MA542 Lecture Notes - Galoris Theory

Instructor: Tullia Dymarz   Note taken by: Yujia Bao

1 Field Extension

Recall A field E is a commutative ring with 1 s.t. $1 \neq 0$ and every nonzero element of E is a unit.

Example. $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}/p\mathbb{Z}$

A **subfield** of E is a subring that contains 1 and is closed under multiplicative inverses. So

1. $0 \in F$
2. $a \in F \Rightarrow -a \in F$
3. $a, b \in F \Rightarrow a + b, ab \in F$
4. $1 \in F$
5. $a \in F,\ a \neq 0 \Rightarrow a^{-1} \in F$

Note: A subfield is a field.

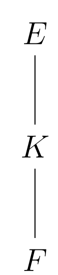
Definition (Extension)**.** Suppose F is a field. An extension of F is a field E which contains F as a subfield. We write E/F is an extension. (Let E/F be a field extension)

Example. $\mathbb{C}/\mathbb{Q}$ is an extension.

Basic problem: Given a field F what are its extensions?

Definition. Suppose E/F is an extension. A subring of E/F is a subring of E which contains F. A subfield of E/F is a subfield of E that contains F.

Definition (Diagram)**.** If K is a subfield of E/F, we draw



e.g. $\mathbb{C}/\mathbb{Q}$ contains $\mathbb{R}$ as a subfield. Because $\mathbb{C} \longrightarrow \mathbb{R} \longrightarrow \mathbb{Q}$.

Definition. Suppose E/F is an extension, and $F[S] = \{u_1, ..., u_r\} \subseteq E$, then

$$\begin{aligned} F[S] &= F[u_1, ..., u_r] \\ &= \text{ set of } F\text{-linear combinations of elements of the form } u_1^{i_1} \cdots u_r^{i_r}, \text{ where } i_j \geq 0 \\ F(S) &= \left\{ \frac{v}{w} \mid w, v \in F[S], w \neq 0 \right\} \end{aligned}$$

Recall: $F[\lambda]$-polynomials with coefficients in F

Clearly $F[S]$ is the smallest subring of E/F that contains S. And $F(S)$ is the smallest subfield containing S. We say $F[S]$ is the subring of E/F generated by S and $F(S)$ is the subfield generated by S.

Example. Consider E/F and let $u \in E$. Then

$$\begin{aligned} F[u] &= \left\{ a_0 + a_1 u + a_2 u^2 + \cdots + a_k u^k | a_i \in F, k \in \mathbb{N} \right\} \\ &= \{f(u) | f(\lambda) \in F[\lambda]\} \\ F(u) &= \left\{ \frac{f(u)}{g(u)} \mid f, g \in F[\lambda],\ g(u) \neq 0 \right\} \end{aligned}$$

Example. Consider $\mathbb{C}/\mathbb{Q}$, let $u = \sqrt{2}$.

$$\begin{aligned} \mathbb{Q}[\sqrt{2}] &= \left\{ a_0 + a_1\sqrt{2} + a_2(\sqrt{2})^2 + \cdots + a_k(\sqrt{2})^k \mid a_i \in \mathbb{Q} \right\} \\ &= \left\{ a_0' + a_1'\sqrt{2} \mid a_0', a_1' \in \mathbb{Q} \right\} \\ \mathbb{Q}(\sqrt{2}) &= \left\{ \frac{a_0 + a_1\sqrt{2}}{b_0 + b_1\sqrt{2}} \mid a_0, a_1, b_0, b_1 \in \mathbb{Q},\ b_0 + b_1\sqrt{2} \neq 0 \right\} \\ &= \left\{ c_0 + c_1\sqrt{2} \mid c_0, c_1 \in \mathbb{Q} \right\} \\ &= \mathbb{Q}[\sqrt{2}] \end{aligned}$$

Question: When is $F(u) = F[u]$?

Definition. Suppose E/F is an extension and $f(\lambda) \in F[\lambda]$. A root of $f(\lambda)$ in E is an element $u \in E$ s.t. $f(u) = 0$.

Definition. We say that u is algebraic over F if it is the root of some nonzero polynomial in $F[\lambda]$. Otherwise we say u is transcendental over F.

Example. Consider $\mathbb{C}/\mathbb{Q}$. Let $u = \sqrt[3]{5}$, then u is a root of $\lambda^3 = 5$. So u is algebraic over $\mathbb{Q}$.

Definition (Minimal Polynomial)**.** Suppose E/F is an extension. Let $u \in E$ be an element that is algebraic over F. Let

$$I = \{f(\lambda) \in F[\lambda] \mid f(u) = 0\}$$

Then I is an ideal over the ring of polynomials and $I \neq \{0\}$ since u is algebraic over F. So $I = (m(\lambda))$ since $F[\lambda]$ is a PID where $m(\lambda)$ is a monic polynomial of degree ≥ 1. $m(\lambda)$ is called the minimal polynomial of u over F (Note $m(u) = 0$ by definition)

Note, if $f(\lambda) \in F[\lambda]$, then $f(u) = 0$ if and only if $m(\lambda) \mid f(\lambda)$. So $m(\lambda)$ is the monic polynomial of smallest degree ≥ 1 over F which has u as a root.

Definition. Suppose E/F is an extension and $u \in E$ is algebraic over F. The degree of u over F is denoted by $\deg_F(u)$, which is the degree of the minimal polynomial $m(\lambda)$.

Proposition. Suppose E/F is an extension and $u \in E$ is algebraic over F. Then the minimal polynomial of u over F is the unique irreducible polynomial over F which has u as a root.

Proof. Let $m(\lambda)$ be the minimal polynomial of u over F. Suppose for contradiction

$$m(\lambda) = g(\lambda)h(\lambda)$$

where $g(\lambda), h(\lambda) \in F[\lambda]$ has smaller degree than $m(\lambda)$. Plug in u, then we have

$$0 = m(u) = h(u)g(u)$$

Since $g(u), h(u) \in E$ which is a field. So one of $g(u)$ or $h(u)$ is zero. Without loss of generality, $g(u) = 0$. But this contradicts that $m(\lambda)$ is the smallest degree polynomial with u as a root. Therefore $m(\lambda)$ is irreducible.

Now we show the uniqueness of $m(\lambda)$. Suppose p is another monic irreducible polynomial over F that has root u. Then we know $m(\lambda) \mid p(\lambda)$ since it has u as a root which implies $p(\lambda) \in (m(\lambda))$. Since $p(\lambda)$ is irreducible, it follows that either $m(\lambda) = 1$ or $p(\lambda)$. Since the degree of $m(\lambda)$ is at least 1. So $m(\lambda) = p(\lambda)$. ☐

Example. Consider $u = \sqrt[3]{5}$ in $\mathbb{C}/\mathbb{Q}$. Then $\sqrt[3]{5}$ is root of $\lambda^3 - 5 \in \mathbb{Q}[\lambda]$. Using Eisenstein's criterion which is for $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$, where a_i are integers, if

1. p divides each a_i for $i \neq n$
2. p does not divide a_n and p^2 does not divide a_0

then $f(x)$ is irreducible over $\mathbb{Q}$.

Definition. Suppose E/F is an extension. Then E is a vector space over F. The vector space addition is the usual addition in E. The scalar multiplication is given by multiplication of elements of E by elements of F. The **degree** of E/F is the dimension of E as a vector space. Denote it by $[E : F]$.

If $[E : F]$ is infinite, we call the extension E/F infinite and write $[E : F] = \infty$. If $[E : F]$ is finite, we called E/F finite and write $[E : F] < \infty$.

Example. $\mathbb{C}/\mathbb{Q}$ is infinite extensions and $\mathbb{R}/\mathbb{Q}$ as well. So they have infinity degrees.

For $\mathbb{C}/\mathbb{R}$, $[\mathbb{C} : \mathbb{R}] = 2$ because $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$. The corresponding diagram is:

$$\begin{array}{c} \mathbb{C} \\ 2\Big| \\ \mathbb{R} \end{array}$$

Note: If $[E : F] = 1$, then $E = F$.

Proposition. Suppose that E/F is a field extension and $u \in E$ that is algebraic over F. Then

1. $F(u) = F[u]$
2. $\{1, u, ..., u^{n-1}\}$ is an F-basis (as a vector space over F) for $F(u)$ where $n = \deg_F(u)$. (The degree of u in terms of the minimal polynomial.)
3. $F(u)/F$ is a finite extension with $[F(u) : F] = \deg_F(u)$.

Proof. Let $m(\lambda)$ be the minimal polynomial of u over F, say $m(\lambda) = \lambda^n + a_{n-1}\lambda^{n-1} + \cdots + a_0$, $a_i \in F$. $n = \deg_F(u)$.

1. We must show that $\forall x \in F[u] \setminus \{0\} \Rightarrow x^{-1} \in F[u]$. So $x = f(u) \neq 0$ for some $f(\lambda) \in F[\lambda]$, $m(\lambda) \nmid f(\lambda)$ since $f(u) \neq 0$. Also $m(\lambda)$ is irreducible over F. Hence $\gcd(f(\lambda), m(\lambda)) = 1$. So $\exists s(\lambda), t(\lambda) \in F[\lambda]$ such that $s(\lambda)m(\lambda) + t(\lambda)f(\lambda) = 1$. Plug in u, we get $s(u)m(u) + t(u)f(u) = 1$. So we have $t(u) = x^{-1} \in F[u]$.

   Note: This shows how to find x^{-1}.

2. Since $F(u) = F[u]$, every element of $F(u)$ is a linear combination of $1, u, u^2, ...$ But $m(u) = 0$ which implies $u^n + a_{n-1}u^{n-1} + \cdots + a_0 = 0$. So u^n is a linear combination of $\{1, u, ..., u^{n-1}\}$. Hence by induction, u^k is a linear combination of $\{1, u, ..., u^{n-1}\}$ for $k \geq n$. Thus $\{1, u, ..., u^{n-1}\}$ spans $F(u)$. This is an independent set over F since u is not a root of non-zero polynomial over F of degree less than $n - 1$.

