2})$ is a root of $x^3 - 2$. But the only root in E is $\sqrt[3]{2}$. Hence $\text{Aut}(E/\mathbb{Q}) = \{\text{Id}\}$.
2. Let $E = \mathbb{Q}(\omega)$ where $\omega = e^{2\pi i/n}$. To compute $\text{Aut}(E/\mathbb{Q})$, first recall that $\text{Irr}(\omega, \mathbb{Q}) = \Phi_n(x) = \prod_{(i,n)=1}^n (x - \omega^i)$. For each ω^i with $(i, n) = 1$, there exists a $\phi : E \rightarrow E$ sending ω to ω^i . Therefore, we have that $\text{Aut}(E/\mathbb{Q}) = \{ \phi_i : E \rightarrow E \mid \phi_i(\omega) = \omega^i \}$. Hence $|\text{Aut}(E/\mathbb{Q})| = \phi(n)$.

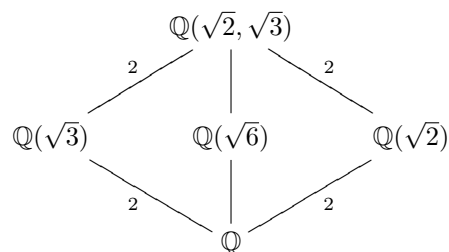
Proposition: Let E/F be finite. Then $|\text{Aut}(E/F)| \leq [E : F]_s$ with equality $\Leftrightarrow E/F$ is normal. Also, we have $|\text{Aut}(E/F)| = [E : F] \Leftrightarrow E/F$ is normal and separable.

Proof: Recall that $[E : F]_s = |S|$ where $S = \{ \phi : E \rightarrow \bar{F} \mid \phi|_F = \text{Id}_F \}$. But $\text{Aut}(E/F) \subseteq S$ and is the whole set if and only if E/F is normal. For the second assertion, certainly we have that $|\text{Aut}(E/F)| = [E : F]_s$ as E/F is normal. But since E/F is separable, we also have that $|\text{Aut}(E/F)| = [E : F]$. Note that all of the above implications reverse.

Definition: An algebraic extension E/F is **Galois** if E/F is normal and separable. In this case, the group $\text{Aut}(E/F)$ is called the **Galois group** of E/F and is denoted $\text{Gal}(E/F)$.

Examples:

1. Let $E = \mathbb{Q}(\omega)$ where ω was a primitive n th root of unity, we have that $\text{Gal}(E/\mathbb{Q}) = \mathbb{Z}_n^\times$.
2. Let $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. It is clear that E/\mathbb{Q} is Galois and that $|\text{Gal}(E/\mathbb{Q})| = [E : \mathbb{Q}] = 4$. We have the following field diagram:



Where we have the above degrees of extensions since $x^2 - 2$ is irreducible over both \mathbb{Q} and $\mathbb{Q}(\sqrt{3})$ and $x^2 - 3$ is irreducible over both \mathbb{Q} and $\mathbb{Q}(\sqrt{2})$. So, there are automorphisms (since we may only permute roots of the same polynomial)

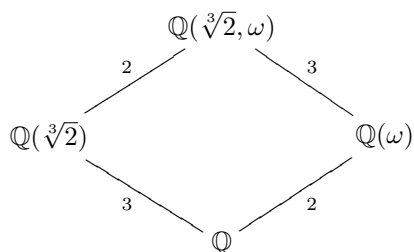
$$\begin{array}{ll}
 \tau : E \longrightarrow E & \sigma : E \longrightarrow E \\
 \sqrt{2} \mapsto -\sqrt{2} & \sqrt{2} \mapsto \sqrt{2} \\
 \sqrt{3} \mapsto \sqrt{3} & \sqrt{3} \mapsto -\sqrt{3}
 \end{array}$$

Note that the identity map works too, and composing the above maps gives us the map:

$$\begin{array}{l}
 \sigma\tau : E \longrightarrow E \\
 \sqrt{2} \mapsto -\sqrt{2} \\
 \sqrt{3} \mapsto -\sqrt{3}
 \end{array}$$

Therefore, we have that $\text{Aut}(E/\mathbb{Q}) \cong C_2 \times C_2$, the Klein 4-group.

3. Let E be the splitting field of $x^3 - 2$ over \mathbb{Q} . Then E/\mathbb{Q} is Galois and $E = \mathbb{Q}(\sqrt[3]{2}, \omega)$, where ω is a cube root of unity. Then as we have calculated before, we have that $[E : \mathbb{Q}] = |\text{Gal}(E/\mathbb{Q})| = 6$. We have the following diagram:



So we have two mappings right away

$$\begin{array}{ll}
 \tau : E \longrightarrow E & \sigma : E \longrightarrow E \\
 \sqrt[3]{2} \mapsto \omega \sqrt[3]{2} & \sqrt[3]{2} \mapsto \sqrt[3]{2} \\
 \omega \mapsto \omega & \omega \mapsto \omega^2
 \end{array}$$

Which are indeed field maps that fix \mathbb{Q} since $x^3 - 2$ is irreducible over $\mathbb{Q}(\omega)$ and $x^2 + x + 1$ is irreducible over $\mathbb{Q}(\sqrt[3]{2})$. Note also that $|\sigma| = 3$ and $|\tau| = 2$. Therefore, we get that $\text{Gal}(E/\mathbb{Q}) = \langle \sigma, \tau \rangle$. This

is S_3 , as note that $\sigma\tau : E \rightarrow E$ sends $\sqrt[3]{2}$ to $\omega\sqrt[3]{2}$ and $\tau\sigma$ sends $\sqrt[3]{2}$ to $\omega^2\sqrt[3]{2}$, hence $\text{Gal}(E/\mathbb{Q})$ is nonabelian (and so S_3). Note also that $E = \mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2})$. Any $\pi : E \rightarrow E$ permutes the set $\{\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}\}$. This gives a natural isomorphism from $\text{Gal}(E/\mathbb{Q}) \rightarrow S_3$ where σ corresponds to (123) and τ corresponds to (12).

Remark:

1. Let E/F be a Galois extension and L an intermediate field. Then E/L is Galois and $\text{Gal}(E/L) < \text{Gal}(E/F)$.
2. Also, let E/F be Galois and H a subgroup of $\text{Gal}(E/F)$. Then let $E_H := \{\alpha \in E \mid \sigma(\alpha) = \alpha \ \forall \sigma \in H\}$. Then E_H is an intermediate field of E/F , and is often called the **Fixed Field of H** . In fact we have the **Galois Correspondence**.

$$\begin{array}{ccc} \left\{ \text{Intermediate fields of } E/F \right\} & \longleftrightarrow & \left\{ \text{Subgroups of } \text{Gal}(E/F) \right\} \\ \\ L \dashv & \longrightarrow & \text{Gal}(E/L) \\ \\ E_H \longleftarrow & & \dashv H \end{array}$$

We will show that $L = E_{\text{Gal}(E/L)}$ and $\text{Gal}(E/E_H) = H$, i.e. that the above functions are mutually inverses.

Theorem: Suppose that E/F is Galois and let $G = \text{Gal}(E/F)$. Then $F = E_G$.

Proof: Certainly we have that $F \subseteq E_G$. Let $\alpha \in E_G$. Let $\sigma : F(\alpha) \rightarrow \bar{F}$ be an embedding which fixes F . Extend σ to $\tau : E \rightarrow E$ as E is normal. Hence $\tau \in G$. Since $\alpha \in E_G$, $\tau(\alpha) = \alpha$. Hence $\sigma(\alpha) = \alpha$. Therefore σ is the identity map. Hence $[F(\alpha) : F]_s = 1$ and since $F(\alpha)/F$ is separable, $[F(\alpha) : F] = 1$. Therefore $\alpha \in F$.

