MAT 250A: Abstract Algebra

Greg DePaul

September 13, 2021

1 The Isomorphism Theorems

1.1 Quotient Groups

Definition 1.1. *A subgroup H of a group G is called normal provided for all $g \in G, gHg^{-1} = H$.*

Definition 1.2. *Suppose G a group, and H is a normal subgroup of G. Then we can define the quotient group of equivalence classes*

$$G/H := \{gH : g \in G\}$$

equipped with the binary operation:

$$gH \cdot g'H = gHg'H = gg'(g')^{-1}Hg'H = gg'HH = gg'H$$

Example 1.3. *A classic example is*

$$\mathbb{Z}/5\mathbb{Z} = \{g + 5\mathbb{Z} : g \in \mathbb{Z}\}$$

What are the equivalence classes, and or the elements of this quotient group? We see that all integers with remainder $gmod5$ upon division by 5 represent their own class. So:

$$\mathbb{Z}/5\mathbb{Z} = \{[1], [2], [3], [4], [5]\} \implies |\mathbb{Z}/5\mathbb{Z}| = 5$$

Example 1.4. *Let $GL_n(\mathbb{R})$ be the $n \times n$ invertible matrices with entries in $\mathbb{R}$ with non-zero determinant, while $SL_n(\mathbb{R})$ is the subgroup such that the determinant is exactly 1. Then we notice that $SL_n(\mathbb{R}) \trianglelefteq GL_n(\mathbb{R})$.*

So what are the cosets of $SL_n(\mathbb{R})$ in $GL_n(\mathbb{R})$?

$$AH = BH \iff A^{-1}B \in H \iff det(A) = det(B)$$

That is, there is one coset per each $r \in \mathbb{R}^\times$. Therefore, we see

$$GL_n(\mathbb{R})/SL_n(\mathbb{R}) \cong \mathbb{R}^\times$$

1.2 The First Isomorphism Theorem

Theorem 1.5. *First Isomorphism Theorem If $\phi : G \to G'$ is a group homomorphism, then $H := ker(\phi) \trianglelefteq G$ and $G/H \cong Im(\phi)$.*

Example 1.6. *Define* $\phi : GL_n(\mathbb{R}) \to \mathbb{R}^\times$ *such that*

$$\phi(A) = det(A)$$

Then ϕ *is a group homomorphism and* $ker(\phi) = SL_n(\mathbb{R})$ *and* $Im(\phi) = \mathbb{R}^\times$. *Therefore, by the First Isomorphism Theorem,*

$$GL_n(\mathbb{R})/SL_n(\mathbb{R}) \cong \mathbb{R}^\times$$

Proof. (Of the First Isomorphism Theorem)

- To show the normality of H:
  Suppose $h \in ker(\phi) = H \iff phi(h) = 1$. Then

  $$\phi(ghg^{-1}) = \phi(g) \cdot 1 \cdot \phi(g^{-1}) = \phi(gg^{-1}) = \phi(e) = 1 \implies H \trianglelefteq G$$

- Now to show $G/H \cong Im(\phi)$
  Consider

  $$\begin{aligned} f : G/H &\to Im(\phi) \\ gH &\to \phi(g) \end{aligned}$$

  To check that f is well defined, we see:

  $$gH = g'H \implies g = g'h \implies \phi(g) = \phi(g'h) = \phi(g')\phi(h) = \phi(g')$$

  To show that its a homomorphism, we need to show three things:

  1. f is a homomorphism
     Exercise
  2. $ker(f) = \{[1]\}$

     $$f(gH) = \phi(g) = 1 \iff g \in ker(\phi) \iff gH = eH \implies g \in [e] \implies ker(f) = \{[1]\}$$

  3. f is onto.
     Exercise

  Since f is an isomorphism, we conclude $G/H \cong Im(\phi)$

■

Definition 1.7. *A sequence of group homomorphisms*

$$G_1 \xrightarrow{\phi_1} G_2 \xrightarrow{\phi_2} G_3 \xrightarrow{\phi_3} \dots \xrightarrow{\phi_{k-1}} G_k$$

is <u>exact</u> *if and only if* $Im(\phi_i) = ker(\phi_{i+1})$ *for all* $1 \leq i \leq k-2$.

Consider the following diagram:

$$\begin{array}{ccccccccc} 1 & \xrightarrow{trivial} & H & \xrightarrow{inclusion} & G & \xrightarrow{\phi} & Im(\phi) & \xrightarrow{trivial} & 1 \\ \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\ 1 & \xrightarrow{trivial} & H & \xrightarrow{inclusion} & G & \xrightarrow{\text{canonical morphism}} & G/H & \xrightarrow{trivial} & 1 \end{array}$$

This diagram is commutes.

1.3 The Second Isomorphism Theorem

Definition 1.8. *Given a subgroup $K \subset G$, the normalizer N_K is the set:*

$$N_K := \{g \in H : gKg^{-1} = K\}$$

Theorem 1.9. *The Second Isomorphism Theorem Let G be a group, H, K are subgroups where $H \subset N_K$, then*

1. *The set $HK := \{hk : h \in H, k \in K\}$ is a group.*
2. *$H \cap K \trianglelefteq H$*
3. *$K \trianglelefteq HK$, and*
4. *$H/H \cap K \cong HK/K$*

Proof. 1. Since $H \subset N_K$, then

$$hkh'k' = \underbrace{h\,\underbrace{h'\underbrace{(h')^{-1}kh'}_{\in K}}_{\in K}\,k'}_{\in K} \in HK$$

Also, given $hk \in HK$, we have

$$k^{-1}h^{-1} = h^{-1}\underbrace{hk^{-1}h^{-1}}_{\in K} \in HK$$

Therefore, HK is a subgroup. In fact, since $H \subset N_K$, then $HK = KH$. Notice, we heavily relied on the fact that H resides within the normalizer of K.

2. If follows immediately $H \cap K \trianglelefteq H$ since H normalizes K.

3. To see $K \trianglelefteq HK$, we write

$$h\underbrace{kKk^{-1}}_{\in K}h^{-1} = K$$

since $H \subset N_K$.

4. Let $\phi : H \to HK/K$ be defined as

$$h \xrightarrow{\phi} (he)K$$

We need to check that ϕ is a surjective group homomorphism. We see:

$$ker(\phi) = H \cap K \text{ since } hK = K \iff h \in K$$

So by the first isomorphism theorem, we see:

$$H/H \cap K \cong H/ker(\phi) \cong Im(\phi) \cong HK/K$$

■

Example 1.10. *Consider the map $\phi : \mathbb{Z} \to 2\mathbb{Z}$ defined by*

$$a \xrightarrow{\phi} 2a$$

Since $ker(\phi) = \{0\}$, by the First Isomorphism Theorem, we see:

$$\mathbb{Z} \cong \mathbb{Z}/\{0\} \cong 2\mathbb{Z}$$

1.4 The Third Isomorphism Theorem (Dr. Fuch's Favorite)

Theorem 1.11. *The Third Isomorphism Theorem Let G be a group, $H \trianglelefteq G, K \trianglelefteq G, K \subset H$. Then $K \trianglelefteq H$ and*

$$(G/K)/(H/K) \cong G/H$$

Example 1.12.

$$(\mathbb{Z}/12\mathbb{Z})/(6\mathbb{Z}/12\mathbb{Z})$$

Notice, the cosets of $6\mathbb{Z}/12\mathbb{Z}$ are $\{[0],[6]\}$ while $\mathbb{Z}/12\mathbb{Z}$ has twelve cosets. So we'd expect the end up with 6 cosets as a result of this theorem.

Proof. (Of Third Isomorphism Theorem)

- We'll leave the proof of $K \trianglelefteq H$ as an exercise.
- Now define

$$\begin{aligned} \phi : G/K &\to G/H \\ gK &\to gH \end{aligned}$$

  We should check that ϕ is well-defined, a homomorphism, and surjective, which will also be left as an exercise. Now,

$$ker(\phi) = \{\text{cosets } gK : g \in H\} = H/K$$

  Therefore, by the first isomorphism theorem, we know

$$(G/K)/(H/K) \cong (G/K)/ker(\phi) \cong Im(\phi) \cong G/H$$

■

1.5 The Correspondence Theorem

Theorem 1.13. *Correspondence Theorem Let G be a group, and $N \trianglelefteq G$. There is a bijection of subgroups $A \leqslant G$ containing N and G/N. Further,*

- *Every subgroup of G/N is of the form A/N for some $A \leqslant G$ containing N.*
- $A \leqslant B \iff A/N \leqslant B/N$
- $A \leqslant B \implies [B : A] = [B/N : A/N]$
- $A \trianglelefteq G \iff A/N \trianglelefteq G/N$.

2 Composition Series

This technique allows us to build interesting groups from what we call simple groups.

Definition 2.1. *Recall, a group is simple provided it has no nontrivial normal subgroups.*

Definition 2.2. *A group G has a composition series if and only if it has a series of subgroups*

$$G = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \ldots \trianglelefteq G_r = \{e\}$$

such that for each quotient G_i/G_{i+1} is simple for all $0 \leq i \leq r-1$. Such a series is called a subnormal series and the quotient groups G_i/G_{i+1} are referred to as composition factors.

Example 2.3. *Consider S_5. We recall that $A_5 \trianglelefteq S_5$ and A_5 is simple. So*

$$S_5 \trianglelefteq A_5 \trianglelefteq 1$$

is a composition series with composition factors:

$$S_5/A_5 \cong \mathbb{Z}/2\mathbb{Z}$$

$$A_5/1 \cong A_5$$

Example 2.4. *Does $\mathbb{Z}$ have a composition series? If so, then we want*

$$\mathbb{Z} \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_{r-1} \trianglelefteq \{0\}$$

Notice, G_{r-1} must be abelian since $\mathbb{Z}$ is abelian as well as being nontrivial. Further, all G_{r-1}'s subgroups are normal. In particular, if we consider $2G_{r-1}$, it is a normal subgroup. However, this shows G_{r-1} is not simple! Therefore, there cannot exist a composition series for $\mathbb{Z}$.

2.1 Existence of Composition Series for Finite Groups

Theorem 2.5. *Every finite group G has a composition series.*

Proof. Applying induction over the order of G.
Basis of Induction: $G = \{e\} \trianglelefteq \{e\}$.
Inductive Step: Suppose $|G| < n \implies G$ has a composition series. Now consider a group G of order n.

- G is simple, then G has the composition series:

$$G \trianglelefteq \{e\}$$

- G is not simple, then let $H \trianglelefteq G$ be a maximal, normal subgroup. So $H \neq G$ and G/H is simple.

  Note 2.6. *Such an H exists because G is finite, and we can apply the correspondence theorem. Specifically, for any $N \trianglelefteq G$, we assume we can identify N' such that $G \trianglelefteq N' \trianglelefteq N$. Clearly, we must terminate at some point due to the finiteness of G.*

  Now, since $|H| < n$, we know H has a composition series,

$$H \trianglelefteq H_1 \trianglelefteq H_2 \trianglelefteq \ldots \trianglelefteq H_r = \{e\}$$

  Then we arrive at the subnormal series:

$$G \trianglelefteq H \trianglelefteq H_1 \trianglelefteq H_2 \trianglelefteq \ldots \trianglelefteq H_r = \{e\}$$

  Further, since H is a maximal subgroup of G, we know G/H is simple. Therefore, this series also serves as a composition series!

■

2.2 Interesting Examples

Example 2.7.

$$\mathbb{Z}/pq\mathbb{Z} \trianglelefteq q\mathbb{Z}/pg\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z} \trianglelefteq \{0\}$$

is a composition series with composition factors:

$$\mathbb{Z}/p\mathbb{Z} \text{ and } \mathbb{Z}/q\mathbb{Z}$$

Question 2.8. *Can we say no infinite group has a composition series?* $\implies$ *No!*

Example 2.9. *Claim:* $SL_2(\mathbb{R}) \trianglelefteq \{\pm I\} \trianglelefteq \{e\}$ *is a composition series.*
Checking the composition factors:

$$\{\pm I\} \cong \mathbb{Z}/2\mathbb{Z} \text{ is simple}$$

$$SL_2(\mathbb{R})/\{\pm I\} \cong PSL_2(\mathbb{R}) \text{ is simple (Proof on course website)}$$

Notice that the subgroup of $SL_2(\mathbb{R})$ *generated by*

$$\left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle \cong \mathbb{Z}$$

which does not have a composition series!

Remark 2.10. *Two different groups can have composition series with the same composition factors.*

Example 2.11. $D_q := \langle x, y\rangle$ *where* $x^4 = y^2 = 1$ *and* $yx = x^3y$. *Since it's finite, it should have a composition series, specifically,*

$$D_q \trianglelefteq \langle x\rangle \trianglelefteq \langle x^2\rangle \trianglelefteq \{1\}$$

with composition factors:

$$D_q/\langle x\rangle \cong \mathbb{Z}/2\mathbb{Z}$$
$$\langle x^2\rangle/\langle x\rangle \cong \mathbb{Z}/2\mathbb{Z}$$

This isn't unique! There are a total of 6 ways to write this composition series.

Example 2.12.

$$\mathbb{Z}/8\mathbb{Z} \trianglelefteq 2\mathbb{Z}/8\mathbb{Z} \trianglelefteq 4\mathbb{Z}/8\mathbb{Z} \trianglelefteq \{0\}$$

with composition factors all congruent to $\mathbb{Z}/2\mathbb{Z}$

Remark 2.13. *Groups in a composition series of* G *need not be normal in* G.