3. Follows from above. Think of this picture:

$$\begin{array}{c} E \\ \Big| \\ F(u) \\ \deg_F(u)\Big| \\ F \end{array}$$

□

Example. $u = \sqrt[3]{5}$ in $\mathbb{C}/\mathbb{Q}$. u has minimal polynomial $m(\lambda) = \lambda^3 - 5 \in \mathbb{Q}[\lambda]$. Thus $\deg_{\mathbb{Q}}(\sqrt[3]{5}) = 3$. $\mathbb{Q}[\sqrt[3]{5}] = \mathbb{Q}(\sqrt[3]{5})$ and basis for $\mathbb{Q}(\sqrt[3]{5})/\mathbb{Q}$ is $\{1, \sqrt[3]{5}, (\sqrt[3]{5})^2\}$. i.e. every element of $\mathbb{Q}(\sqrt[3]{5})$ can be written as $a_0 + a_1\sqrt[3]{5} + a_2(\sqrt[3]{5})^2$, $a_0, a_1, a_2 \in \mathbb{Q}$. Also $[\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}] = 3$.

ex: Find $(1 + 2\sqrt[3]{5} + 7(\sqrt[3]{5})^2)^{-1}$. (Write it in the form of $a_0 + a_1\sqrt[3]{5} + a_2(\sqrt[3]{5})^2$)

Proposition (Characterization of algebraic elements)**.** Suppose E/F and $u \in E$, then TFAE

1. u is algebraic over F.
2. $F(u) = F[u]$
3. $F(u)/F$ is finite. (The field extension is finite. No need of F being finite.)

Proof. We have $1) \Rightarrow 2), 1) \Rightarrow 3)$ from before. Now we proof $2) \Rightarrow 1)$ and $3) \Rightarrow 1)$.

'$2) \Rightarrow 1)$': Suppose $F(u) = F[u]$, then $F[u]$ is closed under inverses. Assume $u \neq 0$. (If $u = 0$, the minimal polynomial for u is $m(\lambda) = \lambda$)

So $u^{-1} = f(u) \in F[u]$. Then we have $u \cdot f(u) = 1$. Let $g(\lambda) = \lambda f(\lambda) - 1$. Then $g(\lambda) \in F[\lambda]$ with $g(u) = u \cdot f(u) - 1 = 0$. Hence u is algebraic over F.

'$3) \Rightarrow 1)$': Suppose $F(u)/F$ is finite. Let $n = [F(u) : F]$, then $\{1, u, u^2, ..., u^{n-1}, u^n\}$ has $n + 1$ elements and so is dependent. i.e. $0 = a_0 + a_1u + \cdots + a_nu^n$ where $a_i \in F$ not all zero. So u is the root of the polynomial $a_0 + a_1\lambda + \cdots + a_n\lambda^n$. $\square$

Example. We can show that π is transcendental, so $\mathbb{Q}(\pi) \neq \mathbb{Q}[\pi]$ and $\mathbb{Q}(\pi)/\mathbb{Q}$ is infinite.

Proposition (Multiplicativity of degree)**.** Suppose $K/E/F$ is a tower of extensions. Then

$$[K : F] < \infty \Longleftrightarrow [K : E] < \infty, [E : F] < \infty$$

Moreover, in this case we have

$$[K : F] = [K : E] \cdot [E : F]$$

And

$$\begin{array}{l} K \\ \big| \; [K : E] \\ E \\ \big| \; [E : F] \\ F \end{array}$$

So $[K : E] \mid [K : F]$ and $[E : F] \mid [K : F]$.

Proof. '$\Rightarrow$': If $[K : F] < \infty$, so K is a finite dimension vector space over F. But $F \subseteq E$, so any spanning set over F for K is also a spanning set over E for K. So $[K : E]$ is finite. Also since $E \subseteq K$, then E is a subspace of K over F and any subspace of a finite dimensional vector space is finite dimensional. So $[E:F]<\infty$.

'$\Leftarrow$': Suppose K/E, E/F are finite extensions. Let $\{u_1,...,u_n\}$ be a basis of K/E. Let $\{v_1,...v_s\}$ be a basis of E/F. We will show that $\{u_iv_j\}$, where $i=1,...,n; j=1,...,s$, is a basis for K/F. This will show K/F is finite and $[K:F]=[K:E]\cdot[E:F]=n\cdot s$.

Generation: Let $x\in K$ then $x=\sum_{i=1}^n e_iu_i$, $e_i\in E$. Since we can write $e_i=\sum_{i=1}^s a_{ij}v_j$, $a_{ij}\in F$, we have $x=\sum_{i=1}^n\sum_{j=1}^s a_{ij}(v_ju_i)$.

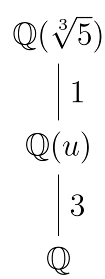
Independence: Suppose $\sum_{i=1}^n\sum_{j=1}^s a_{ij}(v_ju_i)=0$. Want to show that $a_{ij}=0$ for all i,j. Then we have $\sum_{i=1}^n(\sum_{j=1}^s a_{ij}v_j)u_i=0$. Since u_i are basis, so $\sum_{j=1}^s a_{ij}v_j=0$ for all i. By the independence of v_j, we get $a_{ij}=0$. Therefore it is independent. □

Corollary 1. Suppose K/F is finite. Let $u\in K$. Then u is algebraic over F and $\deg_F(u)\mid[K:F]$.

Proof. By theorem from last time, $F(u)/F$ is finite since K/F is finite. So u is algebraic. By the multiplicativity of degree, we get $[K:F]=[K:F(u)][F(u):F]$ and $\deg_F(u)=[F(u):F]$. So we have $\deg_F(u)\mid[K:F]$. □

Note: If $[F(u):F]=1$, then $u\in F$.

Example. $\mathbb{Q}(\sqrt[3]{5})/\mathbb{Q}$ is an extension of degree 3. Let $u=1+\sqrt[3]{5}-(\sqrt[3]{5})^2$. Then u is algebraic over $\mathbb{Q}$ and $\deg_{\mathbb{Q}}(u)$ is 1 or 3. Since u is not inside $\mathbb{Q}$ (u has a unique expression as $a_0\cdot 1+a_1\cdot\sqrt[3]{5}+a_2(\sqrt[3]{5})^2$), so $\deg_{\mathbb{Q}}(u)$ can only be 3.

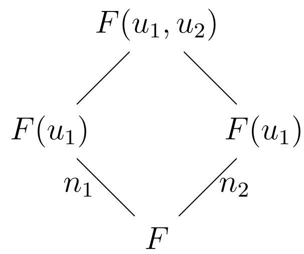


From the diagram, we see $\mathbb{Q}(u)=\mathbb{Q}(\sqrt[3]{5})$.

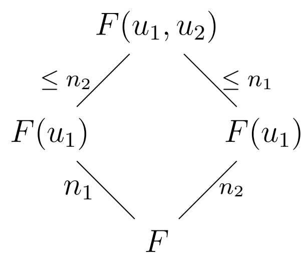
Proposition. Suppose $u_1,...,u_k$ are elements of some extension of F. Suppose u_i is algebraic over F with degree n_i, $i=1,...,k$. Then $F(u_1,...,u_k)/F$ is finite and $[F(u_1,...,u_k):F]\leq n_1n_2\cdots n_k$. Moreover if $n_1,...,n_k$ are pairwise relatively prime, then $[F(u_1,...,u_k):F]=n_1n_2\cdots n_k$.

Proof. Case $k=2$. ($k\geq 2$ follows similarly)

Suppose u_1,u_2 are algebraic with $\deg_F(u_1)=n_1$ and $deg_F(u_2)=n_2$. Then we have the following diagram



Notice that $F(u_1, u_2) = \{v/w \mid v, w \in F(u_1), w \neq 0\}$. But u_2 is a root of a polynomial over F of degree n_2. Thus (using the same polynomial) u_2 is a root of a polynomial with coefficients in $F(u_1)$ of deg n_2. Hence u_2 is algebraic over $F(u_1)$ with $deg_{F(u_1)}(u_2) \leq n_2$. (Minimal polynomial divides this polynomial!) Thus $F(u_1, u_2)/F(u_1)$ is finite of degree $\leq n_2$. So $F(u_1, u_2)/F$ is finite and $[F(u_1, u_2] : F] \leq n_1 n_2$

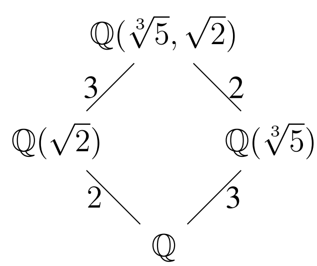


Now suppose $\gcd(n_1, n_2) = 1$. Since $n_1 \mid [F(u_1, u_2) : F]$ and $n_2 \mid [F(u_1, u_2) : F]$. So $\gcd(n_1, n_2) = 1$ implies $n_1 n_2 \mid [F(u_1, u_2) : F]$. Since $[F(u_1, u_2) : F] \leq n_1 n_2$, we must have equality. $\square$

Exercise. Suppose $u_1, ..., u_k$ are as in the proposition. Show that the elements of the form $u_1^{l_1} \cdots u_k^{l_k}$ with $0 \leq l_i \leq n_i - 1$ generate $F(u_1, ..., u_k)$ over F. Hence $F[u_1, ..., u_k] = F(u_1, ..., u_k)$.

Definition. Suppose $u_1, ..., u_k$ are elements of an extension E of F, then $F(u_1, ..., u_k)$ is called the subfield of E/F generated by $u_1, ..., u_k$. Also we can say the "extension of F generated by $u_1, ..., u_k$".

Example. Let $K = \mathbb{Q}(\sqrt[3]{5}, \sqrt{2})$ an extension of $\mathbb{Q}$ which is generated by $\sqrt[3]{5}$, $\sqrt{2}$. Then we have



Since $2, 3$ are relatively prime, we have $[\mathbb{Q}(\sqrt[3]{5}, \sqrt{2}) : \mathbb{Q}] = 6$. The generating set is given by

$$\left\{1, \sqrt[3]{5}, (\sqrt[3]{5})^2, \sqrt{2}, \sqrt[3]{5}\sqrt{2}, (\sqrt[3]{5})^2\sqrt{2}\right\}$$

This is actually a basis since the degree of the extension is 6.

Definition. Let p be a prime, $\mathbb{F}_p = \mathbb{Z}/(p) = \{\overline{0}, \overline{1}, ..., \overline{p-1}\}$ Since p is a prime, $\mathbb{F}_p$ is a field. By abuse of notation, we will drop the bars, $\mathbb{F}_p = \{0, 1, ..., p-1\}$.

Example. $\mathbb{F}_3 = \{0, 1, 2\}$. Let $f(\lambda) = \lambda^2 - 2 \in \mathbb{F}_3[\lambda]$. Check that this polynomial has no roots. $f(0) = -2 = 1, f(1) = -1 = 2, f(2) = 2$. So $f(\lambda)$ is irreducible over $\mathbb{F}_3$. (Since f is of degree 2 and has no roots.)

How to build an extension of $\mathbb{F}_3$ in which $\lambda^2 - 2$ ha a root?