Corollary: Let E/F be Galois and L an intermediate field of E/F and $H = \text{Gal}(E/L) < \text{Gal}(E/F)$. Then $E_H = L$. Then the map:

$$\begin{array}{ccc} \left\{ \text{Intermediate fields of } E/F \right\} & \longleftrightarrow & \left\{ \text{Subgroups of } \text{Gal}(E/F) \right\} \\ \\ L \dashv & \longrightarrow & \text{Gal}(E/L) \end{array}$$

is injective.

Proof: Suppose that $\text{Gal}(E/L_1) = \text{Gal}(E/L_2) = H$. Then by the above theorem, $L_1 = E_H = L_2$. This proves half of the Galois correspondence.

Lemma: Let E/F be a separable extension. Suppose that there exists $n \in \mathbb{Z}$ such that $[F(\alpha) : F] \leq n$ for all $\alpha \in E$. Then E/F is finite and of degree n .

Proof: Choose $\alpha \in E$ such that $[F(\alpha) : F] = m$ is maximal. We claim that $E = F(\alpha)$. If not, then $\exists \beta \in E \setminus F(\alpha)$. Then $F(\alpha, \beta) \supsetneq F(\alpha)$ and by the primitive element theorem, there exists a primitive element for $F(\alpha, \beta)$ whose degree would violate maximality of m . Therefore $E = F(\alpha)$, for some $\alpha \in E$ and $[F(\alpha) = E : F] = m \leq n$.

Artin's Theorem: Let E be an arbitrary field and G a finite group of automorphisms of E . Let $F = E_G$, the fixed field of G in E . Then we have that E/F is Galois and finite and $G = \text{Gal}(E/F)$.

Proof: Let $\alpha \in E$. Let $\{\sigma_1, \dots, \sigma_r\}$ be a maximal subset of G such that $\sigma_1(\alpha), \dots, \sigma_r(\alpha)$ are distinct. If $\tau \in G$, then $\tau\sigma_1(\alpha), \dots, \tau\sigma_r(\alpha)$ are also distinct since τ is injective. Let $f_\alpha(x) = \prod_{i=1}^r (x - \sigma_i(\alpha))$. Note that $f_\alpha^\tau = \prod_{i=1}^r (x - \tau\sigma_i(\alpha)) = f_\alpha$. Hence $f_\alpha \in F[x]$. Since $\alpha = \sigma_i(\alpha)$ for some i , α is a root of f_α . Hence we have that $\text{Irr}(\alpha, F) \mid f_\alpha(x)$. Therefore $[F(\alpha) : F] \leq r \leq |G|$. Also, f_α has distinct roots, hence $\text{Irr}(\alpha, F)$ does, and hence α is separable over F . Therefore E/F is separable. By the lemma, $[E : F] \leq |G|$. As f_α splits over E , so does $\text{Irr}(\alpha, F)$ for all $\alpha \in E$. Therefore, E/F is normal and so it is Galois. Note that $G \subseteq \text{Gal}(E/F)$. Then $|G| \leq |\text{Gal}(E/F)| = [E : F] \leq |G|$. Hence $G = \text{Gal}(E/F)$ (and so $|G| = [E : F]$).

Corollary: Let E/F be a finite Galois extension and H a subgroup of $\text{Gal}(E/F)$. Then $\text{Gal}(E/E_H) = H$. For the proof, apply Artin's theorem to E and let H be the finite group of automorphisms of E .

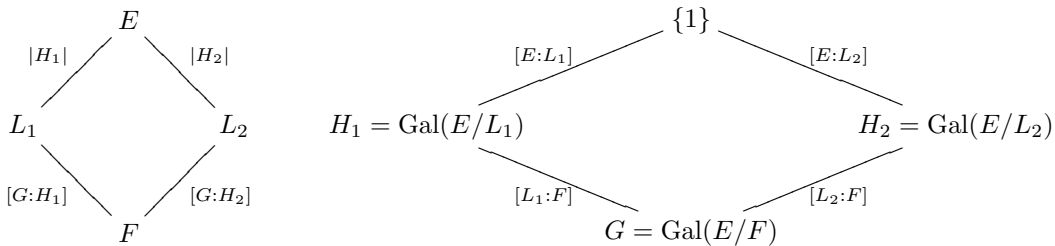
Fundamental Theorem of Galois Theory: Let E/F be a finite Galois extension. Then there exists a 1-1 inclusion reversing correspondence between

$$\left\{ \text{Intermediate fields of } E/F \right\} \longleftrightarrow \left\{ \text{Subgroups of } \text{Gal}(E/F) \right\}$$

$$L \longmapsto \text{Gal}(E/L)$$

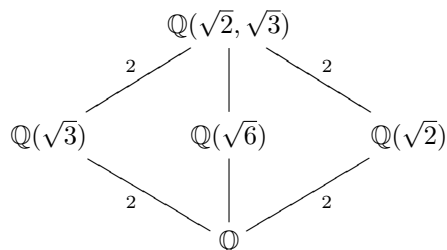
$$E_H \longleftarrow H$$

such that if $L_1 \subseteq L_2$ then $\text{Gal}(E/L_1) \supseteq \text{Gal}(E/L_2)$. Similarly, if we have $H_1 \subseteq H_2$ then $E_{H_1} \supseteq E_{H_2}$. Also, note that $[E : E_H] = |\text{Gal}(E/E_H)| = |H|$ and thus $[E_H : F] = \frac{[E:F]}{[E:E_H]} = \frac{|G|}{|H|} = [G : H]$. In other words, we have the following picture below as an illustrative example.



Examples:

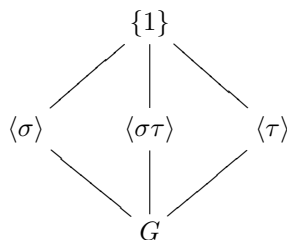
1. Find all intermediate fields of E/\mathbb{Q} where $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. We have calculated above what the field diagram looks like:



We also know that $G = \text{Gal}(E/\mathbb{Q}) = \{1, \sigma, \tau, \sigma\tau\}$ where σ and τ are given by:

$$\begin{array}{ll}
 \tau : E \longrightarrow E & \sigma : E \longrightarrow E \\
 \sqrt{2} \mapsto -\sqrt{2} & \sqrt{2} \mapsto \sqrt{2} \\
 \sqrt{3} \mapsto \sqrt{3} & \sqrt{3} \mapsto -\sqrt{3}
 \end{array}$$

The (upside down) subgroup lattice of G is



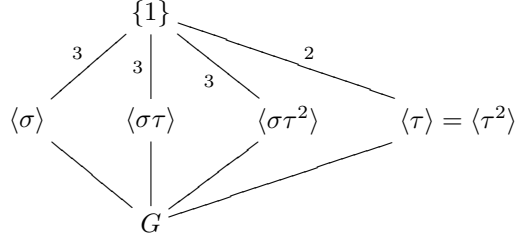
Where the subgroups of G correspond to the intermediate subfields of E/F that are in the same place. To justify this, note that σ clearly fixes $\sqrt{2}$ and τ clearly fixes $\sqrt{3}$. Also, note that $\sigma\tau(\sqrt{6}) = \sqrt{6}$ and therefore $\mathbb{Q}(\sqrt{6}) \subseteq E_{\langle\sigma\tau\rangle}$. Since $[\mathbb{Q}(\sqrt{6}) : \mathbb{Q}] = 2 = [G : \langle\sigma\tau\rangle] = [E_{\langle\sigma\tau\rangle} : \mathbb{Q}]$, we have that $\mathbb{Q}(\sqrt{6}) = E_{\langle\sigma\tau\rangle}$.