Example 2.14.

$$S_4 \trianglerighteq A_4 \trianglerighteq \underbrace{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}}_{\langle (1,2),(3,4),(1,3),(2,4)\rangle} \trianglerighteq \underbrace{\mathbb{Z}/2\mathbb{Z}}_{\langle (1,2),(3,4)\rangle} \trianglerighteq 1$$

However,

$$\langle (1,2),(3,4)\rangle \not\trianglelefteq S_4$$

Remark 2.15. *You can get groups where all permutations of composition factors are possible!*

Example 2.16. *Let* $Simp_1, \ldots, Simp_k$ *be* k *simple groups. Then*

$$Simp_1 \times \ldots \times Simp_k \trianglerighteq (\text{product of any } k-1 \text{ simple groups}) \trianglerighteq \ldots \trianglerighteq \{e\}$$

Remark 2.17. *You can also have groups that lack the ability to permute normal groups.*

Example 2.18. *Consider* $D_{12} = \langle x, y | x^6 = y^2 = 1, yx = x^5y\rangle$. *Then*

$$D_{12} \trianglerighteq \langle x\rangle \trianglerighteq \langle x^2\rangle \trianglerighteq 1$$

with composition series $\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}$, *and* $\mathbb{Z}/3\mathbb{Z}$. *As an exercise, show there are no normal order 4 subgroups of* D_{12}, *which can be done easily using the Sylow Theorems. Notice, another series must start with*

$$D_{12} \trianglerighteq \langle x\rangle \trianglerighteq \langle x^3\rangle \trianglerighteq 1$$

We also leave as an exercise to find the other two composition series.

2.3 Jordan-Holder Program

Theorem 2.19. *Let G be a group with a composition series and let $N \trianglelefteq G$. Then N also has a composition series.*

Proof. We consider the series

$$G = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_r = 1$$

Define $N_i = N \cap G_i$. We shall leave it as an exercise to prove the claim that $G_{i+1}/G_i \implies N_{i+1} \trianglelefteq N_i$. Now consider,

$$N_i/N_{i+1} = N \cap G_i/N_{i+1} \cap G_{i+1} \cong (N \cap G_i)G_{i+1}/G_{i+1}$$

Now, we consider the canonical projection

$$\pi : G_i \to G_i/G_{i+1}$$

which has the interesting property

$$(N \cap G_i)G_{i+1}/G_{i+1} = \pi(N \cap G_i) \trianglelefteq \pi(G_i)$$

since $N \cap G_i \trianglelefteq G_i$. Further,

$$(N \cap G_i)G_{i+1}/G_{i+1} \cong N_i/N_{i+1} \trianglelefteq G_i/G_{i+1} = \pi(G_i) \text{ which is simple}$$

Therefore, $N_i/N_{i+1} = G_i/G_{i+1} \implies N_i/N_{i+1}$ is simple or $N_i = N_{i+1} \implies$ trivial. Therefore, we can finally write the subnormal series:

$$N = N_0 \trianglelefteq N_1 \trianglelefteq \ldots \trianglelefteq N_r = 1$$

Further, we can reduce this chain by crossing out $N_i = N_{i+1}$, leaving us with a composition series for N! ■

Theorem 2.20. *Jordan-Hölder Let G be a group with a composition series. Then any two composition series of G of the same length are equivalent*

$$G = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_r \trianglelefteq 1$$

$$G = H_0 \trianglelefteq H_1 \trianglelefteq \ldots \trianglelefteq H_r \trianglelefteq 1$$

under the relation

$$\{G_i/G_{i+1} : 0 \leq i \leq r-1\} = \{H_i/H_{i+1} : 0 \leq i \leq r-1\}$$

That is, they are equivalent in their composition factors! (Notice, the order at which these factors appear are not the same).

Proof. We can assume G has at least two composition series:

$$G = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_r \trianglelefteq 1$$

$$G = H_0 \trianglelefteq H_1 \trianglelefteq \ldots \trianglelefteq H_s \trianglelefteq 1$$

We can assume without loss of generality that $r \leq s$. We shall prove this via induction on r.

- *Basis of Induction:* When $r = 1$, we see have the composition series:

$$G = G_0 \trianglelefteq G_1 = \{e\} \implies G \cong G_0/G_1 \text{ is simple}$$

Therefore, G has only one proper normal subgroup, and therefore $s = 1$ with an equivalent composition series.

- *Inductive Step:* Now suppose that the theorem is true for every group with a composition series of length less than r.

  - *Case:* Suppose $G_1 = H_1$. Then we have

$$G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \ldots \trianglelefteq G_r$$

$$G_0 \trianglelefteq G_1 \trianglelefteq H_2 \trianglelefteq \ldots \trianglelefteq H_r$$

But we see,

$$G_1 \trianglelefteq G_2 \trianglelefteq \ldots \trianglelefteq G_r$$

$$G_1 \trianglelefteq H_2 \trianglelefteq \ldots \trianglelefteq H_r$$

are two composition series of length $r - 1$. Therefore, by our inductive hypothesis, we see $r = s$ and the series are equivalent. Further, the composition factors

$$G_0/G \cong H_0/H_1$$

and the remaining composition factors are equivalent by the inductive hypothesis.

  - *Case:* $G_1 \neq H_1$. Note that $G_1 \trianglelefteq G, H_1 \trianglelefteq G \implies G_1H_1 \trianglelefteq G$. So

$$G_1H_1/G_1 \cong \underbrace{G/G_1}_{\text{simple}}$$

by the correspondence theorem. On the other hand, by the second isomorphism theorem,

$$G_1H_1/G_1 \cong H_1/H_1 \cap G_1$$

Also,

$$G_1H_1/H_1 \cong \underbrace{G/H_1}_{\text{simple}}$$

Claim: $G_1 \not\leq H$
We know $G_1 \neq H_1$. If $G_1 < H_1$, then

$$H_1/G_1 \cap H_1 = H_1/G_1 \trianglelefteq G/G_1$$

since $H_1 \trianglelefteq G$. But we found a proper, nontrivial normal subgroup of a simple group, which is a contradiction. So we can't have $G_1 \not\leq H$.

In particular, we must see that $H_1 \trianglelefteq G_1H_1$. So

$$G_1/H_1 \cap G_1 \cong G_1H_1/H_1 \trianglelefteq G/H_1$$

We must have $G_1H_1/H_1 = G/H_1$, which can only happen if $G = G_1H_1$. Now let $K = G_1 \cap H_1 \trianglelefteq G$.

Note 2.21. *$G/G_1 \cong H_1/K$ by the second isomorphism theorem. Further, this group is simple. Also, $G/H_1 \cong G_1/K$ which is also simple.*

Since $K \trianglelefteq G$, then by the previous theorem K has a composition series.

$$K = K_0 \trianglelefteq K_1 \trianglelefteq K_2 \trianglelefteq \ldots \trianglelefteq K_t = \{e\}$$

Then have three composition series:

$$G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \ldots \trianglelefteq G_r$$

$$G_0 \trianglelefteq G_1 \trianglelefteq K \trianglelefteq K_1 \trianglelefteq \ldots \trianglelefteq G_t$$

$$G_0 \trianglelefteq H_1 \trianglelefteq H_2 \trianglelefteq \ldots \trianglelefteq H_r$$

$$G_0 \trianglelefteq H_1 \trianglelefteq K \trianglelefteq K_1 \trianglelefteq \ldots \trianglelefteq G_t$$

By the induction hypothesis, we see:

$$G_1 \trianglelefteq G_2 \trianglelefteq \ldots \trianglelefteq G_r$$

$$G_1 \trianglelefteq K_0 \trianglelefteq K_1 \trianglelefteq \ldots \trianglelefteq G_t$$

are equivalent by the induction hypothesis with $t = r - 2$. Also,

$$\{G_1/G_2 \ldots., G_{r-1}/G_r\} = \{G_1/K_0, K_0/K_1, \ldots, K_{r-3}/K_{r-2}\}$$

Further, the same can be said about the series

$$H_1 \trianglelefteq K \trianglelefteq K_1 \trianglelefteq \ldots \trianglelefteq G_t$$

Therefore,

$$\{H_1/H_2 \ldots., H_{s-1}/H_s\} = \{H_1/K_0, K_0/K_1, \ldots, K_{r-3}/K_{r-2}\}$$

Lastly, we already know by the previous note that $G/H_1 \cong G_1/K_0$. So

$$\begin{aligned}\{G/H_1, H_1/H_2, \ldots, H_{r-1}/H_r\} &= \{G/K, H_1/K_0, \ldots, K_{r-3}/K_{r-2}\} \\ &= \{G_1/K, G/G_1, K_0/K_1, \ldots, K_{r-3}/K_{r-2}\} \\ &= \{G/G_1, G_1/G_2, \ldots, G_{r-1}/G_r\}\end{aligned}$$

■

Remark 2.22. *As a special case of Jordan-Holder is unique factorization in $\mathbb{Z}$.*

Example 2.23. *Let $n > 1$ and $n \in \mathbb{Z}$, such that*

$$n = p_1^{r_1} \ldots p_k^{r_k}$$

Then

$$(\mathbb{Z}_{p_1})^{r_1} \times (\mathbb{Z}_{p_2})^{r_2} \times (\mathbb{Z}_{p_k})^{r_k} \trianglerighteq (\mathbb{Z}_{p_1})^{r_1 - 1} \times (\mathbb{Z}_{p_2})^{r_2} \times (\mathbb{Z}_{p_k})^{r_k} \trianglerighteq \ldots$$

Now in order to ensure the simplicity of the composition factors, we do need to show care when it comes to the order of the normal groups.

3 Solvable Groups

3.1 Other Interesting Series

- We already know where a subnormal series is:

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \ldots \trianglerighteq G_m$$

- A abelian series is:

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \ldots \trianglerighteq G_m$$

  such that

$$G_{i+1}/G_i \text{ is abelian}$$

- A cyclic series is:

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \ldots \trianglerighteq G_m$$

  such that

$$G_{i+1}/G_i \text{ is cyclic}$$

We notice, that each of the series can be "transformed" or "refined" into eachother.

Definition 3.1. *A refinement of a series*

$$G_0 > G_1 > \ldots > G_m$$

is a series obtained by inserting finitely many subgroups into the series.

Definition 3.2. *A group which admits an abelian series ending with 1 is called solvable.*

Example 3.3.

$$S_4 \trianglerighteq A_4 \trianglerighteq 1$$

which has an abelian refinement

$$S_4 \trianglerighteq A_4 \trianglerighteq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \trianglerighteq 1$$

as well as a cyclic refinement

$$S_4 \trianglerighteq A_4 \trianglerighteq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \trianglerighteq \mathbb{Z}/2\mathbb{Z} \trianglerighteq 1$$

Theorem 3.4. *Every abelian series of a finite group G_0 admits a cyclic series.*

In order to prove this theorem, we need to rely on a useful lemma.

Lemma 3.5. *Let $f : G \to G^1$ be a homomorphism, and let*

$$G' = G'_0 \trianglerighteq \ldots \trianglerighteq G'_m$$

be a subnormal series. Let $G_i = f^{-1}(G'_i)$. Then

$$G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \ldots \trianglerighteq G_m$$

is a subnormal series. If the G'_i's form an abelian (or cyclic) series, then the G_i's form an abelian (or cyclic) series.

Proof. Check $G_0 \trianglerighteq \ldots \trianglerighteq G_m$ is a subnormal series. Note that the map

$$\begin{aligned} \phi : G_i/G_{i+1} &\to G_i'/G_{i+1}' \\ gG_{i+1} &\to f(g)G_{i+1}' \end{aligned}$$

is a well defined, injective homomorphism. This tells us

$$G_i/G_{i+1} \cong H \leqslant G_i'/G_{i+1}'$$

Since a subgroup of an abelian is abelian (or a subgroup of a cyclic group is cyclic), then it follows H is abelian (cyclic). Therefore,

$$G_i/G_{i+1} \text{ is abelian (or cyclic)}$$

■

Proof. (Of Theorem)
Basis of Induction: Let $|G_0| = 1 \implies$ trivial!
Inductive Step: Suppose this theorem is true for all groups G or order less than n. Now, let $|G_0| = n$ and consider an abelian series:

$$G_0 \trianglerighteq G_1 \trianglerighteq \ldots \trianglerighteq G_m$$

By the inductive hypothesis, $G_1 \trianglerighteq \ldots \trianglerighteq G_m$ must have a cyclic refinement since $|G_1| < n$. That is,

$$G_1 \trianglerighteq H_1 \trianglerighteq \ldots \trianglerighteq H_k$$

is a cyclic refinement. Now consider the canonical map:

$$\begin{aligned} f : G_0 &\to G_0/G_1 \\ g &\to gG_1 \end{aligned}$$

We have

$$\begin{array}{ccccc} G_0 & \trianglerighteq & G_1 & \text{(abelian series)} \\ \downarrow_f & & \downarrow_f & \\ G_0/G_1 & \trianglerighteq & 1 & \text{(abelian series)} \end{array}$$

Case: If $G_1 \neq 1$, then $|G_0/G_1| < n$, and so by the inductive hypothesis, the bottom abelian series admits a cyclic refinement, and the lemma says its preimage is also a cyclic series. Therefore,

$$G_0 \trianglerighteq K_1 \trianglerighteq \ldots \trianglerighteq G_1 \trianglerighteq H_1 \trianglerighteq \ldots \trianglerighteq H_k$$

Case: If $G_1 = 1$, we have

$$G_0 \cong G_0/G_1 \text{ is abelian}$$

Let $x_0 \in G_0, x \neq 1$, let $K = \langle x \rangle \neq 1$.