In general, suppose $f(\lambda) \in F[\lambda]$ has degree ≥ 1 over $\mathbb{F}$. Can we construct an extension of F in which $f(\lambda)$ has a root? When we do this, we can assume that f is monic and irreducible. The field will be $F(r)$ where r is this root in some extension of F.

Proposition (Existense & Uniqueness of $F(r)$)**.** Suppose $p(\lambda)$ is an irreducible monic polynomial over F.

1. Suppose E/F is an extension such that $E = F(r)$ where r is a root of $p(\lambda)$. Then $E \simeq F[\lambda]/(p(\lambda))$. (Field extesion). In fact, $f(r) \in E = F(r)$ cooresponds to $f(\lambda) + (p(\lambda)) \in F[\lambda]/(p(\lambda))$.
2. Let $E = F[\lambda]/(p(\lambda))$ then E/F is an extension such that $E = F(r)$ for some root r of $p(\lambda)$ in E.

Proof. 1. Suppose E/F is an extension, so that $E = F(r)$ where r is root of $p(\lambda)$. Since $p(\lambda)$ is irreducible, we know it is the minimal polynomial of r. Hence $\{f(\lambda) \in F[\lambda] \mid f(r) = 0\} = (p(\lambda))$. Define $\varphi : F[\lambda] \to E$, such that $\varphi(f(\lambda)) = f(r)$. Check that this is a ring homomorphism. Note $\text{Ker}(\varphi) = (p(\lambda))$. Note φ is surjective since $\text{Im}(\varphi) = F[r] = F(r) = E$. (Because r is algebraic) By the first isomorphic theorem, we have $E \simeq F[\lambda]/(p(\lambda))$ with $f(r) \longleftrightarrow f(\lambda) + (p(\lambda))$.

2. Let $E = F[\lambda]/(p(\lambda))$. Then the elements of E can be written uniquely as

$$a_0 + a_1\lambda + \cdots + a_{n-1}\lambda^{n-1} + (p(\lambda))$$

where $n = \deg(p(\lambda))$, $a_i \in F$. Identify $a \in F$ with $a + (p(\lambda))$ (Isomorphism). Then F is a subfield of E so E/F is an extension. Let $r = \lambda + (p(\lambda))$. We can write the above form as following:

$$\begin{aligned} & a_0 + a_1\lambda + \cdots + a_{n-1}\lambda^{n-1} + (p(\lambda)) \\ &= (a_0 + (p(\lambda))) + (a_1 + (p(\lambda)))(\lambda + (p(\lambda))) + \cdots + (a_{n-1} + (p(\lambda)))(\lambda + (p(\lambda)))^{n-1} \\ &= a_0 + a_1 r + \cdots + a_{n-1} r^{n-1} \end{aligned}$$

So we have $E = F[r]$ and since E is a field, we have $E = F(r)$.

Claim r is a root of $p(\lambda)$. $p(r) = p(\lambda + (p(\lambda))) = p(\lambda) + (p(\lambda)) = 0 + (p(\lambda)) = 0 \in F$. So r is a root of $p(\lambda)$.

□

Example. $F = \mathbb{F}_3$ and $p(\lambda) = \lambda^2 - 2 \in \mathbb{F}_3[\lambda]$ (irreducible).

$E = F(\lambda)/(\lambda^2 - 2) = \{a_0 + a_1\lambda + (p(\lambda)) \mid a_0, a_1 \in \mathbb{F}_3\} = \{a_0 + a_1 r \mid a_0, a_1 \in \mathbb{F}_3\}$, where r is a root of $p(\lambda)$ in E, i.e. $r^2 - 2 = 0$.
Sample calculation: $(1 + 2r)(1 + 2r) = 1 + 4r + 4r^2 = 1 + r + r^2 = 1 + r + 2 = 3 + r = r$

The number of elements of E is 9. The degree of the extension E/F is 2 since $\deg(p(\lambda)) = 2$.

Example. Let $F = \mathbb{F}_5$ and $p(\lambda) = \lambda^3 + \lambda + 1$. Claim that $p(\lambda)$ is irreducible over $\mathbb{F}_5$. Let $E = F(r)$ where r is root of $p(\lambda)$. Then elements of E are uniquely written as $a_0 + a_1 r + a_2 r^2$. So $[E : F] = 3$.
Sample calculation: Use the fact that $r^3 + r + 1 = 0$, $r^3 = -r - 1 = 4r + 4$.

$(1 + r^2)^2 = 1 + 2r^2 + r^4 = 1 + 2r^2 + r(4r + 4) = 1 + 2r^2 + 4r^2 + 4r = 1 + 4r + r^2$.

Definition. An extension E/F is said to be **simple** is $E = F(r)$ for some $r \in E$.

Summary. Element of E are uniquely written as

$$a_0 + a_1 r + \cdots + a_{n-1} r^{n-1}$$

where n is the degree of the minimal polynomial $p(\lambda)$ and to compute in E, use fact that $p(r) = 0$.

Definition. Suppose F is a field. The **order** of F is the number of elements in F and denoted as $|F|$.

Thus we have $|F| < \infty$ or $|F| = \infty$.

2 Field Automorphism

Definition. Suppose R, R' are rings with identity. A homomorphism $\varphi : R \to R'$ is a map that satisfies

1. $\varphi(a + b) = \varphi(a) + \varphi(b)$
2. $\varphi(ab) = \varphi(a)\varphi(b)$
3. $\varphi(1) = 1$

Isomorphism is a bijective homomorphism.

Note. $\varphi : R \to R'$ is injective **iff** $\text{Ker}(\varphi) = \{0\}$.

Definition. An automorphism is an isomorphism $\varphi : R \to R$.

Example. Let $\varphi : \mathbb{C} \to \mathbb{C}$, s.t. $\varphi(a + bi) = a - bi$. Here φ is an automorphism.

Note. The only automorphism of $\mathbb{R}$ is the identity. But there are infinity many automorphism of $\mathbb{C}$.

Lemma. *Suppose $\varphi : F \to F'$ is a homomorphism of fields, then φ is injective.*

Proof. Recall that $\text{Ker}(\varphi)$ is an ideal. Also the only ideals of a field are $\{0\}$ or F. Since $\varphi(1) = 1$ which is not inside the kernel of φ, this means $\text{Ker}(\varphi)$ cannot be F. So $\text{Ker}(\varphi)$ is zero and this implies φ is injective. $\square$

Definition. Suppose $\varphi : F \to F'$ is a homomorphism of fields. Define $\tilde{\varphi} : F[\lambda] \to F'[\lambda]$ by

$$\tilde{\varphi}(a_0 + a_1\lambda + \cdots + a_n\lambda^n) = \varphi(a_0) + \varphi(a_1)\lambda + \cdots + \varphi(a_n)\lambda^n$$

Claim that $\tilde{\varphi}$ is a ring homomorphism. We say $\tilde{\varphi}$ is induced by φ or φ induces $\tilde{\varphi}$. For $f(\lambda) \in F[\lambda]$, we define $({}^{\varphi}f)(\lambda) \in F'[\lambda]$, where $({}^{\varphi}f)(\lambda) = \tilde{\varphi}(f(\lambda))$.

Example. Let $\varphi : \mathbb{C} \to \mathbb{C}$ be complex conjugation and $f(\lambda) = (2+i)\lambda^3 + (1+i)\lambda + 6$. So $({}^{\varphi}f)(\lambda) = (2-i)\lambda^3 + (1-i)\lambda + 6$.

Definition. Suppose E/F and E'/F' are extensions. Suppose $\varphi : F \to F'$ and $\sigma : E \to E'$ are field homomorphism. We say that σ extends φ if $\sigma\mid_F = \varphi$. (Restrict σ to F, i.e. $\sigma(a) = \varphi(a)$ for $a \in F$)

Lemma. *Suppose E/F and E'/F' are extensions and $\varphi : F \to F'$ and $\sigma : E \to E'$ are field homomorphisms and σ extends φ. Suppose $f(\lambda) \in F[\lambda]$ and r is a root of $f(\lambda)$ in E. Then $\sigma(r)$ is a root of $({}^{\varphi}f)(\lambda) \in F'[\lambda]$.*

Proof. Let $f(\lambda) = a_0 + a_1\lambda + \cdots + a_n\lambda^n$, where $a_i \in F$. Then $0 = f(r) = a_0 + a_1 r + \cdots + a_n r^n$. Apply σ to both sides. Then we get

$$0 = \varphi(a_0) + \varphi(a_1)\sigma(r) + \cdots + \varphi(a_n)(\sigma(r))^n$$

Therefore, $\sigma(r)$ is a root of $({}^{\varphi}f)(\lambda) \in F'[\lambda]$. $\square$

Theorem 1 (Extension Theorem for simple extensions)**.** *Suppose $E = F(r)$, where r is algebraic over F. Let $p(\lambda)$ be the minimal polynomial of r. Let E'/F' be another extension and $\varphi : F \to F'$ is a homomorphism. Let $p'(\lambda) = ({}^{\varphi}p)(\lambda)$.*

1. *Suppose r' is a root of $p'(\lambda)$ in E'. Then there exist an unique homomorphism $\sigma : E \to E'$ that extends $\varphi : F \to F'$ and maps r to r'.*

   Moreover, if φ is an isomorphism and $E' = F'(r')$. Then σ is also an isomorphism.

2. *The number of extensions of φ to homomorphisms from E to E' is the number of roots of $p'(\lambda)$ in E'.*

Proof. Proof of 2) from 1): Since any homomorphism $\sigma : E \to E'$ maps r to a root of $p'(\lambda)$ and by 1), there is only one that does this for each root r' of $p'(\lambda)$.

Proof of 1). Uniqueness: Suppose σ_1, σ_2 map r to r' and they extend φ. Then if $a \in F$, $\sigma_1(r) = \varphi(a) = \sigma_2(r)$. Also $\sigma_1(r) = \sigma_2(r) = r'$. Hence, since $E = F(r) = F[r]$, we have $\sigma_1(x) = \sigma_2(x)$ for any $x \in E$. So $\sigma_1 = \sigma_2$.

Existence: We can assume φ is surjective. (Else replace F' with $\mathrm{Im}(\varphi)$.) So φ is an isomorphism. Also assume $E' = F'(r')$. (Else replace E' by $F'(r')$.) Since $E = F(r)$, $E \simeq F[\lambda]/(p(\lambda))$. Also since

φ is an isomorphism, $p'(\lambda)$ is irreducible over F'. (Think about it.) Now since $E' = F'(r')$, we have $E' \simeq F'[\lambda]/(p'(\lambda))$.