Let $K = \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Check that $\sqrt{2} + \sqrt{3}$ is not fixed by any $\sigma \in G \setminus \{1\}$. Therefore, $\text{Gal}(\mathbb{Q}(\sqrt{2} + \sqrt{3})/\mathbb{Q}) = \{1\}$ and hence $K = E$. This is another way to come up with a primitive element for an extension.

2. Let E be the splitting field of $x^3 - 2$ over \mathbb{Q} . We know that $E = \mathbb{Q}(\sqrt[3]{2}, \omega)$ where ω is a primitive 3rd root of unity. Also, we know that $\text{Gal}(E/\mathbb{Q}) \cong S_3 = \{1, \sigma, \tau, \tau^2, \sigma\tau, \sigma\tau^2\}$, where

$$\begin{array}{ll}
 \tau : E \longrightarrow E & \sigma : E \longrightarrow E \\
 \sqrt[3]{2} \mapsto \omega \sqrt[3]{2} & \sqrt[3]{2} \mapsto \sqrt[3]{2} \\
 \omega \mapsto \omega & \omega \mapsto \omega^2
 \end{array}$$

The subgroup lattice of $\text{Gal}(E/\mathbb{Q})$ is below:



Note that $E_{\langle \sigma \rangle} = \mathbb{Q}(\sqrt[3]{2})$. Indeed, we know that $\mathbb{Q}(\sqrt[3]{2}) \subseteq E_{\langle \sigma \rangle}$ and also $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3 = [G : \langle \sigma \rangle] = [E_{\langle \sigma \rangle} : \mathbb{Q}]$. Hence $E_{\langle \sigma\tau \rangle} = \mathbb{Q}(\omega\sqrt[3]{2})$. Similar arguments may be given for why $E_{\langle \sigma\tau^2 \rangle} = \mathbb{Q}(\omega^2\sqrt[3]{2})$, $E_{\langle \sigma\tau^2 \rangle} = \mathbb{Q}(\omega^2\sqrt[3]{2})$, and $E_{\langle \tau \rangle} = \mathbb{Q}(\omega)$. Note also that here $\omega + \sqrt[3]{2}$ is not fixed by any non-identity element in G . Therefore $E = \mathbb{Q}(\omega + \sqrt[3]{2})$.

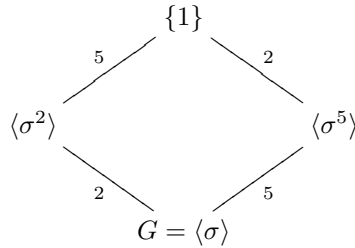
Proposition: Let E/F be a finite Galois extension and H a subgroup of $\text{Gal}(E/F)$. Let $\alpha \in E$ and $\{\sigma_1(\alpha), \dots, \sigma_r(\alpha)\}$ be a maximal set of distinct conjugates of α where $\sigma_i \in H$. Then $\sigma_1(\alpha) + \dots + \sigma_r(\alpha) \in E_H$ and so is $\sigma_1(\alpha) \cdots \sigma_r(\alpha)$.

Proof: Let $\tau \in H$. Then $\tau(\sigma_1(\alpha) + \dots + \sigma_r(\alpha)) = \tau\sigma_1(\alpha) + \dots + \tau\sigma_r(\alpha)$. Also, since τ is injective, we have that $\tau\sigma_i(\alpha) \neq \tau\sigma_j(\alpha)$ for all $i \neq j$. As $\tau \in H$, and $\sigma_i \in H$, we have that $\tau\sigma \in H$. Then the above list $\{\tau\sigma_1(\alpha), \dots, \tau\sigma_r(\alpha)\}$ is a permutation of $\{\sigma_1(\alpha), \dots, \sigma_r(\alpha)\}$. Therefore, the sum and the product are fixed by τ and hence in E_H .

Theorem: Let ω be a primitive n th root of unity over \mathbb{Q} . Then $\text{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \cong \mathbb{Z}_n^\times$.

Proof: If $[i]_n \in \mathbb{Z}_n^\times$, define $\psi([i]_n) = \sigma_i$ where $\sigma_i : \mathbb{Q}(\omega) \rightarrow \mathbb{Q}(\omega)$ sends ω to ω^i . This is clearly an isomorphism.

Example: Let ω be a primitive n th root of unity. Thus by the above theorem, $\text{Gal}(E/\mathbb{Q}) \cong \mathbb{Z}_{11}^\times$, where $E = \mathbb{Q}(\omega)$. Now $\mathbb{Z}_{11}^\times = \langle 2 \rangle$. Therefore $G = \langle \sigma \rangle$ where $\sigma : \mathbb{Q}(\omega) \rightarrow \mathbb{Q}(\omega)$ sends ω to ω^2 . The subgroup lattice for G is below:



Note that in the above correspondence $\sigma^j \in G \longleftrightarrow 2^j \in \mathbb{Z}_{11}^\times$. By the proposition applied to $\langle \sigma^5 \rangle = \{1, \sigma^5\}$, we have that $\omega + \omega^{10} \in E_{\langle \sigma^5 \rangle}$. So, we know that $\mathbb{Q}(\omega + \omega^{10}) \subseteq E_{\langle \sigma^5 \rangle}$. Since 5 is prime, we only need to check if $\omega + \omega^{10} \in \mathbb{Q}$. Suppose that $\omega + \omega^{10} = q \in \mathbb{Q}$. Then ω is a root of $x^{10} + x - q \in \mathbb{Q}[x]$. But we know that $\text{Irr}(\omega, \mathbb{Q}) = x^{10} + x^9 + \dots + x + 1$ which does not divide $x^{10} + x - q$. So $\omega + \omega^{10} \notin \mathbb{Q}$, and hence $\mathbb{Q}(\omega + \omega^{10}) = E_{\langle \sigma^5 \rangle}$. Now consider $\langle \sigma^2 \rangle = \{1, \sigma^2, \sigma^4, \sigma^6, \sigma^8\}$. Note that the complete set of conjugates of ω in this group are $\omega, \omega^4, \omega^5, \omega^9$, and ω^3 (listed in the same order as the σ s above). Therefore, $\beta = \omega + \omega^3 + \omega^4 + \omega^5 + \omega^9 \in E_{\langle \sigma^2 \rangle}$. By a similar argument as above $\beta \notin \mathbb{Q}$ and hence $\mathbb{Q}(\beta) = E_{\langle \sigma^2 \rangle}$.

Definition: An algebraic extension E/F is called abelian (resp. cyclic) if E/F is Galois and $\text{Gal}(E/F)$ is abelian (resp. cyclic).

Theorem: Let E/F be a finite Galois extension and L an intermediate field. Let $G = \text{Gal}(E/F)$ and $H = \text{Gal}(E/L)$. Then

1. L/F is normal $\Leftrightarrow H \triangleleft G$.
2. If L/F is normal then $\text{Gal}(L/F) \cong G/H$ (note that we always have that $[L : F] = [G : H]$).