- If $K = G_0$, we are done!
- If $K \neq G_0$, then let

  $$\pi : G_0 \to G_0/K$$

  which is well defined since every subgroup of an abelian group is normal. Then

  $$\begin{array}{ccccc} G_0 & \trianglerighteq & 1 & \text{(abelian series)} \\ \downarrow_\pi & & \downarrow_\pi & \\ G_0/K & \trianglerighteq & 1 & \text{(abelian series)} \end{array}$$

  By the induction hypothesis, the bottom series admits a cyclic refinement since $|G_0/K| < n$. By the lemma, we know this refinement lifts its cyclic refinement to a cyclic refinement of the top series!

  $$G_0 \trianglerighteq L_1 \trianglerighteq \ldots \trianglerighteq K \trianglerighteq 1$$

■

Corollary 3.5.1. *A finite solvable group admits a cyclic series ending with 1.*

Example 3.6. *Recall the group S_4 is solvable by:*

$$S_4 \trianglerighteq A_4 \trianglerighteq \mathbb{Z}_2 \times \mathbb{Z}_2 \trianglerighteq \mathbb{Z}_2 \trianglerighteq 1$$

S_3 is also solvable with

$$S_3 \trianglerighteq A_4 \trianglerighteq 1$$

So one might be tempted to ask is this is true for any n? Turns out, S_n is not solvable for $n \geq 5$. This is because A_n is simple for $n \geq 5$ and not abelian. (Proof available on course website)

3.2 The Derived Series

Recall, the commutator subgroup of G is given by

$$[G, G] := \{ghg^{-1}h^{-1} : g, h \in G\}$$

Lemma 3.7. *$G/[G, G]$ is abelian.*

Proof.

$$h[G,G] \cdot h'[G,G] = hh'[G,G] = hh'(h')^{-1}h^{-1}h'h[G,G] = h'h[G,G] = h'[G,G] \cdot h[G,G]$$

■

Lemma 3.8. *Also, if G/N is abelian, then $[G, G] \leqslant N$.*

Proof.

$$hh'N = h'hN \implies hh'h^{-1}h'^{-1} \in N \implies [G,G] \implies [G,G] \leqslant N$$

■

Definition 3.9. *Let*

$$G^{(0)} = G, G^{(1)} = [G, G], G^{(2)} = [G^{(1)}, G^{(1)}], \ldots, G^{(i)} = [G^{(i-1)}, G^{(i-1)}]$$

Then the series

$$G = G^{(0)} \trianglerighteq G^{(1)} \trianglerighteq G^{(1)} \trianglerighteq \ldots \trianglerighteq G^n$$

is the derived series of G.

Theorem 3.10. *G is solvable if and only if $G^{(n)} = 1$ for some $n \geq 0$.*

Proof. ($\Leftarrow$). Let $G^{(n)} = 1$. Then

$$G = G^{(0)} \trianglerighteq G^{(1)} \trianglerighteq G^{(1)} \trianglerighteq \ldots \trianglerighteq G^n$$

is an abelian series ending with 1.
($\Rightarrow$) Suppose G is solvable. Then G possesses an abelian series

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \ldots \trianglerighteq G_m = 1$$

Claim: $G^{(i)} \leqslant G_i$ for all i.
Basis: $G^{(0)} = G_0$.
Inductive Step: Suppose $G^{(i)} \leqslant G_i$ for all $i < k$. Now,

$$G^{(k)} = [G^{(k-1)}, G^{(k-1)}] \leqslant [G_{k-1}, G_{k-1}] \leqslant G_k$$

since G_{k-1}/G_k is abelian. So

$$G^{(m)} \leqslant G_m = 1 \implies G^{(m)} = 1$$

■

Now we can prove a pretty major theorem,

Theorem 3.11. *Let G be a group, let $H \trianglerighteq G$. then G is solvable if and only if H and G/H is solvable.*

Proof. ($\Rightarrow$) Suppose G is solvable. Then

$$G^{(0)} \trianglerighteq G^{(1)} \trianglerighteq \ldots \trianglerighteq G^{(m)} = 1$$

Note that $H^{(i)} \leqslant G^{(i)}$ for all i. So we get

$$H^{(0)} \trianglerighteq \ldots \trianglerighteq H^{(m)} = 1 \implies H \text{ is solvable}$$

Now consider our favorite map, the canonical map

$$\begin{aligned} G &\xrightarrow{f} G/H = K \\ g &\to gH \end{aligned}$$

Exercise 3.12. $f(G^{(i)} = K^{(i)}$.

As a result of this exercise, we have

$$K = K^{(0)} \trianglerighteq K^{(1)} \trianglerighteq \ldots \trianglerighteq K^{(m)} = 1$$

Therefore, $K = G/H$ is solvable. ($\Leftarrow$) If $K = G/H$ and H are solvable, we have

$$\begin{aligned} G &\xrightarrow{f} G/H = K \\ g &\to gH \end{aligned}$$

Now we can pull back from K,

$$K = K^{(0)} \trianglerighteq K^{(1)} \trianglelefteq \ldots \trianglerighteq K^{(n)} = 1$$

Then the series

$$G^{(0)} \trianglerighteq G^{(1)} \trianglerighteq \ldots \trianglerighteq \underbrace{G^{(n)}}_{\leqslant H}$$

Since H is solvable, we can chain abelian series of H to complete the series of $G^{(0)}$ ∎

Corollary 3.12.1. *S_n is <u>not</u> solvable for $n \geq 5$.*

Example 3.13.

$$D_{2n} \trianglerighteq \underbrace{[D_{2n}, D_{2n}] = \langle r^2 \rangle}_{D_{2n}^{(1)}} \trianglerighteq \underbrace{1}_{D_{2n}^{(2)}}$$

Example 3.14.

$$S_n \trianglerighteq [S_n, S_n] = A_n$$

This is because $g \in S_n$ can be written $g = (a,b,c) = (a,c,b)^2 = ((a,b),(a,c))^2$ and since 3-cycles generate A_n for $n \geq 3$ and $[S_n, S_n] \leqslant A_n$. Therefore we reach equality. If $n \geq 5$, then A_n is simple $\implies$ $[A_n, A_n]$ is 1 or A_n. So we see:

$$S_n \trianglerighteq A_n \trianglerighteq A_n \trianglerighteq \ldots \trianglerighteq A_n \trianglerighteq \ldots$$

Notice we don't get termination.

Example 3.15. $[GL_2(\mathbb{Q}), GL_2(\mathbb{Q})] = SL_2(\mathbb{Q})$ *and* $[SL_2(\mathbb{Q}), SL_2(\mathbb{Q})] = SL_2(\mathbb{Q})$.

4 Group Actions

4.1 A Toolbox of Theoretic Techniques (aka Review)

Definition 4.1. *A group action of G on a set S is a map*

$$G \times S \to S$$
$$(g, s) \to gs$$

such that

- $es = s$ *for all* $s \in S$,
- $(gh)s = g(hs)$ *for all* $g, h \in H$ *and* $s \in S$

Definition 4.2. *We define* $G_s := \{g \in G : gs = s\}$ *as the stabilizer of* s *in* G. *This is a subgroup of* G.

Definition 4.3. *We define* $O_s := \{gs : g \in G\}$ *as the orbit of* s *in* G.

Theorem 4.4. *The orbits* O_s *partition* S, *so for some indexing set* I,

$$S = \bigsqcup_{i=I} O_{s_i}$$

Theorem 4.5 (Orbit Stabilizer)**.** *If* $[G : G_s]$ *is finite, then* $|O_s| = [G : G_s]$. *Otherwise,* O_s *has infinitely many elements.*

Example 4.6. *Let* $H \trianglelefteq G$. *Then* G *acts on* H *by conjugation:*

$$g(h) = ghg^{-1}$$

Example 4.7. *Let* $H \leqslant G$. *Then* G/H *is the set of left cosets of* H *in* G. G *acts on* G/H *by*

$$g(g'H) = (gg')H$$

Corollary 4.7.1 (For Conjugation Actions)**.** *If* $H \leqslant G$. *Then the number of subgroups of* G *conjugate to* H *is the index* $[G : N_H]$ *of the normalizer of* H *in* G.

Theorem 4.8 (Orbit Decomposition Formula)**.** *If* S *is finite, then*

$$|S| = \sum_{i \in I} [G : G_{s_i}]$$

Theorem 4.9 (The Class Equation)**.** *Let* G *be a finite group, then*

$$|G| = \sum_{x \in C} [G : G_x] = |Z(G)| + \sum_{x \in C, x \notin Z(G)} [G : C_G(x)]$$

where C *is a set of representatives for distinct conjugacy classes* $\{gxg^{-1} : g \in G\}$, *and*

$$C_G(x) := \{g \in G : gx = xg\}$$

Proof. The first equals sign is the result of the orbit decomposition formula, where G acts on G by conjugation. x is alone in a conjugacy class if and only if $x \in Z(G)$. So

$$\sum_{x \in C} [G : G_x] = |Z(G)| + \sum_{x \in C, x \notin Z(G)} [G : G_x]$$

where $G_x = \{g \in G : gxg^{-1} = x\}$. But we see:

$$G_x = \{g \in G : gxg^{-1} = x\} = C_G(x) = \{g \in G : gx = xg\}$$

■

Definition 4.10. *If X, Y are G-sets, then $\phi : X \to Y$ is a <u>G-set homomorphism</u> if*

$$\phi(gx) = g\phi(x)$$

for all $g \in G, x \in X$. If ϕ is bijective, then ϕ is a <u>G-set isomorphism.</u>

Note 4.11. *To prove the Orbit-Stabilizer Theorem, one shows that X is a transitive G-set, then*

$$X \cong G/G_x$$

for any $x \in X$.

Theorem 4.12. *If $H, K \leqslant G$, then the G-sets G/H and G/K are isomorphic if and only if H and K are conjugate in G.*

Remark 4.13. $x = H \in G/H \implies G_x = G$

Remark 4.14. *Every element $x' = H \in G/H$ is of the form gx for some $g \in G$. So u inG_x if and only if*

$$ux = ugx; = gxx'$$

if and only if

$$g^{-1}ug \in G_x = H.$$

Also, every group of the form gHg^{-1} stabilizes some element in G/H

$$\{\text{set of stabilities of } x' \in G/H\} = \{gHg^{-1} : g \in H\}$$

Proof. ($\Rightarrow$) If $G/H \cong G/K$ as G-sets, then the set of stabilizers of elements in G/H are the same as the set of stabilizers of element in G/K. This is because, for every $x \in G/H$ and suppose $g \in G_x$. Then

$$\phi(x) = \phi(gx) = \phi(g)\phi(x) \implies G_x \leqslant G_{\phi(x)} \forall x \in G/H$$

By the same argument,

$$G_{\phi(x)} \leqslant G_{\phi^{-1}\phi(x)} = G_x$$

Therefore, $G_x = G_{\phi(x)}$ for all $x \in G/H$. Moreover, this shows that H and K are conjugate. ($\Leftarrow$) Now suppose H and K are conjugate. Then

$$H = gKg^{-1}$$

for some $g \in G$. Moreover, H is the stabilizer of $gK \in G/K$. We now define the map

$$\begin{aligned} \phi : G/H &\to G/K \\ g'H &\to g'gK \end{aligned}$$

Checking that ϕ is a G-set homomorphism:

- *Claim:* ϕ is well-defined
  Check

- *Claim:* ϕ is one-to-one
  Suppose $\phi(g_1'H) = \phi(g_2'H)$. Then
  $$g_1'gK = g_2'gK$$
  $$\implies (g_1'g)^{-1}g_2'g = g^{-1}(g_1')^{-1}g_2'g \in K$$
  $$\implies (g_1')^{-1}g_2' \in gKg^{-1} = H$$
  Therefore, $g_1'H = g_2'H$

- *Claim:* ϕ is onto
  Check

■

A useful theorem to have as a tool:

Theorem 4.15. *Let G be finite, and p divides $|G|$ is the smallest prime dividing $|G|$. Then if $[G : H] = p$ then*
$$H \trianglelefteq G$$

4.2 Automorphism Groups

Definition 4.16. *Let G be a group. An automorphism of G is an isomorphism from G to G. The set of all automorphisms of G is called $Aut(G)$.*

Remark 4.17. *One should check that $Aut(G)$ is a group under composition of morphisms and a subgroup of $S_{|G|}$*

Theorem 4.18. *Let $H \trianglelefteq G$. Then for every $g \in G$, then conjugation $h \to ghg^{-1}$ is an automorphism of H. This provides a homomorphism $G \to Aut(H)$ with kernel $C_G(H)$. This implies*
$$G/C_G(H) \cong \text{ subgroup of } Aut(G)$$

Note 4.19. *If $K \leqslant G, g \in G$, then $K \cong gKg^{-1}$.*

Definition 4.20. *For $g \in G$, conjugation by g is called an inner automorphism of G. Further, the group of all inner automorphism is called $Inn(G)$.*

Remark 4.21. $Inn(G) \trianglelefteq Aut(G)$.

Remark 4.22. *By the previous theorem, $Inn(G) \cong G/Z(G)$.*

Question 4.23. *You might ask, since there are inner automorphisms, is there such a thing as outer automorphisms?*

Turns out there is some notion, by endowing the algebraic structure:
$$Out(G) = Aut(G)/Inn(G)$$

Example 4.24. $Inn(D_8) \cong D_8/Z(D_8) = D_8/\langle r^2 \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$

Example 4.25. *For $n \geq 3, Inn(S_n) \cong S_n/Z(S_n) \cong S_n$ since $Z(S_n)$ is trivial for $n \geq 3$.*
In fact, for $n \geq 3, n \neq 6, Aut(S_n) \cong S_n$ too! (Homework)

Example 4.26. *Let's consider $Aut(\mathbb{Z})$. That is,*

$$\phi : \mathbb{Z} \to \mathbb{Z}$$

Then $\phi(1) = 1$ or $\phi(1) = -1$. That is, when thinking of automorphisms, we have to think of where the generators are being sent. Specifically, generators map to generators.