Recall we have $\tilde{\varphi} : F[\lambda] \to F'[\lambda]$. But $\tilde{\varphi}(p(\lambda)) = p'(\lambda)$ by definition of $p'(\lambda)$. So $\tilde{\varphi}$ induces:

$$\begin{aligned} \tilde{\tilde{\varphi}} : F[\lambda]/(p(\lambda)) &\longrightarrow F'[\lambda]/(p'(\lambda)) \\ \text{where } f(\lambda) + (p(\lambda)) &\longmapsto f'(\lambda) + (p'(\lambda)) \end{aligned}$$

Note, if $\varphi : F \to F'$ is an isomorphism, then $\tilde{\varphi} : F[\lambda] \to F'[\lambda]$ is an isomorphism, then $\tilde{\tilde{\varphi}} : F[\lambda]/(p(\lambda)) \to F'[\lambda]/(p'(\lambda))$ is an isomorphism. So we have

$$E \simeq F[\lambda]/(p(\lambda)) \xrightarrow{\tilde{\tilde{\varphi}}} F'[\lambda]/(p'(\lambda)) \simeq E'$$

So σ is composition of these isomorphisms.

To see σ extends φ. Let $a \in F$. Then $a \mapsto a + (p(\lambda)) \mapsto \varphi(a) + (p'(\lambda)) \mapsto \varphi(a)$. So $\sigma(a) = \varphi(a)$.

Next, $r \mapsto \lambda + (p(\lambda)) \mapsto \lambda + (p'(\lambda)) \mapsto r'$. So $\sigma(r) = r'$. $\square$

Definition. Suppose F is a field, then let $\mathrm{Aut}(F)$ be the group of automorphisms whith group operation composition of maps. It is called the automorphism group of F. The identity is

$$\begin{aligned} \epsilon_F : F &\longrightarrow F \\ a &\longmapsto a \end{aligned}$$

Example. $\mathrm{Aut}(\mathbb{R}) = \{\epsilon_{\mathbb{R}}\}$. $\mathrm{Aut}(\mathbb{C})$ is infinite.

Definition. Any subgroup of $\mathrm{Aut}(F)$ is called an automorphism group.

Definition. Suppose E/F is an extension. An automorphism of E/F is an automorphism σ of E which extends ϵ_F, i.e. $\sigma\mid_F = \epsilon_F$.

Definition. Let $\mathrm{Gal}(E/F)$ = set of automorphisms of E/F. Then $\mathrm{Gal}(E/F)$ is a subgoup of $\mathrm{Aut}(E)$ and it is called the Galois group of E/F.

Example. $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{\epsilon_{\mathbb{C}}, \sigma\}$, where σ is the complex conjugation automorphism.

Notes on $\mathrm{Gal}(E/F)$

1. Suppose E/F is finite. Suppose $\sigma : E \to E$ is a homomorphism extending $\epsilon : F \to F$. Claim that σ is an isomorphism.

   Proof. σ is injective since all homomorphisms of fields are. Also σ is surjective since σ is an injective linear map from E to E as vector spaces over F. By Rank-Nullity theorem (since E is finite dimensional over F), σ is surjective.

   So any homomorphism of E to E extending ϵ_F is an isomorphism of E. So $\mathrm{Gal}(E/F)$ is the set of all homomorphisms from E to E extending ϵ_F. $\square$

2. (Roots are permuted) Suppose $f(\lambda) \in F[\lambda]$ and $\sigma \in \text{Gal}(E/F)$. If r is a root of $f(\lambda)$, i.e. $f(r) = 0$, then $\sigma(r)$ is also a root of $f(\lambda)$. This is because $\sigma(r)$ is a root of $({}^{\sigma}f)(\lambda)$ and $({}^{\sigma}f)(\lambda) = f(\lambda)$. (Since $\sigma\mid_F = \epsilon_F$ which is an identity map of F) So σ permutes the roots of f.

Proposition. $E = F(r)$ where r is algebraic over F. Let $p(\lambda)$ be the minimal polynomial of r over F. Let $r_1, ..., r_l$ be distinct roots of $p(\lambda)$ in E.

1. For $i = 1, ..., l$, there exists unique $\sigma_i \in \text{Gal}(E/F)$, such that $\sigma_i(r) = r_i$. WIOG, assume $r_1 = r$, then $\sigma_1 = \epsilon_E$. Also, if $x \in E = F(r)$, then $x = a_0 + a_1 r + \cdots + a_{n-1}r^{n-1}$. Then $\sigma_1(x) = a_0 + a_1 r_i + \cdots + a_{n-1}r_i^{n-1}$.
2. $\text{Gal}(E/F) = \{\sigma_1, ..., \sigma_l\}$
3. $|\text{Gal}(E/F)| = l \leq [E : F]$

Proof.

1. Use part 1 of the extension theorem for simple extensions with $E = E'$ and $F = F'$ and $\varphi = \epsilon_F$.
2. Use part 2 of the extension theorem for simple extensions. The number of extensions of ϵ_F is the number of distinct roots of $p(\lambda)$.
3. Let $n = \deg(p(\lambda))$. Then $[E : F] = n$. Since $p(\lambda)$ has at most n distinct roots, so $l \leq n$. (in any extension!)

□

Example. Suppose $E = \mathbb{Q}(\sqrt{2})$. The minimal polynomial of $\sqrt{2}$ is $p(\lambda) = \lambda^2 - 2$ and it has $\sqrt{2}, -\sqrt{2}$ as roots. Thus $\text{Gal}(E/\mathbb{Q}) = \{\sigma_1, \sigma_2\}$, where $\sigma_1 = \epsilon_E$ and $\sigma_2(\sqrt{2}) = -\sqrt{2}$.

In this case, $[E : \mathbb{Q}] = |\text{Gal}(E/Q)| = 2$.

2.1 nth roots of unity

Suppose $G = \{x \in \mathbb{C} \mid x^n = 1\}$. This is a cyclic group of order n with generator

$$e^{\frac{2\pi i}{n}} = \cos(\frac{2\pi}{n}) + i\sin(\frac{2\pi}{n})$$

Note. If $z^n = 1$, then z is a root of $\lambda^n - 1$. However

$$\lambda^n - 1 = (\lambda - 1)(\lambda - z_2)\cdots(\lambda - \lambda_{z_n})$$

Example. Let $E = \mathbb{Q}(\sqrt[3]{5})$. Then the minimal polynomial is $p(\lambda) = \lambda^3 - 5$ over $\mathbb{Q}$. Let $z = e^{\frac{2\pi i}{3}} = \cos(\frac{2\pi}{3}) + i\sin(\frac{2\pi}{3}) = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$. Then $\bar{z} = z^2 = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$. Now $\sqrt[3]{5}$, $z\sqrt[3]{5}$, $z^2\sqrt[3]{5}$ are roots of $p(\lambda)$ in $\mathbb{C}$. Note $z\sqrt[3]{5}$, $z^2\sqrt[3]{5} \notin E = \mathbb{Q}(\sqrt[3]{5})$. So $\sqrt[3]{5}$ is the only root of $p(\lambda)$ in E. So $\text{Gal}(E/Q) = \{\epsilon_E\}$ since there is only one distinct root to $p(\lambda)$ in E.

In this case, we have $|\operatorname{Gal}(E/\mathbb{Q})| = 1$ while $[E : \mathbb{Q}] = 3$. We didn't include enough roots of $p(\lambda)$ to make E. We should have studied $\mathbb{Q}(\sqrt[3]{5},\ z\sqrt[3]{5},\ z^2\sqrt[3]{5})$ instead.

Definition (splitting field)**.** Suppose $f(\lambda) \in F[\lambda]$. $f(\lambda)$ is monic of degree ≥ 1 and suppose E/F is an extension. We say E is a splitting field for $f(\lambda)$ over F if

1. $f(\lambda) = (\lambda - r_1)\cdots(\lambda - r_n)$, where $r_i \in E$, $i = 1, ..., n$.
2. $E = F(r_1, ..., r_n)$.

Also say E/F is splitting field for $f(\lambda)$.

Note. Suppose $f(\lambda) \in F[\lambda]$ monic, degree ≥ 1.

1. If E is a splitting field for $f(\lambda)$, then E/F is finite.
2. Suppose $E/K/F$ and E is a splitting field for $f(\lambda)$ over F, then E is a splitting field for $f(\lambda)$ over K.
3. To find a splitting field for $f(\lambda)$ over F, first find some field L (an extension of F) such that

$$f(\lambda) = (\lambda - r_1)\cdots(\lambda - r_n)$$

where $r_i \in L$ and let $E = F(r_1, .., r_n)$.

Example. Suppose $f(\lambda) = \lambda^2 - 2 \in \mathbb{Q}[\lambda]$. Then $f(\lambda) = (\lambda - \sqrt{2})(\lambda + \sqrt{2})$, where $\sqrt{2}, -\sqrt{2} \in \mathbb{R}$. $E = \mathbb{Q}(\sqrt{2}, -\sqrt{2}) = \mathbb{Q}(\sqrt{2})$ is a splitting field for $\lambda^2 - 2$ over $\mathbb{Q}$.

Example. Let $f(\lambda) = \lambda^3 - 5 \in \mathbb{Q}[\lambda]$. Then $f(\lambda) = (\lambda - \sqrt[3]{5})(\lambda - z\sqrt[3]{5})(\lambda - z^2\sqrt[3]{5})$, where $z = e^{2\pi i/3}$. (Here we let $L = \mathbb{C}$.) So $E = \mathbb{Q}(\sqrt[3]{5},\ z\sqrt[3]{5},\ z^2\sqrt[3]{5}) = \mathbb{Q}(\sqrt[3]{5},\ z)$ is a splitting field for $f(\lambda)$ over $\mathbb{Q}$.

Theorem 2 (Existence of splitting fields)**.** *Suppose $f(\lambda) \in F[\lambda]$ is monic and degree ≥ 1. Then there exists a splitting field of $f(\lambda)$ over F.*

Proof. It is sufficient to show that there exists an extension L of F s.t. $f(\lambda) = (\lambda - r_1)\cdots(\lambda - r_n)$ where $r_i \in L$. We know that there exists an extension K_1 of F in which $f(\lambda)$ has a root. (We know it for irreducible polynomials of degree ≥ 1, so just apply our constructor to an irreducible factor of $f(\lambda)$. A root of irreducible factor is also a root of $f(\lambda)$.) Then $f(\lambda) = (\lambda - r_1)g(\lambda)$, where $r_1 \in K_1$, $g(\lambda) \in K_1[\lambda]$. If the degree of $f(\lambda) = 1$, then we are done. Otherwise, we can find a root of r_2 of $g(\lambda)$ in some extension K_2 of K_1. Repeat this process. □

Definition (Root terminology)**.** Suppose $f(\lambda)$ is monic with degree ≥ 1 over F. Suppose $f(\lambda) = (\lambda - r_1)\cdots(\lambda - r_n)$, where r_i are elements of some extension L of F. If r_i are distinct, then we say $f(\lambda)$ has distinct roots in L. If we list only distinct roots $r_1, ..., r_l$, they are called the distinct roots of $f(\lambda)$ in L.