Proof: Suppose that L/F is normal. Define a map

$$\begin{aligned} \phi : G &\rightarrow \text{Gal}(L/F) \\ \sigma &\longmapsto \sigma|_L \end{aligned}$$

Then ϕ is a group homomorphism. Furthermore, any $\tau \in \text{Gal}(L/F)$ can be extended to a $\sigma \in G$ and $\sigma|_L = \tau$. Therefore ϕ is surjective. Furthermore, we have that $\sigma \in \ker \phi \Leftrightarrow \sigma|_L = \text{Id}_L \Leftrightarrow \sigma \in H$. Hence H is the kernel, hence normal in G , and so $\text{Gal}(L/F) \cong G/H$. Now, for the reverse direction, suppose that $H \triangleleft G$. Let $\psi : L \rightarrow \bar{F}$ be a map which fixes F . Let $\alpha \in L$. It is enough to show that $\psi(\alpha) \in L$. Extend ψ to $\sigma \in G$. Now it is enough to show that $\sigma(\alpha) \in L$. Now $L = E_H$, so it is enough to show that $h(\sigma(\alpha)) = \sigma(\alpha)$ for all $h \in H$. So, let $h \in H$. Then $\sigma^{-1}h\sigma \in H$ as $H \triangleleft G$. Thus, if $\alpha \in L$, we have that $\sigma^{-1}h\sigma(\alpha) = \alpha$. Therefore, $h(\sigma(\alpha)) = \sigma(\alpha)$. Hence $\sigma(\alpha) \in E_H = L$, as desired.

Theorem: Let E/F be a finite extension where F is a finite field. Then $\text{Gal}(E/F)$ is cyclic.

Proof: Let $p = \text{Char } F$. Then we have the tower of fields

$$\begin{array}{c} E \\ \downarrow \text{finite} \\ F \\ \downarrow \text{finite} \\ \mathbb{Z}_p \end{array} \quad \begin{array}{c} \curvearrowright \\ \text{finite} \\ \curvearrowleft \end{array}$$

Note that $\text{Gal}(E/F)$ is a subgroup of $\text{Gal}(E/\mathbb{Z}_p)$. Therefore, it is enough to show that $\text{Gal}(E/\mathbb{Z}_p)$ is cyclic. Let $n = [E : \mathbb{Z}_p]$. Then E is the splitting field of $x^{p^n} - x$ over \mathbb{Z}_p . Let $\sigma : E \rightarrow E$ be the automorphism of E that sends $a \in E$ to a^p . Note that this automorphism fixes \mathbb{Z}_p . Therefore, we have that $\sigma \in \text{Gal}(E/\mathbb{Z}_p)$ so it is enough to show that it has order n . Suppose that $\sigma^k = 1$ for some $k < n$. Then $a^{p^k} = a$ for all $a \in E$. Hence $x^{p^k} - x$ has p^n roots, a contradiction as $p^n > p^k$. Thus, $k = n$ and $\text{Gal}(E/\mathbb{Z}_p) = \langle \sigma \rangle$.

Lemma: Suppose that E/\mathbb{R} is a proper finite extension. Then $2 \mid [E : \mathbb{R}]$.

Proof: Suppose not. Let $\alpha \in E \setminus \mathbb{R}$, and let $f(x) = \text{Irr}(\alpha, \mathbb{R})$. Assume that $[E : \mathbb{R}]$ is odd, and hence $\deg f(x)$ is odd. But $f(x)$ being of odd degree means that it must cross the x axis by the intermediate value theorem. Hence $f(x)$ has a real root, contradicting $f(x)$ being irreducible.

Lemma: If E/\mathbb{C} is a finite extension, then $[E : \mathbb{C}] \neq 2$.

Proof: Suppose that $[E : \mathbb{C}] = 2$. Then $E = \mathbb{C}(\alpha)$ for some $\alpha \in E$. Let $f(x) = x^2 + bx + c = \text{Irr}(\alpha, \mathbb{C})$. Thus

$$\begin{aligned} 0 &= \alpha^2 + b\alpha + c = \alpha^2 + b\alpha + \frac{b^2}{4} + c - \frac{b^2}{4} \\ &= \left(\alpha + \frac{b}{2}\right)^2 - \left(\frac{b^2}{4} - c\right) \\ &= \beta^2 - d \end{aligned}$$

where $\beta = \alpha + \frac{b}{2}$ and $d = \frac{b^2}{4} - c$. Note that $\mathbb{C}(\alpha) = \mathbb{C}(\beta)$ and $\text{Irr}(\beta, \mathbb{C}) = x^2 - d$. But let $d = re^{i\theta}$ where $r \in \mathbb{R}^{\geq 0}$. Then $\sqrt{r}e^{i\theta/2}$ is a root of $x^2 - d$, a contradiction (Here we use the fact that every positive real number has a real square root).

Fundamental Theorem Of Algebra: \mathbb{C} is algebraically closed.

Proof: Let α be an algebraic element over \mathbb{C} . Hence α is algebraic over \mathbb{R} . Let $f(x) = \text{Irr}(\alpha, \mathbb{R})$. Let E be the splitting field of $f(x)(x^2 + 1)$ over \mathbb{R} . Then E/\mathbb{R} is Galois and $\mathbb{C} \subseteq E$ and $\alpha \in E$. We wish to show that $E = \mathbb{C}$. Let $G = \text{Gal}(E/\mathbb{R})$. By lemma 1, $2 \mid |G|$. Let H be a Sylow 2-subgroup of G and let $L = E_H$. Then $[L : \mathbb{R}] = [G : H]$. By lemma 1, $[L : \mathbb{R}]$ and hence $L = \mathbb{R}$ (because we have all the powers of 2 in L). Therefore $G = H$ and so $|G| = 2^n$. Let $P = \text{Gal}(E/\mathbb{C})$. Then $|P| = 2^{n-1}$, since $[E : \mathbb{C}] = \frac{[E:\mathbb{R}]}{[\mathbb{C}:\mathbb{R}]}$. If $P \neq \{1\}$, by Sylow, there exists a subgroup Q of P of order 2^{n-2} . But then $[E_Q : \mathbb{C}] = 2$, contradicting lemma 2. Hence $P = \{1\}$. Therefore, $n = 1$ and $|G| = 2$, so that $E = \mathbb{C}$.

Definition: Let $f(x) \in F[x]$ whose irreducible factors over F are separable. The Galois group of $f(x)$ over F , denoted $\text{Gal}_F(f)$ is $\text{Gal}(E/F)$ where E is the splitting field of $f(x)$ over F .

Remark: We've shown that if $\deg f = n$, then $\text{Gal}_F(f)$ is isomorphic to a subgroup of S_n . When can $\text{Gal}_F(f) \cong S_n$?

Lemma: Let p be a prime and H a subgroup of S_p which contains a transposition and a p -cycle. Then $H = S_p$. (Note that S_n is always generated by $(1\ 2)$ and $(1\ 2\ \dots\ n)$).

Proof: Let $\tau \in H$ be a transposition. We can assume $\tau = (1\ 2)$. Let $\sigma \in H$ be a p -cycle. As $|\sigma^i| = p$ for any $1 \leq i \leq p-1$ and any element of order p in S_p is a p -cycle, we get that σ^i is a p -cycle for all $i \in \{1, \dots, p-1\}$. Consider $S = \{\sigma(1), \sigma^2(1), \dots, \sigma^p(1)\}$. I claim that $|S| = p$. If not, then $\sigma^i(1) = \sigma^j(1)$ for some $i > j$ and hence $\sigma^{i-j}(1) = 1$, a contradiction as σ^{i-j} is a p -cycle. As $|S| = p$, $2 \in S$, i.e. there exists an i such that $\sigma_i(1) = 2$. Replacing σ by σ_i , we can assume that $\sigma = (1\ 2\ 3\ \dots\ p)$. Note that $\sigma(1\ 2)\sigma^{-1} = (2\ 3) \in H$. In general, we have that $\sigma(i-1\ i)\sigma^{-1} = (i\ i+1)$. Hence we have that $H = S_p$.