Exercise 4.27. $Aut(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$

Exercise 4.28. $Aut(\mathbb{Z}/p\mathbb{Z}) \cong (\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$

4.3 Semi-Direct Products

We recall direct products written as $H \times K$. A generalization of this is the semi-direct product

$$H \rtimes K$$

Definition 4.29. *Let $H \leqslant G, N \trianglelefteq G, G = NH$ with $N \cap H = 1$. We call G the internal semi-direct product of N by H,*

$$G = N \rtimes H$$

If also $H \trianglelefteq G$, then $G \cong N \times H$.

Observations:

- $H \cong H/N \cap H \cong NH/N = G/N$. Further, if G is finite, then

$$|G| = |N| \cdot [G : N] = |N||H|$$

- $G = NH \implies x \in G$ then $x = nh$ for some $n \in N, h \in H$ uniquely
- If $x, y \in G, x = n_1h_1, y = n_2h_2$, then

$$\begin{aligned} xy &= (n_1h_1)(n_2h_2) \\ &= \underbrace{(n_1h_1)(n_2}_{\in N}\underbrace{h_1^{-1}h_1h_2)}_{\in H} \end{aligned}$$

- Let $h \in H, N \trianglelefteq G \implies hNh^{-1} = N$. Now let

$$\begin{aligned} \phi_h : N &\to N \\ n &\to hnh^{-1} \end{aligned}$$

  Therefore, $\phi_h \in Aut(N)$. So

$$\phi_h \circ \phi_{h'} = \phi_{hh'}$$

  So I have a homomorphism

$$\begin{aligned} \phi : H &\to Aut(N) \\ h &\to \phi_h \end{aligned}$$

  This is the "conjugation homomorphism" for semi-direct projects G.

  Note 4.30. *$(n_1h_1)(n_2h_2) = n_1\phi_{h_1}(n_2)h_1h_2$ for all $n_1, n_2 \in N, h_1, h_2 \in H$. This gives a way to express the group operation in G in terms of ϕ and the group operations separately in N and H.*

- What if $\phi : H \to Aut(N)$ were trivial? Then

$$nhn^{-1} = n\phi_h(n^{-1})h = nn^{-1}h = h \implies H \trianglelefteq G \implies G \cong N \times H$$

  Conversely, if $G = N \times H$, then the elements of H must commute with the elements of N, which implies ϕ is trivial!

- If $\phi : H \to Aut(N)$ is nontrivial, then G is nonabelian.

Definition 4.31. *Let H, N be groups, and let*

$$\begin{aligned} \phi : H &\to Aut(N) \\ h &\to \phi_h \end{aligned}$$

be a homomorphism. Let

$$G := \{(n, h) : n \in N, h \in H\}$$

with operation

$$(n_1, h_1)(n_2, h_2) = (n_1\phi_{h_1}(n_2), h_1h_2)$$

This is a group, denoted

$$N \rtimes_\phi H,$$

called the external semidirect product of N and H.

Note 4.32. *If ϕ is trivial, then $G \cong N \times H$.*

Theorem 4.33. *Let $N \cong \{(n, 1) : n \in N\} = \bar{N}$ and let $H \cong \{(1, h) : h \in H\} = \bar{H}$. Then*

- $\bar{N} \trianglelefteq N \rtimes_\phi H$
- $\bar{N} \cap \bar{H} = 1$
- *for all $\bar{n} \in \bar{N}, \bar{h} \in \bar{H}$, we have $\bar{h}\bar{n}\bar{h}^{-1} = (\phi_h(n), 1)$*
- $\bar{N}\bar{H} = N \rtimes_\phi H$

Example 4.34. *Consider $H = \langle h \rangle$, and let $n \in N$ where the order of n divides $|H|$. Define*

$$\begin{aligned} \phi : H &\to Aut(N) \\ h &\to n^{-1}(\cdot)n \end{aligned}$$

Now, letting $G = N \rtimes_\phi N$. We consider $\langle (n, h) \rangle \leqslant G$. Then

$$\langle (n, h) \rangle \cong H$$

Also, $\langle (n, h) \rangle \cap \bar{N} = 1$, therefore $G \cong N \rtimes H$.

Example 4.35. *Let $N = \mathbb{Z}/n\mathbb{Z}$ and $H = \mathbb{Z}/2\mathbb{Z}$. Then*

$$\begin{aligned} \phi : H &\to Aut(N) \\ 0 &\to e \\ 1 &\to \text{ inversion map } x \to -x \end{aligned}$$

Then we see that $N \rtimes_\phi H$ is generated by $(1,0)$ and $(1,1)$. Also,

$$\begin{aligned}(1,1)^2 &= (1+\phi_1(1), 1+1)\\ &= (1-1, 1+1)\\ &= (0,0)\end{aligned}$$

and

$$(1,0)^n = (0,0)$$

$$(1,0)(1,1) = (1+\phi_0(1), 0+1) = (2,1) = (1,1)(1,0)^{-1}$$

This is in fact D_{2n}!

Theorem 4.36. *The following are equivalent:*

1. *$N \rtimes_\phi H \cong N \times H$ with an injective map ϕ*
2. *$\phi : H \to Aut(N)$ is trivial*

Proof.

$$(1) \iff (n_1\phi_{h_1}(n_2), h_1h_2) = (n_1n_2, h_1, h_2) \iff \phi_h(n) = n \forall n \in N, h \in H \iff (2)$$

■

Exercise 4.37. *If $N \rtimes_\phi H$ is abelian, then N, H are abelian and ϕ must be trivial.*

Theorem 4.38 (Recognition)**.** *Suppose G is a group, $H, N \leqslant G$ with*

- *$N \trianglelefteq G$*
- *$N \cap H = 1$*

Let ϕ be a homomorphism

$$\begin{aligned}\phi : H &\to Aut(N)\\ h &\to h^{-1}(\cdot)h\end{aligned}$$

Then $NH \cong N \rtimes_\phi H$. If $G = NH$, then $G \cong N \rtimes_\phi H$.

Theorem 4.39. *Let p, q be primes such that $p \not| q-1, p \leq q$. Then any group G of order pq is abelian.*

Proof. $|Z(G)|$ divides pq. So $|Z(G)| = 1, p, q$ or pq

- *Case:* Suppose $Z(G) \neq 1$. Then $|Z(G)| = p, q$, or pq
  - *Subcase:* $|Z(G)| = pq \implies G$ is abelian.
  - *Subcase:* $|Z(G)| = p$ or $|Z(G)| = q$, then $G/Z(G)$ is cyclic $\implies G$ is abelian.
- *Case:* Suppose $Z(G) = 1$.
  Claim: G has a subgroup of order p and and subgroup of order q.
  Suppose G only has a subgroup of order p. Then by the class equation,

$$|G| = pq = |Z(G)| + \sum_{g \in G, g \notin Z(G)} [G : C_G(g)] = 1 + kq$$

But $pq \not\equiv 1 mod q \implies$ contradiction.

Now, let $|H| = p$ and $|N| = q$, with $H, N \leqslant G$. Then

$$[G : N] = p \implies N \trianglelefteq G$$

And $N \cap H = 1$. Finally $NH \leqslant G$ and $|NH| = pq \implies NH = G$. Further,

$$G = N \rtimes_\phi H$$

with

$$\phi : \underbrace{H}_{order p} \to \underbrace{Aut(N)}_{order q-1}$$

Either ϕ is trivial $\implies G \cong N \times H \cong \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ or $p|q-1 \implies$ contradiction!

■

5 Sylow Theorems

Definition 5.1. *G is a p-group, with p prime, provided $|G| = p^n$.*

Definition 5.2. *Let G be a finite group with $H \leqslant G$. Then H is a p-subgroup, with p prime, provided $|H| = p^n$. If n is the highest power of p dividing $|G|$, then H is called a p-Sylow subgroup.*

Example 5.3. *S_6 has a 3-Sylow Subgroup*

$$\langle (1,2,3),(4,5,6)\rangle \text{ with order } 9$$

as well as a 2-Sylow Subgroup

$$\langle (1,2,3,4),(3,4),(5,6)\rangle \text{ with order } 16$$

Question 5.4. *Is it true in general that if p divides the order of G, can it be said that G has a p-Sylow Subgroup?*

Theorem 5.5 (Sylow's First Theorem)**.** *Let p divide the order of G, with p prime. Then there exists a p-Sylow subgroup of G.*

In order to prove this theorem, we need the following Lemma:

Lemma 5.6. *Let G be finite and abelian, and let p be prime and p divides the order of G. The G has an element of order p.*

Proof. Homework ■

Proof. (Of Sylow's First Theorem)
We will induce on the order of G.

- Basis: When $|G| = 1$, then conclusion is immediate,
- Inductive Hypothesis: Suppose the theorem is proven for all G with $|G| < n$
- Inductive Step: Let $|G| = n$.
  - *Case:* If n is prime, then G is its own p-Sylow subgroup
  - *Case:* If there exists $H \leqslant G$ with $p \not| [G : H]$, then the highest power of p dividing $|H|$ is the same as the highest power of p dividing $|G|$. Therefore, any p-Sylow subgroup of H is a p-Sylow subgroup of G. Further, since H is a proper subgroup of G, it follow $|H| < n$. Therefore, by the inductive hypothesis, there exists a p-Sylow subgroup!
  - *Case:* Now if there exists $H \leqslant G$ with $p|[G : H]$, we an consider conjugation action of G on G. By the class equation

    $$|G| = |Z(G)| + \sum_{x \in C, x \notin Z(G)} [G : C_G(x)]$$

    By our assumption, we know p divides $[G : C_G(x)]$ and p divides $|G|$. Therefore,

    $$|Z(G)| = |G| - \sum_{x \in C, x \notin Z(G)} [G : C_G(x)]$$

    must also be divisible by $p \implies G$ has a nontrivial center. Now since $Z(G)$ is abelian, then $Z(G)$ contains an element of order p by the lemma mentioned. So

    $$\langle a \rangle \trianglelefteq Z(G) \quad \langle a \rangle \trianglelefteq G$$

Now, consider the canonical projection

$$\pi : G \to G/\langle a \rangle g \to g\langle a \rangle$$

And let p^n be the highest power of p dividing $|G|$. Then we see:

$$p^{n-1} \text{ divides } G/\langle a \rangle$$

and, by the inductive hypothesis, must have a p-Sylow subgroup K. Let $H = \pi^{-1}(K)$. We notice, $\langle a \rangle \leqslant H$ and $\pi(H) = K$, then

$$H/\langle a \rangle \cong K$$

with $|H| = p \cdot p^{n-1} = p^n$. But this is a contradiction!

■

To prove the remaining theorems, we would like to leverage the following lemma:

Lemma 5.7. *Let P be a p-Sylow subgroup of G. Let S be the set of all conjugates of P in G. Let $H \leqslant G$ be a p-subgroup, and therefore acts on S by conjugation. Then*

1. *p does not divide $|S|$*
2. *if $k := \#\{$ fixed points of H acting on $S\}$, then*

$$k \equiv |S| (mod p)$$

3. *If $k = 1$, then $|S| \equiv 1 (mod p)$*

Proof. 1. Consider the action of G on all subgroups of G by conjugation. Then $|S| = [G : G_p] = [G : N_P]$ where we have $P \leqslant N_P \implies |N_P|$ is divisible by the highest power of p dividing G. Therefore, p cannot divide $[G : N_P] = |S|$.

2. If $x \in S$ is a fixed point of H, the $H_x = H$. On the other hand, if $x \in S$ is not a fixed point of H, then $p|[H : H_x]$ since H is a p-subgroup. Then by the Orbit-Decomposition formula,

$$|S| = \sum_{\text{orbit reps} x} [H : H_x] = \#\{\text{fixed points}\} + pm$$

$\implies |S| \equiv k \ (mod p)$!

■

Theorem 5.8 (The Second Sylow Theorem)**.** *Let H be a p-subgroup of G. Then H is contained in some p-Sylow subgroup of G.*

Proof. Let H be a p-subgroup of G. Let $P \leqslant G$ be a p-Sylow subgroup of G. Write $|P| = p^n$.

- *Case: $H \leqslant N_G(P)$.* Then $HP \leqslant G$ and $P \trianglelefteq HP$ and $[HP : P] = [H : H \cap P]$ as a result of the second isomorphism theorem. If $HP \neq P$, then p divides $[HP : P]$ and $[HP : P] = p^k$ for some k. Now,

$$|HP| = p^m \text{ where } m > n$$

But this is a contradiction since P is p-Sylow and must be the highest power p-Group in G. Therefore, $HP = P \implies H = H \cap P \implies H \leqslant P$.

- *Case:* $H \not\leqslant N_G(P)$.
  Let S be as in the previous lemma, noting that H acts on S via conjugation. So p does not divide $|S|$ by the first part of the lemma, and the number of fixed points of $H \neq 0$.

  Letting $Q \in S$ be a fixed point of G, then

  $$H \leqslant N_Q \implies H \leqslant Q$$

  since Q is a p-Sylow subgroup (because it is the conjugate of a p-Sylow subgroup).