Challenge: Find irreducible polynomials with multiple distinct roots.

Theorem 3 (Extension theorm for splitting fields)**.** *Suppose $\varphi : F \to F'$ is an isomorphism. Let $f(\lambda)$ be a monic polynomial of degree $n \geq 1$ over F. Let $f'(\lambda) = ({}^{\varphi}f)(\lambda)$. (Apply φ to coefficients of f.) Let E be a splitting field for $f(\lambda)$ over F. Let E' be a splitting field for $f'(\lambda)$ over F'.*

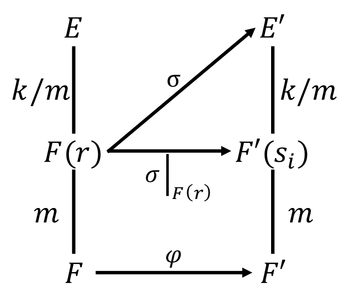
1. *There exists an extension of φ to an isomorphism $E \to E'$.*
2. *The number of extension of φ to an isomorphism $E \to E'$ is $\leq [E : F]$.*
3. *If $f'(\lambda)$ has distinct roots in E', then equality holds.*

Proof. By induction on $k = [E : F]$. Base case, $k = 1$. Then $E = F$. Therefore, $f(\lambda)$ is a product of degree one factors over F. Thus, the image polynomial $f'(\lambda)$ is a product of degree one factors over F'. Then $E' = F'$ and 1. holds. (Since $\varphi : E \to E'$ is the extension.) Then 2. 3. holds as well.

Suppose now $k > 1$ and Theorem holds for smaller k. Then $E \neq F$. Hence there exists a root r of $f(\lambda)$ in E not in F. So there exists an irreducible factor $p(\lambda)$ of $f(\lambda)$ which has r as a root in E not in F with $\deg(p(\lambda)) \geq 2$. (Since r is not in F.)

Now we have $f(\lambda) = g(\lambda)p(\lambda)$ and $p(r) = 0$, $g(\lambda) \in F[\lambda]$. Consider the induce polynomial. Since φ is an isomorphism, $f'(\lambda) = p'(\lambda)g'(\lambda)$ and $p'(\varphi(r)) = 0$. Also $\deg(p'(\lambda)) = \deg(p(\lambda)) \geq 2$, and $p'(\lambda)$ is irreducible over F' as well.

Suppose $s_1, ..., s_l$ are distinct roots of $p'(\lambda)$ in E'. Note $l \leq m$, where $m = \deg(p'(\lambda))$. Then we have the following relationship.



By *extension theorem for simple extensions*, there exists an unique extension σ_i of φ to a homomorphism of $F(r)$ into E' so that $\sigma_i(r) = s_i$. Then σ_i restricted on $F(s_i)$ is an isomorphism of $F(r)$ onto $F'(s_i)$. By multiplicativity of degree, we get the degrees in the picture. But $m \geq 2$, so $k/m < k$. By induction, σ_i extendes to an Isomorphism of E to E'. This proves 1.

To prove 2, define $e(\varphi)$ as the number of extensions of φ to an isomorphism E to E'. Define $e(\sigma_i)$ as the number of extensions of σ_i to an isomorphism E to E'.

Now any extension of φ to an isomorphism of E to E' must map r to some s_i. Hence it must extend some σ_i. So we have

$$e(\varphi) = \sum_{i=1}^{l} e(\sigma_i)$$

By induction, $e(\sigma_i) \leq [E : F(r)] = k/m$. Plug this into the formula, we have

$$e(\varphi) \leq \sum_{i=1}^{l} \frac{k}{m} = l \cdot \frac{k}{m} \leq m \cdot \frac{k}{m} = k$$

This proves 2.

If the roots are distinct, then $l = m$. Again by induction, we have $e(\sigma_i) = k/m$. So

$$e(\varphi) = \sum_{i=1}^{m} \frac{k}{m} = k$$

□

Corollary 2 (Uniqueness of splitting fields)**.** Suppose $f(\lambda)$ is monic polynomial of $\deg \geq 1$ over F. Suppose E/F and E'/F are splitting extensions of $f(\lambda)$. Then there exists an isomorphism from E to E' which extends $\epsilon_F : F \to F$. And thus we have $E = E'$.

Corollary 3. Suppose $f(\lambda)$ monic of $\deg \geq 1$ over F. Let E/F be the splitting extension of $f(\lambda)$. Then

$$|\operatorname{Gal}(E/F)| \leq [E : F]$$

also if $f(\lambda)$ has distinct roots in E, then $|\operatorname{Gal}(E/F)| = [E : F]$.

Definition (Notation for elements of $\operatorname{Gal}(E/F)$)**.**

1. Suppose E/F is an extension $E = F(u_1, ..., u_k)$. Then an element $\sigma \in \operatorname{Gal}(E/F)$ is denoted by $\sigma(u_i) = v_i$.

$$\sigma : \begin{array}{ccc} u_1 & \longrightarrow & v_1 \\ u_2 & \longrightarrow & v_2 \\ \cdots & \cdots & \cdots \\ u_k & \longrightarrow & v_k \end{array}$$

2. Suppose E/F is a splitting field of $f(\lambda) \in F[\lambda]$. Let $r_1, ..., r_l$ are distinct roots of $f(\lambda)$ in E. $E = F(r_1, ..., r_l)$. Then each $\sigma \in \operatorname{Gal}(E/F)$ has form

$$\sigma : \begin{array}{ccc} r_1 & \longrightarrow & r_{\pi(1)} \\ r_2 & \longrightarrow & r_{\pi(2)} \\ \cdots & \cdots & \cdots \\ r_l & \longrightarrow & r_{\pi(l)} \end{array}$$

where π is a permutation. ($\pi \in S_l$, S_l is the permutation group on l objects.) Thus we have a map $\operatorname{Gal}(E/F) \to S_l$ that is an injective homomorphism. (It might not be surjective.) It is injective since only the identity in $\operatorname{Gal}(E/F)$ is the identity permutation on roots. i.e. Think of $\operatorname{Gal}(E/F)$ as a subgroup of S_l. Write $\sigma = \pi$. (Since each σ maps to a unique permutation.)

Example. Suppose E is a splitting field of $f(\lambda) = \lambda^3 - 5$ over $\mathbb{Q}$. Then $E = \mathbb{Q}(\sqrt[3]{5}, z\sqrt[3]{5}, z^2\sqrt[3]{5}) = \mathbb{Q}(\sqrt[3]{5}, z)$, where $z = e^{2\pi i/3}$.

Now $\sqrt[3]{5}$ has degree 3 over $\mathbb{Q}$. And z has degree 2 over $\mathbb{Q}$. (It is $(\lambda + \frac{1}{2})^2 + \frac{3}{4}$) Since $2, 3$ are reletively prime, we have $[E : \mathbb{Q}] = 6$.

$$\begin{array}{lclcl} \mathbb{Q}(z, \sqrt[3]{5}) & \xrightarrow{3} & \mathbb{Q}(z) & \xrightarrow{2} & \mathbb{Q} \\ \mathbb{Q}(z, \sqrt[3]{5}) & \xrightarrow{2} & \mathbb{Q}(\sqrt[3]{5}) & \xrightarrow{3} & \mathbb{Q} \end{array}$$

So $|\operatorname{Gal}(E/\mathbb{Q})| = 6$. Label the roots $r_1 = \sqrt[3]{5}$, $r_2 = z\sqrt[3]{5}$, $r_3 = z^2\sqrt[3]{5}$. So $\operatorname{Gal}(E/\mathbb{Q}) \leq S_3$. So $\operatorname{Gal}(E/\mathbb{Q}) = S_3$, since both have order 6.

For example, $\sigma = (123) \in \operatorname{Gal}(E/\mathbb{Q}) = S_3$. So

$$\sigma : \begin{array}{ccc} r_1 & \longrightarrow & r_2 \\ r_2 & \longrightarrow & r_3 \\ r_3 & \longrightarrow & r_1 \end{array}, \quad \begin{array}{ccc} \sqrt[3]{5} & \longrightarrow & z\sqrt[3]{5} \\ z\sqrt[3]{5} & \longrightarrow & z^2\sqrt[3]{5} \\ z^2\sqrt[3]{5} & \longrightarrow & \sqrt[3]{5} \end{array}$$

What about $\sigma(z)$?

$$\sigma(z) = \sigma\left(\frac{z\sqrt[3]{5}}{\sqrt[3]{5}}\right) = \frac{\sigma(z\sqrt[3]{5})}{\sigma(\sqrt[3]{5})} = \frac{z^2\sqrt[3]{5}}{z\sqrt[3]{5}} = z$$

Definition. Suppose $f(\lambda) \in F[\lambda]$.

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

Define the derivative of $f(\lambda)$ to be

$$f'(\lambda) = na_n\lambda^{n-1} + \cdots + a_1$$

where $na_n = a_n + a_n + \cdots + a_n$. Note: roduct rule, sum rule works too.

Example. $f(\lambda) = \lambda^3 + 2\lambda^2 + \lambda + 1 \in \mathbb{F}_3[\lambda]$. Then $f'(\lambda) = 3\lambda^2 + 4\lambda + 1 = 0 + 1\lambda + 1 = \lambda + 1$.

Example. $f(\lambda) = 2\lambda^9 + \lambda^3 + 2 \in \mathbb{F}_3[\lambda]$. Then $f'(\lambda) = 18\lambda^8 + 3\lambda^2 = 0$.

Proposition. Suppose $f(\lambda)$ is monic of deg ≥ 1 over F. Suppose $f(\lambda)$ and $f'(\lambda)$ are relatively prime in $F[\lambda]$. Let E be the splitting field of $f(\lambda)$ over F. Then $f(\lambda)$ has distinct roots in E.

Proof. Since $f(\lambda)$ and $f'(\lambda)$ are relatively prime, we have $\gcd(f(\lambda), f'(\lambda)) = 1$. Then we prove by contradiction.