Theorem: Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of degree p a prime and suppose f has exactly 2 real non-real roots. Then $\text{Gal}_{\mathbb{Q}}(f) \cong S_p$.

Proof: We've shown that $G \cong \text{Gal}_{\mathbb{Q}}(f)$ is isomorphic to a subgroup of S_p . Let E be the splitting field of $f(x)$ and let $\sigma : E \rightarrow E$ be given by complex conjugation. Let $\alpha_1, \dots, \alpha_n$ be the roots of $f(x)$ and say α_1, α_2 are the non-real roots. Then $\sigma(\alpha_1) = \alpha_2$, $\sigma(\alpha_2) = \alpha_1$, and $\sigma(\alpha_i) = \alpha_i$ for all $i \neq 1, 2$. Hence σ is a transposition. So, note that $[\mathbb{Q}(\alpha_1) : \mathbb{Q}] = p$ since $\deg f = p$ and f was irreducible. Therefore, $p \mid [E : \mathbb{Q}] = |G|$. Hence G has an element of order p . However, the only elements of order p in S_p are p -cycles since p is prime. Therefore, by the previous lemma, we have that $G = S_p$.

Example: Let $f(x) = x^5 - 2x^3 - 8x - 2$. Then $f(x)$ is irreducible by Eisenstein. Note that $f'(x) = (5x^2 + 4)(x^2 - 2)$ so that $f(x)$ has exactly three real roots and two complex roots. Therefore, by the above theorem, we have that $\text{Gal}_{\mathbb{Q}}(f) = S_5$.

Definition: Let K be a field and t_1, \dots, t_n be indeterminants over K . Then the general equation of degree n over K is

$$f_n(x) = x^n + t_1x^{n-1} + \dots + t_{n-1}x + t_n$$

So, what is $\text{Gal}_{K(t_1, \dots, t_n)}(f_n)$. (My guess was S_n).

Definition: Let K be a field and t_1, \dots, t_n be indeterminants over K . Let $F = K(t_1, \dots, t_n)$. For each permutation $\sigma \in S_n$, define a map

$$\begin{aligned} \tilde{\sigma} : F &\rightarrow F \\ \frac{p(t_1, \dots, t_n)}{q(t_1, \dots, t_n)} &\mapsto \frac{p(t_{\sigma(1)}, \dots, t_{\sigma(n)})}{q(t_{\sigma(1)}, \dots, t_{\sigma(n)})} \end{aligned}$$

For example, if $n = 3$ and $\sigma = (1\ 2\ 3)$, then $\tilde{\sigma} \left(\frac{2x_1^2x_2 - x_3^3}{x_2x_3 + 5x_2} \right) = \frac{2x_2^2x_3 - x_1^3}{x_3x_1 + 5x_3}$. Then $\tilde{\sigma}$ are automorphisms of F (check this!). In this way, we can think of S_n to be a group of automorphisms of F that fix K . Let $L = F_{S_n}$ be the fixed field of S_n . Things that are in L are $x_1x_2 \cdots x_n$, $x_1 + x_2 + \dots + x_n$, and generally $\sum_{i < j} x_i x_j$ (in fact, these generate L over K). L is called the **field of symmetric rational functions**. Note that by Artin's Theorem, $[F : F_{S_n}] = |S_n| = n!$. Also, F/L is Galois and $\text{Gal}(F/L) \cong S_n$.

To investigate the elements of L , let $f(x) = \prod_{i=1}^n (x - t_i) \in F[x]$. For $\sigma \in S_n$, $f_\sigma(x) = \prod_{i=1}^n (x - t_{\sigma(i)}) = f(x)$. Hence $f(x) \in L[x]$. Writing out what $f(x)$ is, we have

$$f(x) = x^n - s_1x^{n-1} + s_2x^{n-2} + \dots + (-1)^n s_n$$

where $s_1 = t_1 + \dots + t_n$, $s_2 = \sum_{i < j} t_i t_j$, etc. s_i is called the **i th elementary symmetric polynomial** and $s_i \in L$.

Theorem: $L = K(s_1, \dots, s_n)$.

Proof: Note that we have the diagram:

$$\begin{array}{c} F \\ \left| \vphantom{F} \right. \\ n! \\ L \\ \left| \vphantom{L} \right. \\ K(s_1, \dots, s_n) \end{array}$$

So, it is enough to show that $[F : K(s_1, \dots, s_n)] \leq n!$. Note that F is the splitting field for $f(x)$ over $K(s_1, \dots, s_n)$. Hence, as $f(x)$ has degree n , the splitting field has degree at most $n!$ over $K(s_1, \dots, s_n)$, as desired.

Corollary: Let $F = K(t_1, \dots, t_n)$, where the t_i are indeterminants over K . Let s_i be the i th elementary symmetric polynomial in the t s. Then $F/K(s_1, \dots, s_n)$ is Galois and $\text{Gal}(F/K(s_1, \dots, s_n)) \cong S_n$.

Theorem: Let $F = K(t_1, \dots, t_n)$ where t_i are indeterminants over K and let $f(x) = x^n + t_1x^{n-1} + \dots + t_{n-1}x + t_n$ be the general equation of degree n . Then $\text{Gal}_F(f) \cong S_n$.

Proof: Let E be the splitting field for $f(x)$ over F , and let y_1, \dots, y_n be the roots of $f(x)$ in E . So, $E = F(y_1, \dots, y_n)$, and $f(x) = \prod_{i=1}^n (x - y_i) \in E[x]$. Note that $t_i = (-1)^i s_i(y_1, \dots, y_n)$. Consider the

following diagram (where the x_i are indeterminants over K , and the s_i are the elementary symmetric polynomials in the x 's, notation is our worst enemy on this problem):

$$\begin{array}{ccc} K[x_1, \dots, x_n] & \xrightarrow{\tau} & K[y_1, \dots, y_n] \\ \left| \right. & & \left| \right. \\ K[s_1, \dots, s_n] & \xleftarrow{\pi} & K[t_1, \dots, t_n] \end{array}$$

Where π sends t_i to $(-1)^i s_i$ and τ sends y_1 to x_i . Let $p(\underline{t}) \in K[\underline{t}]$. Then we have that $\tau\pi(p(\underline{t})) = \tau(p(-s_i(\underline{x}), \dots, (-1)^n s_i(\underline{x}))) = p(-s_i(\underline{y}), \dots, (-1)^n s_i(\underline{y})) = p(\underline{t})$. Hence, $\tau\pi = \text{Id}_{K[t_1, \dots, t_n]}$, and therefore π is 1-1 hence an isomorphism (as it is clearly surjective). Therefore, the induced map on quotient fields (say \tilde{p}) is also an isomorphism. Recall that $E = K(y_1, \dots, y_n) = F(y_1, \dots, y_n)$ is the splitting field for $f(x)$ over $K(t_1, \dots, t_n)$. But $K(x_1, \dots, x_n)$ is the splitting field for $f^{\tilde{p}}(x)$, as the x_i were the roots of the symmetric polynomial. In summary, we have the picture

$$\begin{array}{ccc} K(x_1, \dots, x_n) & \xrightarrow{\tau} & K(y_1, \dots, y_n) \\ \left| \right. & & \left| \right. \\ K(s_1, \dots, s_n) & \xleftarrow{\tilde{\pi}} & K(t_1, \dots, t_n) \end{array}$$

Where the vertical containments are splitting fields of the aforementioned polynomials. So, by the uniqueness of splitting fields, there exists the isomorphism τ as above. Therefore, we have that $\text{Gal}_F(f(x)) = \text{Gal}(K(y_1, \dots, y_n)/K(t_1, \dots, t_n)) \cong \text{Gal}(K(x_1, \dots, x_n)/K(s_1, \dots, s_n)) \cong S_n$ where the last isomorphism is given by the previous theorem.