■

Theorem 5.9 (The Third Sylow Theorem)**.** *All p-Sylow subgroup of G are conjugate.*

Proof. Let H from above by p-Sylow. Then since $|H| = |Q|$ for any p-Sylow subgroup Q. Let P be a p-Sylow subgroup, say $H \not\leqslant N_P$. So for any p-Sylow subgroup P and H, they are conjugate to one another. ■

Theorem 5.10 (The Fourth Sylow Theorem)**.** *The number of p-Sylow subgroup of G is congruent to* 1 *(mod p) and this number must divide $|G|$.*

Note 5.11. *Let S be as in the previous lemma. Then a p-Sylow subgroup H fixes only itself in $S \implies$ one fixed point. Otherwise, we would have $H \leqslant N_G(Q) \implies H \leqslant Q \implies H = Q$.*

Proof. Now, by the second part of the previous lemma, we know that $|S|$ = the number of p-Sylow subgroups which is congrent to 1 (*mod p*). Also, the number of groups conjugate to P is $[G : N_G(P)]||G|$. ■

Corollary 5.11.1. *A p-Sylow subgroup $P \leqslant G$ is normal in G if and only if the only it is the only p-Sylow subgroup.*

Corollary 5.11.2 (Cauchy's Theorem)**.** *If G is a finite group and p divides $|G|$, then G contains an element (and hence a subgroup) of order p.*

Proof. If H is a p-Sylow subgroup of G, then we can take any element $h \in H$. If $|h| = p^i$, then $h^{p^{i-1}}$ is of order p. ■

5.1 Classifying Finite Groups

Theorem 5.12. *Let G be a finite p-group. If $|G| > 1$, then G has nontrivial center and it is solvable.*

Proof. Nontrivial Center: By the class formula, we know:

$$|G| = |Z(G)| + \sum_{x \in C, x \notin Z(G)} \underbrace{[G : G_x]}_{\text{divide } |G|}$$

$$\implies |Z(G)| = |G| - \sum_{x \in C, x \notin Z(G)} \underbrace{[G : G_x]}_{\text{divide } |G|}$$

$$\implies p||Z(G)| \implies Z(G) \neq 1$$

Solvable: Inducting on $|G|$.

- *Base Case:* Let $|G| = 2 \implies$ solvable.
- *Inductive Hypothesis:* Suppose all p-groups with $|G| < n$ are solvable.

- *Inductive Step:* Let $|G| = n$. Now

$$|G/Z(G)| < n \implies G/Z(G) \text{ is solvable by inductive hypothesis}$$

Now write an abelian series for $G/Z(G)$:

$$G/Z(G) = H_0 \trianglerighteq H_1 \trianglerighteq \ldots \trianglerighteq H_m = 1$$

Letting π be the canonical projection of G to $G/Z(G)$, we know $G = \pi^{-1}(H_0)$. Therefore, we see:

$$G = \pi^{-1}(H_0) \trianglerighteq \pi^{-1}(H_1) \trianglerighteq \ldots \trianglerighteq \pi^{-1}(H_m) = Z(G)$$

Now, tacking on the trivial group at the end, we see:

$$G = \pi^{-1}(H_0) \trianglerighteq \pi^{-1}(H_1) \trianglerighteq \ldots \trianglerighteq \pi^{-1}(H_m) = Z(G) \trianglerighteq 1$$

is an abelian series. Therefore, G is solvable.

■

5.2 Consequences of Sylow Theorems

Example 5.13. *Any group of order pq^n where p, q are prime and $q \geq p$ is solvable.*

Proof. Assume $p \neq q$. Let $|G| = pq^n$. Let Q be a q-Sylow subgroup of order q^n. Notice that $Q \trianglelefteq G$ since

$$[G : Q] = p$$

which is the smallest prime dividing $|G|$. Therefore, Q is a q-group and therefore solvable. Now, we arrive at the abelian series.

$$G \trianglerighteq Q \trianglerighteq Q_1 \trianglerighteq \ldots \trianglerighteq Q_m = 1$$

Also, $G/Q \cong \mathbb{Z}_p$ which is abelian. Therefore G is solvable. ■

Example 5.14. *If p, q are prime with $p|q-1$, then there is a unique (upto isomorphism) non-abelian group of order pq.*

Proof. Let $|G| = pq$ and $p < q$ such that $p|q-1$. Notice, G has subgroups P, Q such that $|P| = p$ and $|Q| = q$. Now $Q \trianglelefteq G$ since it's index p in G is the smallest dividing the order of G. Further, $Q \cap P = 1$ by order considerations. In fact,

$$G = QP \cong Q \rtimes_\phi P$$

for some $\phi : P \to Aut(Q)$. Since P has prime order, $P = \langle x \rangle$. Now $Aut(Q)$ is a cyclic group of order $q-1$. So it contains a unique subgroup of order p, say $\langle y \rangle$. So $\phi(P) \leqslant \langle y \rangle$ and so $\phi(x) = y^k$ for some k. Further, there are exactly p such homomorphisms that map $\phi_i(x) = y^i$ with $0 \leq i < p$. Clearly, ϕ_0 is trivial, and therefore shows G is abelian. Therefore, every other ϕ_i gives a non-abelian group G_i of order pq. Moreover, all of these G_i's are isomorphic because $\phi_i(x') = y$ for some other available generator x' of P. So there is a unique nonabelian group up to isomorphism! ■

Also, just a useful theorem that might be proven later:

Theorem 5.15. *Any finite abelian group A is isomorphic to a product of cyclic groups:*

$$A \cong Z_{p_1^{r_1}} \times \mathbb{Z}_{p_2^{r_2}} \times \ldots \times \mathbb{Z}_{p_n^{r_n}} \times \mathbb{Z} \times \ldots \times \mathbb{Z}$$

where p_i are prime. This is unique up to reordering the factors.

6 Review of Field Theory

6.1 Motivational Examples

Example 6.1. *Consider the number*

$$a = \frac{\sqrt[3]{-27 + 3\sqrt{-11}} + \sqrt[3]{-27 - 3\sqrt{-11}}}{2}$$

As it turns out, $a^3 - 4a + 2 = 0$

Example 6.2.

$$S_3 \trianglerighteq A_3 \trianglerighteq 1$$

an Abelian series.

As it turns out, these two problems are connected. That is, the equation above has a solution if and only if S_3 is solvable!
Consider $a = \sqrt{-1}$. Then $\mathbb{C} = \mathbb{R}$ plus $\sqrt{-1}$. But we recall there are 2 choices for $\sqrt{-1}$. Turns out, interchanging these two roots results in a symmetry of $\mathbb{C}$, fixing only the real numbers.
Say we adjoint the roots of $x^{168} - 161x^{123} + 28x^{28} - 7$ to $\mathbb{Q}$, which is an irreducible polynomial by Eisenstein's criterion.
Further, what can we say about the symmetries of the resulting field?

6.2 Some Reminders about Fields

Definition 6.3. *A <u>ring</u> is a group* $\langle R, + \rangle$ *equipped with a second operation* $\cdot$ *that is both associative and closed.*

Definition 6.4. *An <u>ideal</u> is an additive subgroup of* $\langle R, + \rangle$ *such that* $rI \subset I$ *for all* $r \in R$

Proposition 6.5. *Given a subring* J, $I \cap J$ *is an ideal.*

Proposition 6.6. $IJ := \{x_1 y_1 + \ldots x_n y_n : x_i \in I, y_j \in J\}$ *is an ideal.*

Proposition 6.7. $I + J := \{x + y : x \in I, y \in J\}$ *is an ideal.*

Proposition 6.8. *A field only contains two ideals,* $\mathbb{F}, \{0\}$.

In any field, we can consider any Transcendental and algebraic elements in $\mathbb{F}$.

Definition 6.9. *An element* α *is <u>algebraic</u> of a given field* $\mathbb{F}$ *provided* α *satisfies some polynomial equation*

$$a_n \alpha^n + \ldots + a_1 \alpha + a_0 = 0$$

where $a_i \in \mathbb{F}$. *If no such polynomial equation exists, we say that element is <u>transcendental.</u>*

Definition 6.10. *Let* α *be algebraic over* $\mathbb{F}$. *Then*

$$F(\alpha) = \{a_n \alpha^n + \ldots + a_1 \alpha + a_0 : a_k \in \mathbb{F}\}$$

Proposition 6.11. *Let* τ *be transcendental over* $\mathbb{F}$. *Then*

$$F(\tau) \cong F[x]$$

is <u>not</u> a field.

Theorem 6.12. *If G is a finite subgroup of $F^\times$, where F is a field, then G is cyclic.*

Proof. Say G is a finite group with n elements.

Claim: If for every d dividing n, $\{x \in G : x^d = 1\} \leq d$, then G is cyclic.
Notice, if $x \in F$, then you are looking at most d roots of $x^d - 1$. To prove the claim, we have d is a divisor of n. Define G_d be the in G of order d. Suppose $G_d \neq \emptyset$. Then there exists $y \in G_d, \langle y \rangle \subset \{x \in G : x^d = 1\}$. Also, since y is of order d, then $|\langle y \rangle|$. We hypothesis, we want to show

$$\langle y \rangle = \{x \in G : x^d = 1\}$$

So G_d is the set of generators of $\langle y \rangle$. So

$$|G_d| = \varphi(d)$$

where φ is the Euler-Totient Function. So

$$|G| = n = \sum_{d|n} |G_d| \leq \sum_{d|n} \varphi(d) = n$$

The chain must be equalities. Therefore, for all d dividing n

$$|G_d| = \phi(d)$$

Moreover, this is demonstrates G_n is nonempty. Moreover, there is an element in G_n of order n in G. Therefore, G is cyclic.

■

6.3 Structure Theorems on Fields

Theorem 6.13. *Let $p(x) \in \mathbb{F}[x]$ be the minimal polynomial of $\alpha \in \mathbb{K} = F(\alpha)$ where α is algebraic over $\mathbb{F}$ and let $deg(p) = n$. Then*

$$K \cong F[x]/\langle p(x) \rangle := \{g(x) + p(x) : g(x) \in F[x]\}$$
$$\alpha \leftarrow x$$
$$k \leftarrow k \in F$$

Remark 6.14. *Also, $S = \{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is a basis for K over F. We say*

$$dim_F(K) = n$$

Or the degree of K over F.

Note 6.15. *There are similar theorems for transcendental elements, called transcendent bases.*

Theorem 6.16. *Let K/F, where K is a (possibly finite) field extension of F. The set of elements of K which are algebraic over F is a field.*

Proof. Let S be the set of elements in K algebraic over F. So we want for all $x, y \in S$, we have $x + y, x - y, xy \in S$ and $y \neq 0 \implies xy^{-1} \in S$. Notice, $F \subset S \subset K$. Observe, we can have the tower:

$$\begin{array}{c} F(x,y) \\ | \\ F(x) \\ | \\ F \end{array}$$

we want to show that each of these connections are in fact algebraic extensions. Specifically, these extensions must be finite. To prove the $F(x,y)$ is an algebraic extension, we can leverage the Tower Theorem to show the extension from F to $F(x,y)$ is finite. Notice, if $F(\alpha)$ is finite with degree n, then

$$1, \alpha, \alpha^2, \ldots, \alpha^n$$

so some linear combination of these is 0.
So $F(x,y)$ is an algebraic extension over F. Therefore, $F(x,y) \subset S$. ■

Theorem 6.17. *Suppose $\phi : F \xrightarrow{\sim} F'$. Let $p(x) \in F[x]$ be irreducible and let $q(x) = \phi(p(x))$. Let α be a root of $p(x)$, β be a root of $q(x)$. Then there exists an isomorphism $\sigma : F(\alpha) \xrightarrow{\sim} F'(\beta)$ such that*

$$F(\alpha) = \beta \text{ and } \sigma|_F = \phi$$

Proof. Notice,

$$F(\alpha) \cong F[x]/\langle p(x)\rangle \cong F'[x]/\langle q(x)\rangle \cong F'(\beta)$$
$$\alpha \to x \to x \to \beta$$

where the restriction on F is just ϕ. ■

6.4 Composite Fields

Definition 6.18. *Let K_1, K_2 be subfields of K. The composite field of K_1 and K_2 is denoted by K_1K_2 and is defined as the smallest field of K containing K_1, K_2.*

Example 6.19. *Let $\omega_3 = e^{\frac{2\pi i}{3}}$ and $K = \mathbb{C}$. Define*

$$K_1 = \mathbb{Q}(\sqrt[3]{2}) \quad K_2 = \mathbb{Q}(\omega_3\sqrt[3]{2})$$

Then

$$K_1K_2 = \mathbb{Q}(\sqrt[3]{2}, \omega_3) = \mathbb{Q}(\sqrt[3]{2} + \omega_3)$$

To see this, let $\alpha = \sqrt[3]{2} + \omega_3$ and look at powers of α^i with $0 \le i \le 5$. Then we can write all of these powers as linear combinations of $\sqrt[3]{2}, \omega_3, \sqrt[3]{2}\omega_3$.

Theorem 6.20. *Let K_1/F and K_2/F be finite and*

$$[K_1K_2 : F] \le [K_1 : F][K_2 : F]$$

with equality if and only the F-basis of one of the K_i's remains linearly independent over the other K_i.

Proof. Let $\{\alpha_i\}$ be a basis of K_1 over F, and let $\{\beta_j\}$ be a basis for K_2 over F. Then

$$\begin{aligned} K_1K_1 &= \text{ the smallest subfield of } K \text{ containing } F(\{\alpha_i\}, \{\beta_j\}) \\ &= F(\{\alpha_i\}, \{\beta_j\}) \end{aligned}$$

Claim: $\{\alpha_i\beta_j\}_{i,j}$ spans K_1K_2 over F.

$$\begin{aligned} \alpha_i^n\beta_k^m &= \alpha_i^n \sum_r b_r\beta_r \\ &= \sum_s a_s\alpha_s \sum_r b_r\beta_r \\ &= \sum_{\ell,j} a_\ell b_j \alpha_\ell \beta_j \end{aligned}$$

Therefore,

$$[K_1K_2 : F] \leq [K_1 : F][K_2 : F]$$

To see when equality holds, we notice that since $\alpha_i\beta_j$ spans K_1K_2 over F, we must have that $\{\beta_j\}$ spans K_1K_2 over K_1. Therefore,

$$[K_1K_2 : K_1] \leq [K_2 : F]$$

with equality if and only if $\{\beta_j\}$ are linearly independent over K_1. Consider,

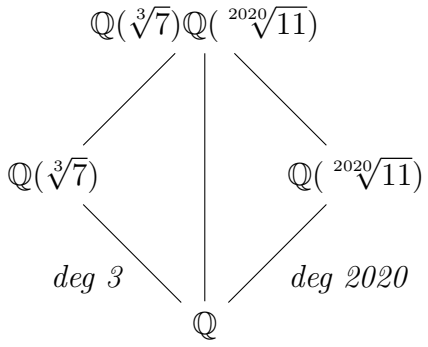
$$\begin{array}{c} K_1K_2 \\ | \\ K_1 \\ | \\ F \end{array}$$

By the Tower Rule,

$$[K_1K_2 : F] = [K_1K_2 : K_1][K_1 : F] = [K_2 : F][K_1 : F]$$

if and only if $\{\beta_j\}$ are linearly independent over K_1. The same can be said for K_2 as the intermediary field. Therefore, the claim holds. ■

Example 6.21. $[\mathbb{Q}(\sqrt[3]{7})\mathbb{Q}(\sqrt[2020]{11}) : \mathbb{Q}]$
Observe,



We see that the degree of the extension is divisible by both 3 and 2020 and hence

$$3 \cdot 2020 = 6060$$

Also, the degree is at most the product of the our two degrees. Therefore, we conclude the degree of the field extension is exactly 6060.