Now $f(\lambda) = (\lambda - r_1)(\lambda - r_2)\cdots(\lambda - r_n)$ where $r_i \in E$. Suppose for contradiction, $r_1 = r_2$. (i.e. $f(\lambda)$ does not have distinct roots.) So $f(\lambda) = (\lambda - r_1)^2 g(\lambda)$. However, $f'(\lambda) = 2(\lambda - r_1)g(\lambda) + (\lambda - r_1)^2 g'(\lambda)$. Since $f(\lambda)$ and $f'(\lambda)$ has r_1 as a root, then both of them can be divided by the minimal polynomial of r_1. Contradiction! □

Note. The converse is also true. If $f(\lambda)$ has distinct roots in E, then $f(\lambda)$ and $f'(\lambda)$ are relatviely prime.

Example. Suppose $f(\lambda) = \lambda^{p^n} - \lambda \in \mathbb{F}_p[\lambda]$, where $n \geq 1$. Then $f'(\lambda) = p^n \lambda^{p^n - 1} - 1 = -1$. So $\gcd(f(\lambda), f'(\lambda)) = 1$. So $f(\lambda)$ has distinct roots in the splitting field.

3 Finite Fields

Proposition. Suppose E is a finite field.

1. Then E is a finite extension of $\mathbb{F}_p \triangleq \mathbb{Z}/p$ for some prime p.
2. Hence $|E| = p^n$ where $n = [E : \mathbb{F}_p]$.

Proof.
1. Define $\varphi : \mathbb{Z} \to E$, s.t. $\varphi(m) = m \cdot 1_E$ for $m \in \mathbb{Z}$. So φ is a homomorphism of rings. Let $F = \{m \cdot 1_E \mid m \in \mathbb{Z}\} = \mathrm{Im}(\varphi)$. Then F is a subring of E. Now $\mathrm{Ker}(\varphi)$ is an ideal of $\mathbb{Z}$. Since $\mathbb{Z}$ is infinite and E is finite. Then $\mathrm{Ker}(\varphi) \neq (0)$. Hence $\mathrm{Ker}(\varphi) = (p)$ (ideal in a PID), where p is a positive integer. By definition, p is the characteristic of E. By a previous homework, p is a prime.

   Recap that φ is a homomorphism of $\mathbb{Z}$ onto F with kernel (p). So $F \simeq \mathbb{Z}/(p) = \mathbb{F}_p$ as a ring.

   Then identify F with $\mathbb{F}_p$. Therefore E contains $\mathbb{F}_p$ as a subring but $\mathbb{F}_p$ is a field. So E contains $\mathbb{F}_p$ as subfield. Therefore E is an extension of $\mathbb{F}_p$ by definition. Since E is finite, E is a finite dimensional vector space over $\mathbb{F}_p$. So $E/\mathbb{F}_p$ is finite.

2. Part 2 follows from part 1. Since E is a finite extension of $\mathbb{F}_p$, this means there is a basis $u_1, ..., u_n$ with all elements in E written uniquely as

   $$a_1 u_1 + a_2 u_2 + \cdots + a_n u_n$$

   where $a_i \in \mathbb{F}_p$. So there are p^n choices for the a_is. (p choices for each a_i.)

□

Proposition. Suppose E is a finite field of order p^n for p a prime and $n \geq 1$. Then $u^{p^n} = u, \forall u \in E$.

Proof. Let $E^\times = \{u \in E \mid u \neq 0\}$. Then $E^\times$ is a group under multiplication. Also $|E^\times| = p^n - 1$. Hence by Langrange's Theorem, we know $u^{p^n - 1} = 1$. So $u \cdot u^{p^n - 1} = u$. So $u^{p^n} = u$. This also trivially holds for zero since $0^{p^n} = 0$. □

Corollary 4 (Fermat's Little Theorem)**.** If $u \in \mathbb{F}_p$, then $u^p = u$.

Corollary 5 (Freshman's Dream)**.** Suppose that E is a field of characteristic p where p is a prime. Then for $v, u \in E$, we have

$$(u + v)^p = u^p + v^p$$

And hence

$$(u + v)^{p^n} = u^{p^n} + v^{p^n}$$

for $n \geq 1$.

Exercise. Suppose $\text{char}(E) = 3$ and $u, v \in E$. Then $(u+v)^3 = u^3 + 3u^2v + 3uv^2 + v^3 = u^3 + v^3$.

Theorem 4 (Classification of finite fields)**.** *Suppose that p is prime and $n \geq 1$. Then $\exists$ a unique field of order p^n up to isomorphism, namely the splitting field of $\lambda^{p^n} - \lambda$ over $\mathbb{F}_p$.*

Proof. Uniqueness: Suppose E is a field of order p^n. By the first proposition, E is an extension of $\mathbb{F}_p$ of degree n. Let $f(\lambda) = \lambda^{p^n} - \lambda$. We want to show that E is the splitting field of $f(\lambda)$ over $\mathbb{F}_p$. By the second proposition, every element of E is a root of $f(\lambda)$. But $|E| = p^n$ and $\deg(f(\lambda)) = p^n$. Hence $f(\lambda) = \prod_{u \in E}(\lambda - u)$ in $E[\lambda]$. Certainly E is generated over $\mathbb{F}_p$ by the roots of $f(\lambda)$. So E is the splitting field of $f(\lambda)$ over $\mathbb{F}_p$.

Existence: Suppose E is the splitting field of $f(\lambda)$ over $\mathbb{F}_p$ where $f(\lambda) = \lambda^{p^n} - \lambda$. We want to show that $|E| = p^n$. Let $K = \{u \in E \mid u^{p^n} = u\}$ = set of all roots of $f(\lambda)$ in E. We'll show that $K = E$ and $|K| = p^n$. By Fermat's Little theorem, $a^p = a$ for all $a \in \mathbb{F}_p$. Therefore $a^{p^n} = a$, $\forall a \in \mathbb{F}_p$. So $a \in K$ and so $\mathbb{F}_p \subseteq K$. Use Freshman's Dream to get that K is a subfield of E. ($E/K/\mathbb{F}_p$.) Since K contains the roots of $f(\lambda)$ and E is generated by the roots, therefore $K = E$. Finally, since $f'(\lambda) = -1$, so $\gcd(f(\lambda), f'(\lambda)) = 1$. So $f(\lambda)$ has distinct roots in E. So $|K| = p^n$. Then $|E| = p^n$. □

Definition. The unique field of order p^n is called the Galois field of order p^n and is denoted by $\mathbb{F}_{p^n}$.

Example. The Galois field of order 81 is the splitting field of $f(\lambda) = \lambda^{81} - \lambda$ over $\mathbb{F}_3$. So $\mathbb{F}_{3^4} = \mathbb{F}_{81} = \{\text{all roots of } \lambda^{81} - \lambda\}$.

For computations, construct $\mathbb{F}_{81}$. $\mathbb{F}_3[\lambda]/(q(\lambda)) \simeq \{a_0 + a_1 r + a_2 r^2 + a_3 r^3 \mid a_i \in \mathbb{F}_3\}$ where $q(\lambda)$ is irreducible of degree 4.

There are 18 such polynomails. $\lambda^4 + \lambda + 2 = q(\lambda)$.

From now on, assume $\text{char}(E) = 0$. i.e. $n \cdot 1_E = 0$ if and only if $n = 0$. Thus for nonzero u, $nu = 0$ if and only if $n = 0$.

Lemma. *Suppose $p(\lambda)$ is a monic irreducible polynomial of degree ≥ 1 over F. Then $p(\lambda)$ has distinct roots in its splitting field.*

Proof. Suppose for contradiction that $p(\lambda)$ does not have distinct roots in its splitting field. As was proved last time, $p(\lambda)$ and $p'(\lambda)$ (the derivative) are not relatively prime. Let $d(\lambda) = \gcd(p(\lambda), p'(\lambda))$ in $F[\lambda]$. So $\deg(d(\lambda)) \geq 1$. Since then $d(\lambda)$ must be a factor of $p(\lambda)$ and $p(\lambda)$ is irreducible, we must have $d(\lambda) = p(\lambda)$. So $p(\lambda) \mid p'(\lambda)$. But $p'(\lambda)$ is either 0 or has degree less than $\deg(p(\lambda))$. So $p'(\lambda) = 0$.

But if $p(\lambda) = \lambda^n + \cdots + a_1\lambda + a_0$, then $p'(\lambda) = n\lambda^{n-1} + \cdots + a_1$. Since $\text{char}(F) = 0$, so $p'(\lambda) \neq 0$. Contradiction. □

Definition (Normal extension)**.** Suppose E/F is an extension. We say E/F is a normal extension if E is the splitting field of some monic polynomial of degree ≥ 1 over F.

Note. Any normal extension is finite, since splitting field are finite.

Proposition. Suppose E/F is normal. Then $\exists$ a monic polynomial $f(\lambda)$ over F of $\deg \geq 1$, s.t. E is the splitting field of $f(\lambda)$ over F and $f(\lambda)$ has distinct roots in E. Hence

$$|\operatorname{Gal}(E/F)| = [E : F]$$

Proof. By definition, E is the splitting field of some $h(\lambda) \in F[\lambda]$. Then $h(\lambda) = p_1(\lambda)^{l_1} \cdots p_k(\lambda)^{l_k}$, where $p_i(\lambda)$ are distinct monic irreducible polynomials over F. Let $f(\lambda) = p_1(\lambda) \cdots p_n(\lambda)$. Then $f(\lambda)$ and $h(\lambda)$ have the same distinct roots. Then E is the splitting field of $f(\lambda)$ over F. Since $\operatorname{char}(E) = 0$, we proved that each $p_i(\lambda)$ has distinct root in E. Also if $i \neq j$, then $p_i(\lambda)$ and $p_j(\lambda)$ cannot have a common root in E. (Since then both p_i and p_j would be the minimal polynomials of that root which means $p_i \mid p_j$ and $p_j \mid p_i$, i.e. $p_i = p_j$.) Therefore, $f(\lambda)$ has distinct roots in E.

Last statement follows from the extension theorem for splitting field. ☐

Definition. Suppose $G \leq \operatorname{Aut}(E)$ (G is a subgroup of automorphisms of the field E). We define $\operatorname{Inv}(G) = \{a \in E \mid \sigma(a) = a, \sigma \in G\}$.

Lemma (Exercise)**.** $\operatorname{Inv}(G)$ *is a subfield of* E *called the subfield of* G*-invariants in* E*.*

Example. Let $E = \mathbb{C}$, $G = \{\epsilon, \sigma\}$. Then if $a \in E = \mathbb{C}$, $a \in \operatorname{Inv}(G) \Leftrightarrow \sigma(a) = a \Leftrightarrow a \in \mathbb{R}$. So $\operatorname{Inv}(G) = \mathbb{R}$. Note, $\mathbb{C}/\mathbb{R}$ has degree 2. Also it is the splitting field of $\lambda^2 + 1$. So it is a normal extension.