Definition: Let E/F be a finite field extension, and let $\sigma_1, \dots, \sigma_r$ be the distinct embeddings of E into \bar{F} fixing F (so $r = [E : F]_s$). Define

$$N_F^E(\alpha) := \left(\sigma_1(\alpha) \cdots \sigma_r(\alpha) \right)^{[E:F]_i}$$

$$Tr_F^E(\alpha) := [E : F]_i \left(\sigma_1(\alpha) \cdots \sigma_r(\alpha) \right)$$

to be the **norm** and **trace** of α respectively.

Examples:

1. Let $E = \mathbb{Q}(\sqrt{2})$. Then $1 : E \rightarrow E$ and $\sigma : E \rightarrow E$, where $\sigma(\sqrt{2}) = -\sqrt{2}$ are the distinct \mathbb{Q} embeddings of E into \bar{F} . Then $N_{\mathbb{Q}}^E(a + b\sqrt{2}) = (a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2 \in \mathbb{Q}$, and $Tr_{\mathbb{Q}}^E = ((a + b\sqrt{2}) + (a - b\sqrt{2})) = 2a \in \mathbb{Q}$.
2. Let $F = \mathbb{Z}_p(t)$, where t is an indeterminant and p a prime. Let $f(x) = x^p - t \in F[x]$. Let E be the splitting field for $f(x)$ over F . Let $\alpha \in E$ be a root of $f(x)$. Then $\alpha^p = t$ and $f(x) = (x - \alpha)^p$ in $E[x]$. Hence $E = F(\alpha)$ and E/F is purely inseparable. Hence $[E : F]_i = [E : F] = p$ and $[E : F]_s = 1$. As $[E : F]_s = 1$, for $\beta \in E$, $N_F^E(\beta) = \beta^p$ and $Tr_F^E = p\beta = 0$. Hence, in this case, trace is degenerate.

Remark: If E/F is inseparable, then $[E : F]_i = p^k$, and hence $Tr_F^E(\beta) = 0$, so trace id degenerate for inseparable extensions. We will see later that it is nondegenerate for separable extensions.

Theorem: Let E/F be a finite extension. Let $N = N_F^E$ and $Tr = Tr_F^E$. Then for all $\alpha \in E$, we have that $N(\alpha) \in F$ and $Tr(\alpha) \in F$.

Proof: First, suppose that E/F is separable. Let $\{\sigma_1, \dots, \sigma_r\}$ be the distinct embeddings of E into \bar{F} fixing F . Let L be the normal closure of E/F . So L/F is Galois, and since we may think of the σ_i as maps from L into \bar{F} fixing F , we know that σ_i actually take values in L . Note also that for the same reason, we have that for any $\phi \in \text{Gal}(L/F)$, we have that $\{\phi\sigma_1, \dots, \phi\sigma_r\} = \{\sigma_1, \dots, \sigma_r\}$. So, let $\alpha \in E$. Then $\phi(N(\alpha)) = \phi(\sigma_1(\alpha) \cdots \sigma_r(\alpha)) = \phi\sigma_1(\alpha) \cdots \phi\sigma_r(\alpha) = N(\alpha)$ by the previous remark. Hence $N(\alpha)$ is in the fixed field of the Galois group, and hence in F . Note that the proof for $Tr(\alpha)$ works the same way. Now, let E/F be an arbitrary finite extension. Let $T = \{\alpha \in E \mid \alpha \text{ is separable over } F\}$. Let $\alpha \in E$. Note that $[F(\alpha) : F]_i \leq [E : F]_i$ and if $p^l = [E : F]_i$, then α^{p^l} is separable by the major proposition above on separability, and hence in T . Let $\{\sigma_1, \dots, \sigma_r\}$ be the distinct F -embeddings of T into \bar{F} . Then $\{\sigma_1|_T, \dots, \sigma_r|_T\}$ are the distinct F -embeddings of T into \bar{F} . Indeed, we have that $[E : F]_s = [T : F]_s$ as E/T is purely inseparable by construction. Then

$$\begin{aligned} N_F^E(\alpha) &= (\sigma_1(\alpha) \cdots \sigma_r(\alpha))^{[E:F]_i} \\ &= \sigma_1(\alpha^{[E:F]_i}) \cdots \sigma_r(\alpha^{[E:F]_i}) \\ &= N_T^E(\alpha^{[E:F]_i}) \end{aligned}$$

which is in F by the separable case above, since T/F was separable by construction. The trace again works the same way.

Properties of Norm and Trace: Let E/F be a finite extension and let $N = N_F^E$ and $Tr = Tr_F^E$. Then

1. For all $\alpha, \beta \in E$, we have that $N(\alpha\beta) = N(\alpha)N(\beta)$ and $Tr(\alpha + \beta) = Tr(\alpha) + Tr(\beta)$.
2. If $\alpha \in F$, then $N(\alpha) = \alpha^{[E:F]}$ and $Tr(\alpha) = [E:F]\alpha$.
3. If L is an intermediate field of E/F then $N_F^L \circ N_L^E = N_F^E$ and similarly for trace.

Proof: The proof of these results are an easy exercise.

Remark:

1. If $\alpha \in E \setminus \{0\}$, then $N(\alpha) \neq 0$, so $N_F^E : E^\times \rightarrow F^\times$ is a group homomorphism.
2. Similarly, $Tr_F^E : E \rightarrow F$ is a homomorphism of additive groups. Moreover, if $c \in F$, then $Tr_F^E(c\alpha) = cTr_F^E(\alpha)$, i.e. it is a linear functional on the F -vector space E .

Lemma: Let E/F be a field extension and $\{\sigma_1, \dots, \sigma_r\}$ distinct embeddings of E into L , where L is any field containing E . Then $\{\sigma_1, \dots, \sigma_r\}$ are linearly independent over F .

Proof: We induct on n with the case $n = 1$ being trivial. Suppose $n = 1$ and suppose that there exists $a_1, \dots, a_r \in F$ not all zero such that $a_1\sigma_1 + \cdots + a_r\sigma_r = 0$. As the lemma is true by induction for $\leq n-1$, we must have that all the a_i are nonzero. Let $\beta \in E$ such that $\sigma_1(\beta) \neq \sigma_2(\beta)$. Then for all $\alpha \in E$, we have that

$$a_1\sigma(\beta\alpha) + a_2\sigma_2(\beta\alpha) + \cdots + a_r\sigma_r(\beta\alpha) = 0$$

and hence

$$a_1\sigma(\beta)\sigma_1(\alpha) + a_2\sigma_2(\beta)\sigma_2(\alpha) + \cdots + a_r\sigma_r(\beta)\sigma_r(\alpha) = 0$$

therefore

$$a_1\sigma(\beta)\sigma_1 + a_2\sigma_2(\beta)\sigma_2 + \cdots + a_r\sigma_r(\beta)\sigma_r = 0$$

Now dividing by $\sigma_1(\beta)$ we have

$$a_1\sigma_1 + a_2\frac{\sigma_2(\beta)}{\sigma_1(\beta)}\sigma_2 + \cdots + a_r\frac{\sigma_r(\beta)}{\sigma_1(\beta)}\sigma_r = 0$$

Subtracting this from the above equation gives

$$a_2\left(1 - \frac{\sigma_2(\beta)}{\sigma_1(\beta)}\right)\sigma_2 + \cdots + a_r\left(1 - \frac{\sigma_r(\beta)}{\sigma_1(\beta)}\right)\sigma_r = 0$$

However, as $\sigma_1(\beta) \neq \sigma_2(\beta)$, $\left(1 - \frac{\sigma_2(\beta)}{\sigma_1(\beta)}\right) \neq 0$ and $a_2 \neq 0$ by assumption. This contradicts our induction hypothesis.