Example 6.22. $\mathbb{Q}(\sqrt[4]{2}, \sqrt{3}) : \mathbb{Q}) = d$. *Obviously by the same argument before, we see that* 4 *must divide* d. *Also,* 2 *must divide* d. *Therefore,* $4 \leq d \leq 8$. *Now,*

- *If* $d = 4$, *then* $\sqrt{3} \in \mathbb{Q}(\sqrt[4]{2})$, *which cannot occur.*

Therefore, $d = 8$.

Example 6.23. $\alpha = \sqrt[4]{2}, \beta = \sqrt[4]{18}$, *with*

$$[\mathbb{Q}(\alpha)\mathbb{Q}(\beta) : \mathbb{Q}] = 8$$

since $\sqrt{18} = 3\sqrt{2}$

Remark 6.24. *If need note be true that* $[K_1K_2 : F]$ *divides* $[K_1 : F][K_2 : F]$

Example 6.25. *Let $F = \mathbb{Q}$ and $K_1 = \mathbb{Q}(\sqrt[3]{2})$ and $K_2 = \mathbb{Q}(\omega_3\sqrt[3]{2})$. Then*

$$K_1K_2 = \mathbb{Q}(\sqrt[3]{2}, \omega_3)$$

But

$$[K_1K_2 : \mathbb{Q}] = 6 \not| \ 9$$

The fundamental issue comes from the fact that both K_1 and K_2 are missing roots of the same polynomial $x^3 - 2$.

7 Field Extensions

7.1 Splitting Fields

Definition 7.1. *Let F be a field, and let $p(x) \in F[x]$. An extension K/F is called a splitting field over F if $p(x)$ factors into linear factors in $K[x]$ but not so over any proper subfield of K containing F.*

Example 7.2. *$\mathbb{C}$ is a splitting field over $\mathbb{R}$ of $x^2+1 \in \mathbb{R}[x]$. Clearly this extension is of degree 2.*

Example 7.3. *What is the splitting field of $x^2-2 \in \mathbb{Q}[x]$ over $\mathbb{Q}$? The first question you should ask yourself is "What are the roots of this polynomial?" Here, the roots are:*

$$\sqrt[3]{2}, \quad \xi_3\sqrt[3]{2}, \quad \text{and} \quad \xi_3^2\sqrt[3]{2}$$

So the splitting field is contained in $\mathbb{Q}(\sqrt[3]{2}, \xi_3)$. In fact, we can show that the splitting field contains $\mathbb{Q}(\sqrt[3]{2}, \xi_3)$ and there the splitting field must be exactly $\mathbb{Q}(\sqrt[3]{2}, \xi_3)$. Next, what is the degree of extension? Observe,

$$[\mathbb{Q}(\sqrt[3]{2}, \xi_3) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}, \xi_3) : \mathbb{Q}(\xi_3)][\mathbb{Q}(\xi_3) : \mathbb{Q}] = 3 \cdot 2 = 6$$

Example 7.4. *Given x^6-1 over $\mathbb{Q}$. Observe, this polynomial is reducible:*

$$x^6 - 1 = (x+1)(x^2-x+1)(x-1)(x^2+x+1)$$

However, we see that the quadratic factors cannot be reduced in $\mathbb{Q}$. The roots of this polynomial are:

$$1, -1, \frac{1 \pm \sqrt{-3}}{2}, \frac{-1 \pm \sqrt{-3}}{2}$$

Therefore, the splitting field needs to include $\sqrt{-3}$. Therefore, the splitting field is $\mathbb{Q}(\sqrt{3})$.

Question 7.5. *Given any polynomial over a field, can we always find a splitting field for such a polynomial?*

Theorem 7.6. *Let F be a field, let $p(x) \in F[x]$. Then there exists a splitting field for $p(x)$ over F.*

Proof. Induct on the degree of $p(x)$, and then use the fact that if α is a root of $p(x)$, then $p(\alpha) = (x-\alpha)q(x)$ where q must have degree less than p. Then we can define the field:

$$F(\alpha) = F[x]/\langle p(x) \rangle$$

Therefore, by the induction hypothesis, we get a field L in which $p(x)$ splits. To get the minimal one, we can take the intersection of all subfields of L in which $p(x)$ splits. ■

Definition 7.7. *An algebraic extension K/F is a normal extension if it is the splitting field of a collection of polynomials in $F[x]$.*

Example 7.8. *Any degree 2 extension K/F is normal. This is because, if $\alpha \in K \setminus F$, then α is the root of a quadratic polynomial over F. That means this quadratic polynomial facts into linear factors in K. Since K is a degree 2 extension, it is the smallest such extension. Therefore, K is the splitting field for this particular polynomial.*

Example 7.9. *Is $\mathbb{Q}(\sqrt[4]{2})$? Is it normal over $\mathbb{Q}$?*

Lemma 7.10. *If K is a splitting field for some polynomial g over F. Say $f(x) \in F[x]$ which is irreducible over F and has a zero in K. Then $f(x)$ splits in K.*

Clearly by this lemma, its not possible for $\mathbb{Q}(\sqrt[4]{2})$ to be normal over $\mathbb{Q}$ since it fails to possess all of the roots of $x^4 - 2 \in \mathbb{Q}[x]$.

Proof. If $\alpha_1, \alpha_2, \ldots$ are the roots of $f(x)$, then $[K(\alpha_i) : K]$ is independent of i. Moreover, by the tower rule

$$[K(\alpha_i) : K][K : F] = [K(\alpha_i) : F] = [K(\alpha_i) : F(\alpha)] \underbrace{[F(\alpha_i) : F]}_{deg(f)}$$

Since K is a splitting field of $g(x)$ over F, then we must have that $K(\alpha_i)$ is a splitting field of $g(x)$ over $F(\alpha_i)$. Now,

$$F(\alpha_i) \cong_\phi F(\alpha_j)$$

for any i, j. Therefore,

$$K(\alpha_i) \cong_\mu K(\alpha_j)$$

with $\mu|_{F(\alpha_i)} = \phi$ for all i, j including $\alpha_j \in K$. But that means, $K(\alpha_j) = K$ for any j. Therefore, K contains all of the roots of f. ■

Theorem 7.11. *Let $\phi : F \xrightarrow{\sim} F'$ be an isomorphism. Let $f(x) \in F[x]$, let $\phi(f(x)) = g(x) \in F'[x]$. Let E be a splitting field of $f(x)$ over F. Let E' be a splitting field for $g(x)$ over F'. Then there exists an isomorphism $\mu : E \xrightarrow{\sim} E'$ such that*

$$\mu|_F = \phi$$

Proof. We shall prove by inducting on the degree of f.

- Basis: If $deg(f) \leq 1$, then $E = F$ and $E' = F'$.
- Inductive Step: Now suppose the theorem is true for polynomials of degree less than n. Consider a polynomial f of $deg(f) = n + 1$. Considering an irreducible factor of $p(x)$ of $f(x)$, let

  $$\phi(p(x)) = q(x)$$

  Let α be a root of $p(x)$. Let β be a root of $q(x)$. By theorem 6.14, there exists a map $\mu_1 : F(\alpha) \to F(\beta)$ where $\mu_1|_F = \phi$. Now write

  $$f(x) = (x - \alpha)h(x) \in F(\alpha)$$
  $$g(x) = (x - \beta)k(x) \in F'(\beta)$$

  $h(x)$ must split in E. If it were to split over a smaller field containing $F(\alpha)$, then this would contradict the fact that E is a splitting field of f over F. Therefore, E is a splitting field of $h(x)$ over $F(\alpha)$ and E' is a splitting field for $k(x)$ over $F'(\beta)$. So we have

  $$\begin{array}{rccc} \mu_1 : & F(\alpha) & \xrightarrow{\sim} & F'(\beta) \\ & \downarrow & & \downarrow \\ & E & & E' \end{array}$$

  By induction, there exists $\mu : E \xrightarrow{\sim} E'$ with $\mu|_{F(\alpha)} = \mu_1$ and $\mu|_F = \mu_1|_F = \phi$.

■

Corollary 7.11.1. *Any two splitting fields of $p(x) \in F[x]$ over F are isomorphic.*

7.2 Algebraically Closed Fields

Definition 7.12. *A field K is algebraically closed if every $p(x) \in K[x]$ has a root in K.*

Example 7.13. *$\mathbb{C}$ is an algebraically closed field.*

Definition 7.14. *Let F be a field. A field $\bar{F}$ is called an algebraic closure of F if $\bar{F}$ is algebraic over F and every $p(x) \in F[x]$ splits completely in $\bar{F}$.*

Note 7.15. *The definition for algebraic closure of a field does not necessarily guarantee algebraically closed.*

Theorem 7.16. *If F is a field, then $\bar{F}$ is algebraically closed.*

Proof. Consider $\alpha_0 + \alpha_1 x + \ldots + \alpha_n x^n \in \bar{F}[x]$. Let α be a root. Then

$$F(\alpha, \alpha_0, \alpha_1, \ldots, \alpha_n)$$

is algebraic over $F(\alpha_0, \ldots, \alpha_n)$. Therefore, $\alpha \in \bar{F}$. ■

Theorem 7.17. *Let F be a field. Then there exists an algebraic closure of F, called $\bar{F}$. Any two algebraic closures of F are isomorphic.*

Before we start the proof, let's recall a couple of set theoretic facts:

- If S, T are sets, then $|S| = |T| \implies$ there exists a bijection between S and T
- If $|S| \leq |T| \implies$ there exist an injection $S \to T$ or a surjection $T \to S$

As well as the following lemmas:

Lemma 7.18. *Let F be a field, let K/F be algebraic. Then $|K| \leq \max\{|F|, |\mathbb{N}|\}$.*

Proof. Let M_{on} be the set of monic polynomials in $F[x]$, and for every $n \geq 1$, let

$$M_{on}^n \subset M_{on}$$

be the subset of degree n monic polynomials. For every $\alpha \in K$, consider the minimal polynomial $m_\alpha \in M_{on}$, with ordered roots of m_α in K

$$\alpha_1, \alpha_2, \ldots$$

We can construct the injective map

$$K \to M_{on} \times \mathbb{N}$$
$$\alpha \to (m_\alpha, i)$$

Therefore, by the second fact recalled from set theory:

$$|K| \leq |M_{on} \times \mathbb{N}| = |M_{on}|$$

So what is $|M_{on}|$? Consider $M_{on}^n := \{x^n + a_{n-1}x^{n-1} + \ldots : a_i \in F\}$. So we have a bijection with F^n via the coefficients. So for finite F,

$$|F^n| = |F|^n$$

On the other hand, for infinite F, $|F|^n = |F|$. Therefore,

$$|M_{on}| = \left| \bigcup_n M_{on}^n \right| = \max\{|F|, |\mathbb{N}|\}$$

■

Lemma 7.19. *Let K be a field. Then the following are equivalent:*

- *If L/K is algebraic, then $L = K$.*
- *Every polynomial $f(x) \in K[x]$ splits completely over K.*

Lemma 7.20 (Zorn)**.** *If A is a nonempty, partially ordered set in which every chain has an upper bound, then A has a maximal element.*

Proof. (Of Theorem)
(Existence) Suppose S is a "giant set" containing F. Specifically, $|S| > \max\{|F|, |\mathbb{N}|\}$. Such a set exists via taking the power set of either F or $\mathbb{N}$. So then there exists an injection $F \to S$, but not a bijection.

Consider $A := \{$ all fields $L \subset S$ such that $F \subset L$ and L is algebraic over $F\}$. A is nonempty since $F \in A$. Now, define the partial order, denoted by $\leq$, by

$$L_1 \leq L_2 \iff L_1 \subset L_2$$

Then any chain $L_1, L_2, L_3, \ldots$ has an upper bound $\bigcup_i L_i$, which is a field since the union of fields is still a field. Now, applying Zorn's Lemma, it must follow that A has a maximal element, say M. We want to show that M is our candidate for our algebraic closure.

Let L be an algebraic extension of M. We want to show that $L = M$, which by one of the above lemmas would show that M is an algebraic closure. By Lemma 6.40, we know

$$|L| \leq \max\{|M|, |\mathbb{N}|\} \leq \max\{|F|, |\mathbb{N}|\} < |S|$$

So there exists an injective map $f : L \to S$ such that $f|_M =$ identity map since $|L \setminus M| < |S|$. Now make $f(L) \subset S$ into a field by defining

$$f(a) + f(b) = f(a + b)$$
$$f(a)f(b) = f(ab)$$

So $f(L)$ is algebraic over F. So $f(L) \in A$ with $M \subset f(L)$. Since M is maximal, then L = M.