Now we are curious about the correspondence between groups and extensions. Suppose E is a field.

1. If F is a subfield of E s.t. E/F is a normal extension. Can we have $\operatorname{Gal}(E/F)$ being a finite subgroup of $\operatorname{Aut}(E)$ and $|\operatorname{Gal}(E/F)| = [E : F]$?

2. If G is a finite subgroup of $\operatorname{Aut}(E)$ and $F = \operatorname{Inv}(G)$. Can we have E/F being a normal extension and $[E : F] = |G|$?

3. Does this establish a one to one correspondence between

$$\text{subfields } F \text{ of } E \text{ such that } E/F \text{ is normal} \longleftrightarrow \text{finite subgroups of } \operatorname{Aut}(E)$$

Lemma (Artin's Lemma)**.** *Suppose* E *is a field,* $G \leq \operatorname{Aut}(E)$ *that is finite. Let* $F = \operatorname{Inv}(G)$*. Then* E/F *is a finite extension and* $[E : F] \leq |G|$*.*

Proof. We will show that any set of more than $m = |G|$ elements in E is linearly dependent over F. This will prove both statements.

Suppose $G = \{\sigma_1, ..., \sigma_m\}$ and $\sigma_1 = \epsilon_E$. Let $u_1, ..., u_n$ be elements of E where $n > m$. We will show that they are dependent. Consider a system of equations

$$A\vec{x} = \vec{0}$$

where

$$A = \begin{bmatrix} \sigma_1(u_1) & \cdots & \sigma_1(u_n) \\ \cdots & \cdots & \cdots \\ \sigma_m(u_1) & \cdots & \sigma_m(u_n) \end{bmatrix}_{m\times n}$$

This is a system with n unknowns and m equations, so there is always a nontrivial solution in E^n. Our goal is to find a solution in F^n. Then since $\sigma_1 = \epsilon_E$, the first equation will give

$$x_1u_1 + x_2u_2 + \cdots + x_nu_n = 0$$

Note if $\overline{s} = \begin{bmatrix} s_1 & \cdots & s_n \end{bmatrix}^T$ is a solution of $A\vec{x} = \vec{0}$. Then $\forall i$, we have $\sigma_i(\overline{s}) = \begin{bmatrix} \sigma_i(s_1) & \cdots \sigma_i(s_n) \end{bmatrix}^T$ is a solution to $\sigma_i(A)\vec{x} = \vec{0}$ where $\sigma_i(A) = (\sigma_i(a_{jk}))$. But $\sigma_i(A)$ is obtained from A by permuting the rows. Therefore both the above to linear systems has the same solution. So $\sigma_i(\overline{s})$ is also a solution of $A\vec{x} = \vec{0}$.

Now choose solution $\overline{s} = \begin{bmatrix} s_1 & \cdots & s_n \end{bmatrix}^T$ with fewest nonzero entries. WLOG, assume $s_1 \neq 0$. Replace $\overline{s}$ with $\overline{s}/s_1$ to get $s_1 = 1$. Now we have $\overline{s} = \begin{bmatrix} 1 & s_2 & \cdots & s_n \end{bmatrix}^T$. Assume for contradiction $\overline{s} \notin F^n$. Therefore $s_i \notin F$ for some i and WLOG $s_2 \notin F$. Since $F = \text{Inv}(G)$ so $\exists \sigma_j \in G$ such that $\sigma_j(s_2) \neq s_2$. But $\sigma_j(\overline{s})$ is also a solution and so is $\overline{s} - \sigma_j(\overline{s})$. Then we have

$$\overline{s} - \sigma_j(\overline{s}) = \begin{bmatrix} 1 \\ s_2 \\ \vdots \\ s_n \end{bmatrix} - \begin{bmatrix} 1 \\ \sigma_j(s_2) \\ \vdots \\ \vdots \end{bmatrix} = \begin{bmatrix} 0 \\ s_2' \\ \vdots \\ \vdots \end{bmatrix}$$

where $s_2' \neq 0$. This is a nontrivial solution with fewer zero extries! Contradiction! □

Remarks. 1. If we have $E/K/F$ and E/F is normal. Then E/K is normal.

2. If $E/K/F$, then $\text{Gal}(E/K) \leq_{\text{subgroup}} \text{Gal}(E/F)$.

Theorem 5 (Characterization of normal extensions)**.** *Suppose E/F, then TFAE*

1. *E/F is normal*
2. *$F = \text{Inv}(G)$ for some finite group $G \leq Aut(E)$.*
3. *E/F is a finite extension with the following property:*

   If $p(\lambda)$ is any monic irreducible polynomial over F which has a root in E. Then $p(\lambda)$ is a product of degree one factors in $E[\lambda]$.

Moreover, in this case, we have

$$Inv(Gal(E/F)) = F \tag{1}$$

Proof. 1⇒2: Suppose E/F is normal. Let $G = \mathrm{Gal}(E/F)$. Let $F' = \mathrm{Inv}(G)$. Then we have $E/F'/F$. By remark 1, we have E/F' is normal since E/F is normal. Let $G' = \mathrm{Gal}(E/F')$. Then by remark 2, we have $G' \leq_{\text{subgroup}} G$. Since E/F and E/F' are normal, we have $|G| = [E : F]$ and $|G'| = [E : F']$.

Now if $\sigma \in G$, then σ fixes elements of F' since $F' = \mathrm{Inv}(G)$. So we see $G \leq G'$. Then we have $G = G'$. Thus $|G| = |G'|$ and we get $[E : F] = [E : F']$. This means $F = F'$. Then we have $F = \mathrm{Inv}(G)$. So 2. and $\mathrm{Inv}(\mathrm{Gal}(E/F)) = F$ follow.

2⇒3: Suppose $F = \mathrm{Inv}(G)$ for some finite $G \leq \mathrm{Aut}(E)$. By Artin's Lemma, E/F is finite.

Suppose $p(\lambda)$ is monic irreducible polynomial over F with a root r in E. Then $p(\lambda)$ is the minimal polynomial of r over f. We want to show $p(\lambda)$ splits as product of degree 1 factors in $E[\lambda]$. This is enough to show that $\exists f(\lambda) \in F[\lambda]$ that splits in $E[\lambda]$ and has r as a root. Since then $p(\lambda) \mid f(\lambda)$ and therefore if $f(\lambda)$ splits as product of degree 1 polynomials in $E[\lambda]$, so does $p(\lambda)$.

Let $f(\lambda) = \prod_{\sigma \in G}(\lambda - \sigma(r)) \in E[\lambda]$. We want to show that $f(\lambda) \in F[\lambda]$.

Now take $\tau \in G$. $({}^\tau f)(\lambda) = \prod_{\sigma \in G}(\lambda - (\tau\sigma)(r)) = \prod_{\delta \in G}(\lambda - \delta(r)) = f(\lambda)$. Now we have $f(\lambda) \in F[\lambda]$. So $f(\lambda)$ is a polynomial with r as a root and coefficients in F. $f(\lambda)$ splits in $E[\lambda]$ by definition and therefore so does $p(\lambda)$.

3⇒1: Suppose any monic irreducible polynomial $p(\lambda)$ with a root in E splits as a product of degree 1 factors in $E[\lambda]$, We want to show that it is a normal extension, namely there is a polynomial $f(\lambda)$ such that E is the splitting field of $f(\lambda)$ over F.

Since E/F is finite. Then we have $u_1, ..., u_k \in E$ such that $E = F(u_1, ..., u_k)$ and u_i is algebraic over F. Let $p_i(\lambda)$ be the minimal polynomial of u_i over F. By assumption, each $p_i(\lambda)$ splits in $E[\lambda]$. Let $f(\lambda) = p_1(\lambda) \cdots p_k(\lambda)$. Then $f(\lambda)$ splits as a product of degree 1 polynomials in $E[\lambda]$. And E is generated by the roots of $f(\lambda)$. So E is the splitting field of $f(\lambda)$. Thus E/F is normal. □

Example. Suppose $E = \mathbb{Q}(\sqrt[3]{5})$. Is it normal?

Solution: $p(\lambda) = \lambda^3 - 5$ is the minimal polynomial of $\sqrt[3]{5}$. But it does not split as product of degree 1 factors in $E[\lambda]$. So it is not normal.

Also since $|\mathrm{Gal}(E/\mathbb{Q})| = 1$ and $E/\mathbb{Q}$ has degree 3. So it is not normal. □

Theorem 6 (General Galois Correspondence)**.** *Suppose E is a field.*

1. *(Fields to groups) Suppose F is a subfield of E such that E/F is normal. Let $G = \mathrm{Gal}(E/F)$. Then G is a finite group. Morever $|G| = [E : F]$ and $\mathrm{Inv}(G) = F$.*
2. *(Groups to fields) Suppose $G \leq \mathrm{Aut}(E)$ such that G is finite. Let $F = \mathrm{Inv}(G)$. Then E/F is a normal extension. Morever $[E : F] = |G|$ and $\mathrm{Gal}(E/F) = G$.*

Proof. 1. Done by previous theorem.

2. By previous theorem, we have E/F is normal. Note, $G \leq \mathrm{Gal}(E/F)$. Since it is normal, $|\mathrm{Gal}(E/F)| = [E : F]$. By Artin's lemma, we have $[E : F] \leq |G|$. So $|\mathrm{Gal}(E/F)| \leq |G| \leq |\mathrm{Gal}(E/F)|$. Thus we have $G = \mathrm{Gal}(E/F)$ and $[E : F] = |\mathrm{Gal}(E/F)| = |G|$.

□

Theorem 7 (The Galois correspondence for normal extensions)**.** *Suppose E/F normal and $G = \mathrm{Gal}(E/F)$. Let*

- $\mathrm{subfield}(E/F)$ *the set of all subfields of E/F*
- $\mathrm{subgp}(G)$ *the set of all subgroups of G.*

There exists a correspondence between the above two.

- *If $K \in \mathrm{subfield}(E/F)$, then let $H = \mathrm{Gal}(E/K)$. So $H \in \mathrm{subgp}(G)$.*
- *If $H \in \mathrm{subgp}(G)$, then let $K = \mathrm{Inv}(H)$. So $K \in \mathrm{subfield}(E/F)$.*

In this case, we write

$$H \longleftrightarrow K \quad \text{or} \quad K \longleftrightarrow H$$

We say H corresponds to K or vice sersa.

Exercise: If E/F is not normal, what will happen? H is still a subgroup of G and K is still a subfield of E, namely $E/K/F$ is an extension.