Corollary: Let E/F be a separable extension. Then $Tr_F^E \neq 0$.

Proof: Note that $Tr_F^E = \sigma_1 + \sigma_r$ where $\{\sigma_1, \dots, \sigma_r\}$ is the set of distinct F embeddings of E into \bar{F} . Thus by the above theorem it is non-zero.

Hilbert's Satz 90: Let E/F be a finite cyclic extension and $\text{Gal}(E/F) = \langle \sigma \rangle$. Then $N_F^E(\beta) = 1 \Leftrightarrow \beta = \frac{\alpha}{\sigma(\alpha)}$ for some $\alpha \in E$.

Proof: Let $|\sigma| = n$, so that $\sigma^n = 1$. First suppose that $\beta = \frac{\alpha}{\sigma(\alpha)}$. Then

$$\begin{aligned} N_F^E(\beta) &= \beta\sigma(\beta) \cdots \sigma^{n-1}(\beta) \\ &= \frac{\alpha}{\sigma(\alpha)} \sigma\left(\frac{\alpha}{\sigma(\alpha)}\right) \sigma^{n-1}\left(\frac{\alpha}{\sigma(\alpha)}\right) \\ &= \frac{\alpha}{\sigma(\alpha)} \frac{\sigma(\alpha)}{\sigma^2(\alpha)} \cdots \frac{\sigma^{n-1}(\alpha)}{\sigma^n(\alpha)} \end{aligned}$$

But $\sigma^n(\alpha) = \alpha$, and hence the above expression is 1. For the reverse direction, suppose that $N(\beta) = 1$. By the lemma on embeddings, we know that $\{1, \sigma, \sigma^2, \dots, \sigma^{n-1}\}$ is linearly independent over F . Let $g = 1 + \beta\sigma + (\beta\sigma(\beta))\sigma^2 + \cdots + (\beta\sigma(\beta)\sigma^2(\beta) \cdots \sigma^{n-2}(\beta))\sigma^{n-1}$. Then $g \neq 0$. So, choose $u \in E$ such that $g(u) \neq 0$, and let $\alpha = g(u)$. Then we have

$$\begin{aligned} \beta\sigma(\alpha) &= \beta\sigma(u + \beta\sigma(u) + (\beta\sigma(\beta))\sigma^2(u) + \cdots + (\beta\sigma(\beta)\sigma^2(\beta) \cdots \sigma^{n-2}(\beta))\sigma^{n-1}(u)) \\ &= \beta\sigma(u) + \beta\sigma(\beta)\sigma^2(u) + \cdots + (\beta\sigma(\beta)\sigma^2(\beta) \cdots \sigma^{n-1}(\beta))u \end{aligned}$$

But as $(\beta\sigma(\beta)\sigma^2(\beta) \cdots \sigma^{n-2}(\beta)) = N_F^E(\beta) = 1$, we have

$$\begin{aligned} &= u + \beta\sigma(u) + \beta\sigma(\beta)\sigma^2(u) + \cdots + (\beta\sigma(\beta)\sigma^2(\beta) \cdots \sigma^{n-2}(\beta))\sigma^{n-1}(u) \\ &= g(u) = \alpha \end{aligned}$$

Hence $\beta = \frac{\alpha}{\sigma(\alpha)}$, as desired.

Additive Version of Hilbert's Satz 90: Let E/F be a finite cyclic extension, and $\text{Gal}(E/F) = \langle \sigma \rangle$. Then $\text{Tr}_{\bar{F}}^E(\beta) = 0 \Leftrightarrow \beta = \alpha - \sigma(\alpha)$ for some $\alpha \in E$. Read in Lang or try mimicing the proof above.

Note: Let F be a field and \bar{F} its algebraic closure. Then the roots of $x^n - 1$ form a finite subgroup of \bar{F}^\times . Such subgroups are cyclic. A **primitive n th root of unity over F** is a cyclic generator for this subgroup.

Theorem: Let E/F be a finite extension and suppose that F contains a primitive n th root of unity, where $\text{Char } F \nmid n$. Then E/F is cyclic of degree $d \mid n \Leftrightarrow E = F(\alpha)$ where $\alpha^n \in F$.

Proof: For the forward direction, let ω be a primitive n th root of unity in F . Then $\zeta = \omega^{n/d}$ is a primitive d th root of unity. Certainly ζ^{-1} is in F , thus $N_{\bar{F}}^E(\zeta^{-1}) = (\zeta^{-1})^{[E:F]} = (\zeta^{-1})^d = 1$. Hence its in the kernel of the norm map. Therefore, $\zeta^{-1} = \frac{\alpha}{\sigma\alpha}$ for some $\alpha \in E$, where $\langle \sigma \rangle = \text{Gal}(E/F)$, by Satz 90. Therefore, $\sigma(\alpha) = \zeta\alpha$, and in general, we have that $\sigma^i(\alpha) = \zeta^i\alpha$. Hence, since $\alpha, \zeta\alpha, \dots, \zeta^{d-1}\alpha$ are distinct, we have that $[F(\alpha) : F]_s \geq d$. Thus, $[F(\alpha) : F] = d$, and thus $E = F(\alpha)$. Also, note that $\sigma(\alpha^d) = \sigma(\alpha)^d = (\zeta\alpha)^d = \alpha^d$, hence $\alpha^d \in E_{\langle \sigma \rangle} = F$, and hence $(\alpha^d)^{n/d} = \alpha^n \in F$.

For the reverse direction, Let $a = \alpha^n \in F$. Then α is a root of $x^n - a \in F[x]$. Since ω , a primitive n th root of unity, is in F , we have that $x^n - a$ splits in $F(\alpha) \in E$. So, E/F is normal, and since $\text{Char } F \nmid n$, $x^n - a$ is separable and so α is separable, and hence E/F is separable. Therefore E/F is Galois. Let $f(x) = \text{Irr}(\alpha, F)$. We know that $f(x) \mid x^n - a$. Let $\omega^{i_1}\alpha, \dots, \omega^{i_k}\alpha$ be the roots of $f(x)$. So $\sigma_{i_j} : F(\alpha) \rightarrow F(\alpha)$ sending α to $\omega^{i_j}\alpha$ is an automorphism of E fixing F . Then $\text{Gal}(E/F) = \{\sigma_{i_1}, \dots, \sigma_{i_k}\}$. Define

$$\phi : \text{Gal}(E/F) \rightarrow \{\omega^i \mid 0 \leq i \leq n-1\} \quad (\text{cyclic and isomorphic to } C_n)$$

$$\sigma_{i_j} \mapsto \omega^{i_j}$$

Then ϕ is an injective group homomorphism, and since subgroups of cyclic groups are cyclic, $\text{Gal}(E/F)$ is cyclic of order $d \mid n$ by Lagrange.