Therefore, by Lemma 6.41, we know that M is an algebraic extension.

(Uniqueness) Suppose K, K' are algebraic closures of F.
Claim: There exists $\tau : K \xrightarrow{\sim} K'$ with $\tau|_F =$ identity map.
Let $S := \{(L, \phi) : L \subset K, \phi : L \to K'$ is an injective homomorphism with $\phi|_F = id\}$. Note, $S \neq \emptyset$ since $(F, id) \in S$. We now define a partial order on S by

$$(L, \phi) \leq (L', \phi') \iff L \subset L' \text{ and } \phi'|_L = \phi$$

Notice that for a chain $\{(L_i, \phi_i)\}$, we have if $L = \bigcup_i L_i$,

$$\phi : L \to K'$$
$$a \to \phi_i(a) \text{ if } a \in L_i$$

Then (L, ϕ) is an upper bound for this chain. Therefore, we may apply Zorn's Lemma, there exists a maximal element (M, τ) in S.

Claim: $M = K$ and $\tau(M) = K'$
If $M \neq K$, then there exists $f \in F[x]$ that does not yet split over M. Let α be a root of f not in M. Let

$\alpha' \in K'$ be a root of $\tau(f(x)) = f(x)$ Note that τ is an isomorphism from M to $\tau(M)$. By Theorem 6.14, there exists

$$\mu : M(\alpha) \to \tau(M)(\alpha') \quad \text{such that} \quad \mu|_M = \tau$$

So $(M(\alpha), \mu) \in S$. But this contradicts the maximality of (M, τ). Therefore, $M = K$.
Clearly $\tau(K) \subset K'$ is an algebraic closure of F. Therefore $K' = \tau(K)$ by Lemma 6.41. ■

7.3 Separability and Positive Characteristic

Question 7.21. *Consider the polynomial*

$$f(x) = x^{p-1} + x^{p-2} + \ldots + x + 1 \in \mathbb{Z}[x]$$

where p is prime. Is this polynomial irreducible over $\mathbb{Q}$?

Answer: Yes! Set $g(x) = f(x+1)$ which has a leading term x^{p-1}. Then

$$g(x) = \frac{(x+1)^p - 1}{(x+1) - 1} = \sum_{i=1}^{p} \frac{p!}{i!(p-i)!} x^{i-1}$$

By Eisenstein's Criterion, we know $g(x)$ is irreducible. Therefore, $f(x)$ is also irreducible. So the roots of $f(x)$ are the roots of unity

$$\xi_p, \xi_p^2, \ldots, \xi_p^{p-1}$$

Definition 7.22. *Let $f(x) \in F[x]$. We say f(x) is <u>separable</u> if all of its roots (in some splitting field) are distinct.*

Question 7.23. *So how do we detect separability?*

Theorem 7.24. *Let $f(x) \in F[x]$. Then $f(x)$ has a multiple root α if and only if α is a root of $f'(x)$. Also, f has no multiple roots if and only if $gcd(f, f') = 1$.*

Proof. Left as an exercise. ■

Theorem 7.25. *Let $f(x) \in F[x]$ be nonzero, irreducible. Then if $char(F) = 0$, then $f(x)$ is separable.*

Proof. $f(x)$ is not separable if and only if it has a multiple root if and only if it has a nontrivial common factor with $f'(x)$ if and only if $f(x)$ divides $f'(x)$. This can be seen since for any

$$g(x)|f(x) \text{ and } g(x)|f'(x)$$

Then $f(x)$ shares a zero α with $f'(x)$. Also, $f(x)$ divides $h(x)$ whenever $h(\alpha) = 0$. But since f is irreducible, this implies $f(x)$ divides $f'(x)$. But since $deg(f) > deg(f') \iff f'(x) = 0$ which, within characteristic 0, means $f(x)$ is constant. Constradiction! Therefore, f is separable. ■

Question 7.26. *What about for positive characteristic p?*

Lemma 7.27. *Let F be a field where $char(F) = p > 0$. Then the Frobenius endomorphism $\phi : F \to F$ given by*

$$x \to x^p$$

is an injective field homomorphism.

Proof.
- We can check this mapping is injective. To do so, we know the $ker(\phi)$ is an ideal of our field. Since a field only possesses two ideals, F and 0, then we see

$$Ker(\phi) = \{0\}$$

- To check that it's a homomorphism:

$$\phi(xy) = (xy)^p = x^p y^p = \phi(x)\phi(y)$$
$$\phi(x+y) = (x+y)^p = x^p + y^p = \phi(x) + \phi(y)$$

- To check surjectivity, we note that an injective endomorphism of a finite field is automatically surjective. Since $char(F) = p$, then F is finite. Therefore, ϕ is surjective.

■

Corollary 7.27.1. *Let F be a finite field of $char(F) = p > 0$. Then every element is F is a pth power. That is,*

$$F = F^p$$

Definition 7.28. *A field F is called perfect if either:*

- *$char(F) = 0$, or*
- *$char(F) = p > 0$ and every element of F is a pth power.*

Theorem 7.29. *Let F be a perfect field. Then every irreducible polynomial $f(x) \in F[x]$ is separable.*

Proof.

- *Case:* When $char(F) = 0$, this has already been proven in theorem 6.47.
- *Case:* When $char(F) = p > 0$, and from the proof of $char(F) = 0$ case, we know that the only chance for $f(x)$ to be inseparable is if $f'(x) = 0$. This happens if

$$f(x) = \sum_i a_i x^i$$

where $a_i \neq 0$ only if p divides i. Now we're going to leverage our definition for perfect fields. Write

$$f(x) = \sum_j a_{pj} x^{pj} = \sum_j b_j^p x^{bj}$$

for some $b_j \in F$. Hence,

$$f(x) = \sum_j (b) j x^j)^p = \left(\sum_j b_j x^j \right)^p$$

But this contradicts the irreducibility of $f(x)$. Therefore, f is separable.

■

Note 7.30. *The converse is also true! If t is not a pth power,*

$$f(x) = x^p - t = (x - t^{1/p})^p$$

is irreducible but inseparable.

Definition 7.31. *An algebraic extension K/F is called separable of every $x \in K$ is the root of a separable polynomial $F[x]$. Otherwise, the extension is inseparable.*

Theorem 7.32. *Let F be a perfect field. Let K/F be an algebraic extension. Then K/F is separable.*

Question 7.33. *Can we think of an inseparable extension?*

Example 7.34. *Let p be prime. Looking at the extension:*

$$\mathbb{F}_p(t)/\mathbb{F}_p(t^p)$$

where

$$\mathbb{F}_p(t) := \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in \mathbb{F}_p[x], g(x) \neq 0 \right\}$$

Then t is a root of $f(x) = x^t - t^p = (x - t)^p$.

7.4 Classifying Finite Fields

Example 7.35. *A finite field that we are all familiar with is*

$$\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$$

with characteristic p.

Question 7.36. *What are all the other finite fields of characteristic p?*

Lemma 7.37. *Every field F of characteristic p contains a subfield isomorphic to $\mathbb{F}_p$*

Proof. Consider the field generated by $\langle 1 \rangle$. Then $\langle 1 \rangle \cong \mathbb{F}_p$ ■

Therefore, every field of characteristic p is an extension of $\mathbb{F}_p$. Therefore, we can ask?

$$[F : \mathbb{F}_p] = n < \infty$$

For what values of n is this true? Does degree determine F? When is $F_1 \subset F_2$. This leads us to the following theorem:

Theorem 7.38. *Let p be prime. Then*

1. *For all $n \geq 1$, $\exists$ a field field F with $[F : \mathbb{F}_p] = n$*
2. *Such an F (as in 1.) is unique up to isomorphism.*
3. *Two finite fields of characteristic p must satisfy*

$$F_1 \subset F_2$$

if and only if

$$[F_1 : \mathbb{F}_p] | [F_2 : \mathbb{F}_p]$$

Proof. 1. For $n \geq 1$, consider a splitting field of $f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$. To see if this polynomial is separable, we often would look at the derivative. Observe,

$$f'(x) = -1$$

Therefore, $f(x)$ has no common factors with $f'(x)$, and therefore $f(x)$ is separable. So $f(x)$ has p^n distinct roots in its splitting field. The set of these roots are closed under addition since for any α, β roots of $f(x)$, then by Freshman's Dream:

$$(\alpha + \beta)^{p^n} - (\alpha + \beta) = (\alpha^{p^n} - \alpha) + (\beta^{p^n} - \beta) = 0 + 0 = 0$$

The set of these roots are also closed under multiplication, since for any α, β roots of $f(x)$, then

$$(\alpha\beta)^{p^n} - \alpha\beta = \alpha^{p^n}\beta^{p^n} - \alpha\beta = \alpha\beta - \alpha\beta = 0$$

Clearly, 0 and 1 are both roots of $f(x)$ and the nonzero roots are invertible. Therefore, the roots form a field of size p^n containing $\mathbb{F}_p$. Moreover, this field has degree:

$$[F : \mathbb{F}_p] = n \iff \{\alpha, \ldots, \alpha_n\} \text{ is a basis } \iff p^n \text{ elements in } F \text{ over } \mathbb{F}_p$$

2. Suppose $[F : \mathbb{F}_p] = n$. Then
$$|F^\times| = p^n - 1$$
So every $\alpha \in F^\times$ satisfies $\alpha^{p^n-1} = 1 \implies \alpha^{p^n} - \alpha = 0$. So F is contained in a splitting field of $x^{p^n} - x$ and $|F| = p^n$ is a splitting field of $x^{p^n} - x$. Splitting fields are unique up to isomorphism. Therefore, we have uniqueness of finite fields.

Note 7.39. *These fields are denoted $\mathbb{F}_q$ where $q = p^n$. But* ***WARNING,*** *$\mathbb{F} \ncong \mathbb{Z}Z/q\mathbb{Z}$!*

3. Let $n_1 = [F_1 : \mathbb{F}_p]$ and $n_2 = [F_2 : \mathbb{F}_p]$
($\Rightarrow$) Suppose $F_1 \subset F_2$. Then by the tower theorem, says n_1 divides n_2.
($\Leftarrow$) Suppose n_1 divides n_2. Let $\alpha \in F_1$. Then $\alpha^{p^{n_1}} - \alpha = 0$ by (2). Now,
$$\alpha^{pin_1} = \alpha$$
for all $i \geq 1$. Also, $n_1 | n_2 \implies n_2 = in_1$ for some i. So
$$\alpha^{p^{n_2}} = \alpha \implies \alpha \in F_2$$

■

8 Galois Theory

8.1 Motivating Problems

- If you take a general polynomial of degree 5, there is no analogue of the quadratic formula.
- $\mathbb{C} = \mathbb{R}(\sqrt{-1})$ is algebraically closed.
- The regular 65537-gon can be constructed with rule and compass. Notice, this number is equal to $2^{16} + 1$, which is a prime number.

8.2 A little history ...

- Evariste Galois lived from 1811-1833
- His father committed suicide, after being involved in political riots as well as serving time in prison.
- He challenged someone to a duel over a girl. Obviously he lost ...
- He refused to prove obvious facts, which cost him entrance to the Ecole Polytechnique
- His work, though impressive to Cauchy, failed to garner the attention of the French mathematical community
- Galois completed his manuscript on the solutions of polynomial equations the evening before the duel.

8.3 Automorphisms on Fields

Definition 8.1. *Let K be a field. A field isomorphism $\sigma : K \xrightarrow{\sim} K$ is called an automorphism of K.*

Definition 8.2. *Recall that the set of automorphisms forms a group under composition, denoted $Aut(K)$.*

Let K/F be an extension. The subset $Aut(K/F)$ of $Aut(K)$ consists of $\sigma \in Aut(K)$ such that $\sigma(x) = x$ for all $x \in F$. Moreover,

$$Aut(K/F) \leqslant Aut(K)$$

Definition 8.3. *We typically refer to any $\sigma \in Aut(K/F)$ as an F-automorphism of K.*

Lemma 8.4. *Let K/F be a field extension and let $\alpha \in K$ be algebraic over F. For every $\sigma \in Aut(K/F)$, then element $\sigma(\alpha)$ is the root of the minimal polynomial $m_{\alpha,F}(x)$ of α over F. Moreover, the minimum polynomial of $\sigma(\alpha)$ over F is $m_{\alpha,F}(x)$.*

Proof. Left as an exercise. ■

Question 8.5. *How many symmetries can be identified in $Aut(K/F)$?*

Example 8.6. *Take $K = \mathbb{Q}(\sqrt{5})$ over $F = \mathbb{Q}$. If $\sigma \in Aut(K/F)$, then for any $a + b\sqrt{5} \in K$:*

$$\sigma(a + b\sqrt{5}) = \sigma(a) + \sigma(b\sqrt{5}) = a + b\sigma(\sqrt{5})$$

Therefore, we can simply carry $\sqrt{5}$ only to another root of the minimum polynomial. In this case, there are only two options: $\pm\sqrt{5}$. Therefore,

$$\sigma_1 : \sqrt{5} \to \sqrt{5}$$
$$\sigma_2 : \sqrt{5} \to -\sqrt{5}$$

And therefore,

$$Aut(K/F) = \mathbb{Z}/2\mathbb{Z}$$

Example 8.7. *The minimum polynomial of* $\mathbb{Q}(\sqrt[3]{2})$*, is* $x^3 - 2$*. However, there are no other roots in this field. Therefore, we only have the option to let*

$$\sigma : \sqrt[3]{2} \to \sqrt[3]{2}$$

And therefore, $Aut(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{1\}$

Example 8.8. *Take* p *prime and consider*

$$Aut(\mathbb{F}_p(t)/\mathbb{F}_p(t^p))$$

In order to classify this automorphism group, we need to know how this extension acts on t*. Here,* t *is a root of*

$$f(x) = x^p - t^p \in \mathbb{F}(t^p)[x]$$

which splits over $\mathbb{F}_p(t)$ *by Freshman's Dream. That is,*

$$f(x) = x^p - t^p = (x - t)^p \in \mathbb{F}_p(t)$$

and therefore only one root. So the group is trivial.