Lemma. *Suppose E/F is normal. $G = \mathrm{Gal}(E/F)$ and $K \longleftrightarrow H$. If $\sigma \in G$, then $\sigma(K) \longleftrightarrow \sigma H \sigma^{-1}$. Note $\sigma(K) = \{\sigma(u) \mid u \in K\}$.*

Proof. Since $K \longleftrightarrow H$, then $K = \mathrm{Inv}(H)$. Also, $\sigma(K) \longleftrightarrow \sigma H \sigma^{-1}$ is equivalent to $\sigma(K) = \mathrm{Inv}(\sigma H \sigma^{-1})$. This is what we are going to show. If $v \in E$, then

$$\begin{aligned} v \in \mathrm{Inv}(\sigma H \sigma^{-1}) &\iff \sigma\tau\sigma^{-1}(v) = v, \quad \forall \tau \in H \\ &\iff \tau(\sigma^{-1}(v)) = \sigma^{-1}(v) \\ &\iff \sigma^{-1}(v) \in \mathrm{Inv}(H) = K \\ &\iff v \in \sigma(K) \end{aligned}$$

So $\mathrm{Inv}(\sigma H \sigma^{-1}) = \sigma(K)$, i.e. $\sigma(K) \longleftrightarrow \sigma H \sigma^{-1}$. $\square$

Theorem 8 (Fundamental Theorem of Galois Theory)**.** *Suppose E/F is normal. $G = \mathrm{Gal}(E/F)$. The bijective correspondence $H \longleftrightarrow K$ (between subgroups and subfields) has the following properties;*

1. *If $K \longleftrightarrow H$, then $[E : K] = |H|$ and $[K : F] = [G : H]$ (Think about $E/K/F$. $[G : H]$ is the index of H in G.)*
2. *If $K_1 \longleftrightarrow H_1$ and $K_2 \longleftrightarrow H_2$, then $K_1 \subseteq_{\mathrm{subgp}} K_2 \iff H_2 \subseteq_{\mathrm{subgp}} H_1$. Thus the correspondence is inclusion reversing and $K_1 \cap K_2 \longleftrightarrow \langle H_1, H_2 \rangle$.*
3. *If $K \longleftrightarrow H$, then*

$$K/F \text{ is normal } \iff H \trianglelefteq G \ (H \text{ is a normal subgp of } G)$$

In that case, $\mathrm{Gal}(K/F) \simeq G/H$.

Proof. 1. Since E/F is normal, then E/K is normal. Then we have $[E : K] = |\mathrm{Gal}(E/K)| = |H|$. For the second part, $[E : F] = [E : K][K : F]$. Since $[E : F] = |G|$. So $|G| = |H|[K : F]$ which implies $[K : F] = |G|/|H|$. By Langrange's theorem from group theory, $[G : H] = |G|/|H|$. Thus we've showed $[K : F] = [G : H]$.

2. We have $K_i = \mathrm{Inv}(H_i)$ and $H_i = \mathrm{Gal}(E/K_i)$. If $K_1 \subseteq K_2$, then $H_2 \subseteq H_1$. If $H_2 \subseteq H_1$, then $K_1 \subseteq K_2$. The second statement is for exercise.

3. Recall $H \trianglelefteq G$ iff $\sigma H \sigma^{-1} = H$ for all $\sigma \in G$.

   '$\Rightarrow$': Suppose K/F is normal, we will show that $\sigma(K) = K$ for all $\sigma \in G$ and by lemma, this will show that $\sigma H \sigma^{-1} = H$ (since $\sigma H \sigma^{-1} \longleftrightarrow \sigma(K)$)

   Since K/F is normal, let $u \in K$ such that $p(\lambda) \in F[\lambda]$ and $p(\lambda)$ has u as a root. Then $p(\lambda)$ splits as a product of degree 1 factors in $K[\lambda]$ so all roots of $p(\lambda)$ lies in K. Thus $\sigma(u) \in K$ for any $\sigma \in G$. (Recall that ${}^{\sigma}p(\lambda) = p(\lambda)$ should has $\sigma(u)$ as a root. Since we know all roots of $p(\lambda)$ is in K, thus $\sigma(u) \in K$.) Thus $\sigma(K) \subseteq K$ holds. Also for $\sigma^{-1} \in G$, we have $\sigma^{-1}(K) \subseteq K$ which implies $K \subseteq \sigma(K)$. So $K = \sigma(K)$.

   '$\Leftarrow$': Suppose $H \trianglelefteq G$. Then $\sigma H \sigma^{-1} = H$ for any $\sigma \in G$. Thus by lemma, $\sigma(K) = K$ for any $\sigma \in G$. For $\sigma \in G$, we have $\sigma|_K \in \mathrm{Gal}(K/F)$. Let $\overline{G} = \{\sigma|_K \mid \sigma \in G\}$, then $\overline{G} \leq_{\text{subgp}} \mathrm{Gal}(K/F)$. But since $\mathrm{Inv}(G) = F$, then we have $\mathrm{Inv}(\overline{G}) = F$. By Characterization of normal extensions, we have K/F is normal.

   To show the last statment, we need a homomorphism $\varphi : G = \mathrm{Gal}(E/F) \longrightarrow \mathrm{Gal}(K/F)$ such that $\sigma \longmapsto \sigma|_K$. $\mathrm{Ker}(\varphi) = \{\sigma \in G \mid \sigma(k) = k, \forall k \in K\} = \mathrm{Gal}(E/K) = H$. Also we need to show the surjectivity of φ. By Langrange's theorem, we know $|\mathrm{Im}(\varphi)| = |G|/|H| = |\mathrm{Gal}(K/F)|$. So φ has to be surjective. Then by the first isomorphic theorem, we have $\mathrm{Gal}(K/F) \simeq G/H$.

$\square$

Example. Suppose $f(\lambda) = \lambda^4 + 1 \in \mathbb{Q}[\lambda]$.

1. Write out the splitting field.

   Since $\lambda^8 - 1 = (\lambda^4 + 1)(\lambda^4 - 1)$. Then we see the roots of $\lambda^4 - 1$ are just $1, z^2, z^4, z^6$. And the roots of $\lambda^4 + 1$ are z, z^3, z^5, z^7. So the splitting field E is $\mathbb{Q}(z, z^3, z^5, z^7) = \mathbb{Q}(z_8)$.

2. What is $[E : \mathbb{Q}]$?

   Note $z + z^7 = \sqrt{2}$ and $z + z^3 = \sqrt{2}i$. So $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(i)$ is a subfield of E. By multiplicativity of degree, we have $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2, \text{ or } 4$. It cannot be 2 since $i \notin \mathbb{Q}(\sqrt{2})$. Thus $[E : \mathbb{Q}] = 4$.

3. Write G as a permutation group. $G = \mathrm{Gal}(\mathbb{Z}/\mathbb{Q})$

   Note $\lambda^4 + 1$ is therefore the minimal polynomial of z. Label roots as $r_1 = z_8, r_2 = z_8^3, r_3 = z_8^5, r_4 = z_8^7$. By extension theorem for simple extensions, $\exists \sigma \in G$, s.t. $\sigma(r_1) = z_8^3$.

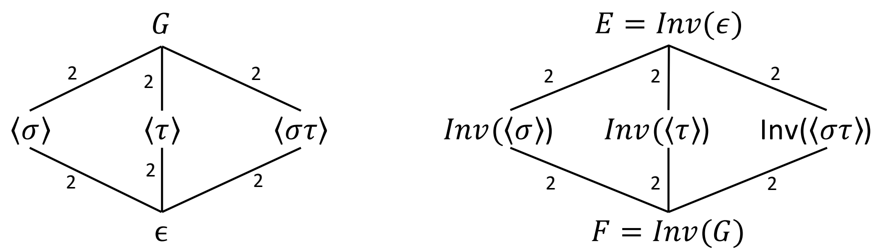
Then $\sigma(r_2) = \sigma(z_8^3) = \sigma(z_8)^3 = (z_8^3)^3 = z_8^9 = r_1$; $\sigma(r_3) = \sigma(z_8^5) = \sigma(z_8)^5 = (z_8^3)^5 = z_8^{15} = z_8^7 = r_4$; $\sigma(r_4) = \sigma(z_8^7) = \sigma(z_8)^7 = (z_8^3)^7 = z_8^{21} = z_8^5 = r_3$. Thus $\sigma = (12)(34)$.

Also there exists another $\tau \in G$ such that $\tau(r_1) = r_3$. Then similarly, we get $\tau(r_1) = r_3, \tau(r_2) = r_1, \tau(r_3) = r_1, \tau(r_4) = r_2$. Thus $\tau = (13)(24)$.

$\sigma\tau = (14)(23) \in G$.

So $G = \{\epsilon, \sigma, \tau, \sigma\tau\}$. It's the Klein 4 group.

4. Find all subgroups of G and their corresponding subfields. Since K_4 is abelian, so all subgroups are normal. Thus all corresponding subfields are normal extension.



$\text{Inv}(\langle\sigma\rangle)$:. $\sigma(r_1 + r_2) = r_2 + r_1 = \sqrt{2}i$. Claim $\text{Inv}(\langle\sigma\rangle) = \mathbb{Q}(\sqrt{2}i)$ by comparing degrees.

$\text{Inv}(\langle\tau\rangle)$:. $r_1 + r_3 = 0$. No extra information from this. Since $\tau(r_1) = r_3 = z_8^5 = -r_1$ So $\tau(r_1^2) = r_1^2 - i$. Claim $\text{Inv}(\langle\tau\rangle) = \mathbb{Q}(i)$ by comparing degrees.

$\text{Inv}(\langle\sigma\tau\rangle)$:. $\sqrt{2} = r_1 + r_4 \in \text{Inv}(\langle\sigma\tau\rangle)$. Claim $\text{Inv}(\langle\sigma\tau\rangle) = \mathbb{Q}(\sqrt{2})$ by comparing degrees.

In general, the splitting field of $x^n - 1$ is called a cyclotomic field.

- Roots are called nth roots of unity.
- If n is prime, then $\frac{\lambda^n - 1}{\lambda - 1}$ is the minimal polynomial of $z_n = e^{2\pi i/n}$. In our example, n is not a prime and also the minimal polynomial for z_8 is $\lambda^4 + 1$.
- In general, minimal polynomial of $z_n = e^{2\pi i/n}$ is $\prod_{\gcd(i,n)=1}(\lambda - z_n^i)$. So $[\mathbb{Q}(z_n) : \mathbb{Q}] = \varphi(n)$ (The Euler function. Number of i that coprime to n).