Recall the quadratic formula: The roots of $f(x) = ax^2 + bx + c \in K[x]$ are $x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$ if the characteristic of K is not 2, and where $\sqrt{b^2 - 4ac}$ is a root of $x^2 - (b^2 - 4ac)$. Thus, the roots of $f(x)$ lie in the field $K(\alpha)$ where α is a root of $x^2 - (b^2 - 4ac)$.

Also, note that Cardano in the 1500s found a formula to solve the general cubic. Indeed, let $f(x) = x^3 + ax^2 + bx + c \in K[x]$. Assume that $\text{Char } K \neq 2, 3$. Replacing x by $x - \frac{1}{3}a$, we may eliminate the x^2 term, so we may assume that $f(x) = x^3 + px + q$. Cardano's formula shows that the roots of $f(x)$ lie in the field $K(\omega, \delta, y_1, y_2)$ where ω is a primitive n th root of unity, $\delta = \sqrt{12pq + 81q^2}$ and $y_1, y_2 = \sqrt[3]{-\frac{27}{2}q \pm \frac{3}{2}\delta}$. So we have a tower of fields (called a root tower):

$$\begin{array}{c}
 E = K(\omega, \delta, y_1, y_2) = F_3(y_2) \\
 \left| \begin{array}{c} y_2^3 \in F_3 \\ F_3 = F_2(y_1) \end{array} \right. \\
 \left| \begin{array}{c} y_1^3 \in F_2 \\ F_2 = F_1(\delta) \end{array} \right. \\
 \left| \begin{array}{c} \delta^2 \in F_1 \\ F_1 = K(\omega) \end{array} \right. \\
 \left| \begin{array}{c} \omega^3 \in K \\ F_0 = K \end{array} \right.
 \end{array}$$

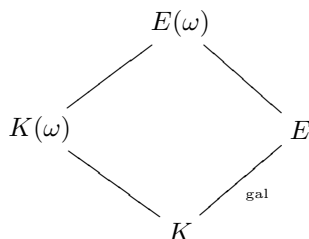
Definition: A finite extension E/K is called a **radical extension** if $\exists u_1, \dots, u_n$ such that for each i $\exists n_i$ with $u_i^{n_i} \in K(u_1, \dots, u_{i-1})$ and $E = K(u_1, \dots, u_n)$. The sequence

$$K \subseteq K(u_1) \subseteq K(u_1, u_2) \subseteq \dots \subseteq K(u_1, \dots, u_n) = E$$

is called a **root tower**. A polynomial in $K[x]$ is said to be **Solvable by Radicals** if $f(x)$ splits in some radical extension.

Theorem: Let $f(x) \in K[x]$ be a separable polynomial and E a splitting field for $f(x)$. Assume that $\text{Char } K \nmid [E : K]$. If $\text{Gal}_K(f(x))$ is solvable, then $f(x)$ is solvable by radicals.

Proof: Let $n = [E : K]$ and ω a primitive n th root of unity. Consider the diagram



By a homework exercise, $E(\omega)/K(\omega)$ is Galois. Furthermore, we have that $\text{Gal}(E(\omega)/K(\omega)) \cong$ a subgroup of $\text{Gal}(E/K)$. As subgroups of solvable groups are solvable, $\text{Gal}(E(\omega)/K(\omega))$ is solvable. If we show that $E(\omega)/K(\omega)$ is a radical extension, then certainly $E(\omega)/K$ is a radical extension, since adjoining ω is a radical extension. Of course f splits in $E(\omega)$ as it splits in E . Hence without loss of generality, we may replace K with $K(\omega)$ and assume K contains all the n th roots of unity. Also, $[E(\omega) : K(\omega)] = |\text{Gal}(E(\omega)/K(\omega))|$ which divides $|\text{Gal}(E/K)|$ by Lagrange. Hence $\text{Char } k \nmid [E(\omega) : K(\omega)]$. So, let $G = \text{Gal}(E/K)$. As G is solvable, there is a normal series

$$\{1\}G_t \triangleleft G_{t-1} \triangleleft \dots \triangleleft G_1 \triangleleft G_0 = G$$

with $G_i/G_{i+1} \cong C_{p_i}$ (the cyclic group on p_i elements). We may assume that we get cyclic groups since any refinement of a solvable series is solvable, and any composition series (i.e. a normal series that all the factor groups are simple) for a solvable group has factor groups that are cyclic of prime order. So we have the correspondence

$$\begin{array}{ccc}
 & \text{Group Side} & \text{Field Side} \\
 & & \\
 \{1\} & \longleftrightarrow & E = F_t \\
 \Delta & & \Big| \text{normal} \\
 G_{k-1} & \longleftrightarrow & F_{t-1} \\
 \Delta & & \Big| \text{normal} \\
 G_{k-2} & \longleftrightarrow & F_{t-2} \\
 \Delta & & \Big| \text{normal} \\
 \vdots & \longleftrightarrow & \vdots \\
 \Delta & & \Big| \text{normal} \\
 G_1 & \longleftrightarrow & F_1 \\
 \Delta & & \Big| \text{normal} \\
 G_0 & & F_0 = K
 \end{array}$$

Where the extensions are normal (and hence Galois) because the series of groups on the left are normal. So, F_i/F_{i-1} is Galois and $\text{Gal}(F_i/F_{i-1}) \cong G_i/G_{i-1} \cong C_{p_i}$ and K contains primitive p_i th roots of unity, ω^{n/p_i} . Note that $p_i \nmid [E : K]$ so $\text{Char } K \nmid p_i$. By the theorem on cyclic extensions, we have that $F_i = F_{i-1}(u)$ where $u^{p_i} \in F_{i-1}$. Hence the above is a root tower, and hence E/F is solvable by radicals.

Lemma: Let F/K be a finite radical extension and let E be the normal closure of F/K . Then E/K is radical.

Proof: $F = K(u_1, \dots, u_n)$ where $u_i^{n_i} \in K(u_1, \dots, u_{i-1})$ for some n_i . Let $\sigma_1, \dots, \sigma_m$ be the distinct embeddings of F into \bar{K} fixing K . Then $E = \sigma_1(F) \cdots \sigma_m(F)$ by a homework exercise. So, $E = K(\{\sigma_i(u_j)\})$. Note that since $u_i^{n_i} \in K(u_1, \dots, u_{i-1})$, $\sigma_j(u_i)^{n_i} = \sigma(u_i^{n_i}) \in K(\sigma_j(u_1), \dots, \sigma_j(u_{i-1}))$. Therefore E/K is radical (apply this to σ_1 and the u s. Next do it for σ_2 and continue up until m).

Theorem (Converse to the above theorem): Let K be a field and $f(x) \in K[x]$ be a separable polynomial. If $f(x)$ is solvable by radicals then $\text{Gal}_K(f(x))$ is solvable.

Proof: Let E be the splitting field of $f(x)$ over K . Then $E \subseteq F$ where F/K is a radical extension. By the lemma, we may assume that F/K is normal. Let $G = \text{Aut}(F/K)$. Want to show that $\text{Gal}(E/K)$ is solvable. There is a homomorphism $\phi : \text{Aut}(F/K) \rightarrow \text{Gal}(E/K)$ that sends $\psi \mapsto \psi|_E$. In fact, by the lifting property, ψ is surjective. So, $\text{Gal}(E/K) \cong G/\ker \psi$. Hence it is enough to show that G