Question 8.9. *In general, what can be said about the size of the Automorphism group?*

Lemma 8.10. *Let* K/F *be a finite extension. Then* $|Aut(K/F)| < \infty$*.*

Proof. Suppose there exists $\alpha_1 \in K \setminus F$. If no such α exists, then the extension is clearly trivial. Now,

$$[K : F(\alpha_1)] < [K : F]$$

Suppose $K \neq F(\alpha_1)$. Then take $\alpha_2 \in K \setminus F(\alpha_1)$

$$\implies [K : F(\alpha_1, \alpha_2)] < [K : F(\alpha_1)]$$

Since the extension K/F is of finite degree, identifying these elements will eventually halt. Suppose these elements are listed

$$\alpha_1, \ldots, \alpha_r \in K$$

such that $K = F(\alpha_1, \ldots, \alpha_r)$. Let $\sigma \in Aut(K/F)$. For all $1 \leq i \leq r$, we know $\sigma(\alpha_i)$ is a root of $m_{\alpha_i, F}(x) \implies$ finitely many options. Also, once you know $\sigma(\alpha_i)$ is for all i, we have determined σ. Sp

$$|Aut(K/F)| < \infty$$

■

Question 8.11. *What can be understood about this extension* K/F *by studying this group* $Aut(K/F)$*.*

Clearly, there are situations where this automorphism group isn't very revealing. For example, when the set of automorphisms is trivial. In the previous examples, it turns out,

$$\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q} \text{ is not normal}$$

$$\mathbb{F}_p(t)/\mathbb{F}_p(t^p) \text{ is not separable}$$

So it could be there is some connection between these two extensions and the trivialness of their automorphism groups.

8.4 L-Valued Characters

Definition 8.12. *Let G be a group and let L be a field. An L-valued character is a group homomorphism $G \to L^\times$.*

Example 8.13. *Let $\sigma \in Aut(L)$. Then $\sigma|_{L^\times} L^\times \to L^\times$ is an L-valued character.*

Definition 8.14. *Let G be a group and L be a field. Then the set $\{x_1, \ldots, x_m\}$ be L-valued characters of G are called linearly independent over L if whenever there are $\ell_1, \ldots, \ell_m \in L$, with*

$$\ell_1 x_1(g) + \ldots + \ell_m x_m(g) = 0$$

for all $g \in G$, then $\ell_i = 0$ for all i.

Theorem 8.15 (Dedekind)**.** *Let G be a group and let L be a field. Let $x_1, \ldots, x_m$ be distinct L-valued characters of G. Then these characters are linearly independent over L.*

Proof. Suppose they are linearly dependent. Let, without loss of generality,

$$a_1 x_1 + \ldots + a_s x_s = 0$$

with $a_i \neq 0$. Let s be the smallest possible number less than or equal to m that is obtained in this way. Clearly, $s \geq 2$ since $\alpha_1 x_1(id) = a_i \neq 0$. So $x_1 \neq x_s \implies$ there exists $g_0 \in G$ with $x_i(g_0) \neq x_s(g_0)$. Now for all $g \in G$, we have

1. $\sum_{i=1}^s a_i x_i(g_0 g) = \sum_{i=1}^s a_i x_i(g_0) x_i(g) = 0$
2. $x_s(g_0) \sum_{i=0}^s a_i x_i(s) = \sum_{i=1}^s a_i x_i(g) x_s(g_0) = 0$

Subtracting (2) from (1), we get

$$\sum_{i=1}^{s-1} \underbrace{a_i(-x_s(g_0) + x_i(g_0))}_{\text{not all zero since } x_s(g_0) \neq x_1(g_0)} \; x_i(g) = 0$$

But we assume that s were the smallest for this relationship to occur. Contradiction! Therefore, they are linearly independent! ∎

Theorem 8.16. *Let K/F be finite. Then*

$$|Aut(K/F)| \leq [K : F]$$

Proof. Let $[K : F] = m$ and $|Aut(K/F)| = n$. Suppose $n > m$. Write

$$Aut(K/F) = \{\sigma_1, \ldots, \sigma_n\}$$

with F-basis of K

$$\{\alpha_1, \ldots, \alpha_m\}$$

Consider the $n \times m$ matrix $A := \{a_{ij}\}_{n \times m}$ where $a_{ij} = \sigma_i(\alpha_j)$. Notice $A \in M_{n \times m}(K)$. Since $n > m$, the rows of A must be linearly dependent over K and so there exists $\lambda_1, \ldots, \lambda_n \in K$, not all of which are zero, such that

$$\lambda_1 A e_1 + \lambda_2 A e_2 + \ldots + \lambda_n A e_n \in 0 \in K^m$$

Looking at each coordinate in this equation:

$$\sum_{i=1}^n \lambda_i \sigma_i(\alpha_r) = 0 \text{ for every } 1 \leq r \leq m$$

Now, for every i, we look at the K-valued character of $K^\times$

$$\sigma_i|_{K^\times} : K^\times \to K^\times$$

These are all distinct. Let $g \in K^\times$. Then there exist $f_j \in F$ for all $1 \leq j \leq m$, such that

$$g = \sum_{j=1}^{m} f_j \alpha_j$$

since $\{\alpha_j\}$ makes a basis. So

$$\begin{aligned}\sum_{i=1}^{n} \lambda_i \sigma_i(g) &= \sum_{i=1}^{n} \lambda_i \sigma_i \left(\sum_{j=1}^{m} f_j \alpha_j \right) \\ &= \sum_{i=1}^{n} \lambda_i \sum_{j=1}^{n} f_j \sigma_i(\alpha_j) \\ &= \sum_{j=1}^{m} f_j \sum_{i=1}^{n} \lambda_i \sigma_i(\alpha_j) = 0\end{aligned}$$

Therefore, the characters $\sigma_i|_{K^\times}$ are linearly dependent. But this contradicts Dedekind's Lemma! ■

8.5 Galois Extensions

Definition 8.17. *Let K/F be finite. We call K/F a <u>Galois Extension</u> if*

$$|Aut(K/F)| = [K : F]$$

In this case, $Aut(K/F)$ is called the <u>Galois Group</u> of K/F, and denoted by $Gal(K/F)$.

Definition 8.18. *Let K be a field and $H \leqslant Aut(K)$. The set $\mathcal{F}(H) := \{k \in K : \sigma(k) = k, \text{ for all } \sigma \in H\}$ is a subfield of K and is called the <u>fixed field of H</u>.*

Theorem 8.19 (Artin)**.** *Let K be a field, and let $H \leqslant Aut(K)$ be a finite subgroup. Let $\mathcal{F}(H)$ be the field field of H. Then*

$$|H| = [K : \mathcal{F}(H)]$$

and so $K/\mathcal{F}(H)$ is Galois with

$$Gal(K/\mathcal{F}(H)) = H$$

Proof. We know that $H \leqslant Aut(K/\mathcal{F}(H))$ since H fixes $\mathcal{F}(H)$.

$$\implies |H| \leq |Aut(K/\mathcal{F}(H))| \leq [K : \mathcal{F}(H)]$$

Now, for contradiction, suppose $|H| < [K : \mathcal{F}(H)]$. Let

$$H = \{\sigma_1, \ldots, \sigma_n\}$$

and for some $m > n$, let $\{\alpha_1, \ldots, \alpha_m\}$ be a set of elements in K that a linearly independent over the fixed field $\mathcal{F}(H)$. Let $A = \{a_{i,j}\} \in M_{n\times m}(K)$ given by $a_{ij} = \sigma_i(\alpha_j)$. Since $n < m$, we have the columns are linearly dependent vectors in K^n. After reordering the columns, then there exists $\lambda_1, \ldots, \lambda_r \in K$ all nonzero where $2 \leq r \leq m$ such that for all $1 \leq j \leq n$ we have

$$\sum_{k=1}^{r} \lambda_k \sigma_j(\alpha_k) = 0$$

Notice $r \not\perp$ since $\underbrace{\lambda_1}_{\neq 0}\sigma_j(\underbrace{\alpha_1}_{\neq 0})$ and an automorphism can't take a nonzero element to zero. Further, assume r is the smallest such number for which we achieve this linear dependence relationship. Observe,

$$\frac{1}{\lambda_1}\sum_{k=1}^{r}\lambda_k\sigma_j(\alpha_k) = \sum_{k=1}^{r}\frac{\lambda_k}{\lambda_1}\sigma_j(\alpha_k) = \sum_{k=1}^{r}\lambda_k'\sigma_j(\alpha_k) = 0$$

where $\lambda_1' = 1$. Note that not all λ_i' are in $\mathcal{F}(H)$. If they were, we can take $\sigma \in H$, then

$$\sigma\left(\sum_{k=1}^{r}\lambda_k'\alpha_k\right) = \sum_{k=1}^{r}\lambda_k'\sigma_j(\alpha_k) = 0$$

Since $\sigma \in Aut(K)$, then

$$\sum_{k=1}^{r}\lambda_k'\alpha_k = 0$$

But this contradicts the linear independence of $\alpha_j \in \mathcal{F}(H)$. Let $\sigma \in H$, then

$$\{\sigma\sigma_1, \ldots, \sigma\sigma_n\} = \{\sigma_1, \ldots, \sigma_n\}$$

So

$$\sigma\left(\sum_{k=1}^{r}\lambda_k'\sigma_j(\alpha_k)\right) = \sum_{k=1}^{r}\sigma(\lambda_k')\sigma_\ell(\alpha_k) = 0$$

Notice, $\lambda_1' = 1 \implies \sigma(\lambda_1') = 1$. Observe, if we subtract:

$$0 = \sum_{k=1}^{r}\lambda_k'\sigma_\ell(\alpha_k) - \sum_{k=1}^{r}\sigma(\lambda_k')\sigma_\ell(\alpha_k) = \sum_{k=2}^{r}(\lambda_k' - \sigma(\lambda_k'))\sigma_\ell(\alpha_k)$$

But by reordering, this contradicts the minimality of r. Therefore,

$$|H| = [K : \mathcal{F}(H)]$$

Now, since $H \leqslant Aut(K/\mathcal{F}(H))$ which has order

$$|H| = [K : \mathcal{F}(H)]$$

Then it must follow that

$$H = Aut(K/\mathcal{F}(H))$$

■

Corollary 8.19.1. *Let $H_1 \neq H_2$ be finite subgroups of $Aut(K)$. Then $\mathcal{F}(H_1) \neq \mathcal{F}(H_2)$.*

Example 8.20. *Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, which is an extension for both the fields $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$. Now, consider*

$$H_1 := \{id, \sqrt{2} \to -\sqrt{2}\}$$
$$H_2 := \{id, \sqrt{3} \to -\sqrt{3}\}$$

Then we see

$$\mathcal{F}(H_1) = \mathbb{Q}(\sqrt{3}) \neq \mathbb{Q}(\sqrt{2}) = \mathbb{F}(H_2)$$

even though the groups $H_1 \cong H_2$.

Example 8.21. *$Gal(\mathbb{Q}(\sqrt{5})/\mathbb{Q}) = \mathbb{Z}_2 \implies$ fixed field is $\mathbb{Q}$.*

Example 8.22. *On the other hand, $Aut(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}) = \{id\} \implies$ fixed field is $\mathbb{Q}(\sqrt[4]{2})$.*

Corollary 8.22.1. *A finite extension K/F is Galois if and only if $\mathcal{F}(Aut(K/F)) = F$.*

Proof. ($\Rightarrow$) Suppose K/F is Galois. Then

$$[K : F] = |Gal(K/F)|$$

So $Gal(K/F) = Aut(K/F)$, which is a finite subgroup of $Aut(K)$. By Artin's Theorem,

$$\mathcal{F}(Gal(K/F)) = \mathcal{F}(H)$$

$$\implies K/\mathcal{F}(H) \text{ is Galois}$$

$$\implies [K : \mathcal{F}(Gal(K/F))] = |H| = |Gal(K/F)|$$

That is,

$$[K : F] = |Gal(K/F)| = [K : \mathcal{F}(Gal(K/F))]$$

$$\implies \mathcal{F}(Gal(K/F)) = F$$

($\Leftarrow$) Suppose $\mathcal{F}(Gal(K/F)) = F$.
Then

$$[K : F] = [K : \mathcal{F}(\underbrace{Gal(K/F)}_{\leqslant Aut(K)})] = |Aut(K/F)|$$

By Artin's Theorem since $Gal(K/F)$ is a finite subgroup of $Aut(K)$. Therefore, K/F is Galois. ■

Corollary 8.22.2. *Let K/F be finite. Then $|Aut(K/F)|$ divides $[K : F]$.*

Proof. By Tower Theorem and Artin,

$$[K : F] = [K : \mathcal{F}(Aut(K/F))][\mathcal{F}(Aut(K/F)) : F]$$

■

Theorem 8.23 (Equivalent Definitions of Galois)**.** *Let K/F be a finite extension. Then the following are equivalent:*

1. *K/F is Galois.*
2. *K/F is normal and separable.*
3. *K is the splitting field of a set of separable polynomials in $F[x]$.*

Proof.

- (1) $\implies$ (2) : Let $\alpha \in K$, and we want the minimal polynomial of α over F $m_{\alpha,F}(x)$ to be separable and split completely in K. If this is true, then K is the splitting field of

$$\{m_{\alpha,F}(x) \in F[x] : \alpha \in K\}$$

Let $Gal(K/F) = \{\sigma_1, \ldots, \sigma_n\}$. Consider

$$\sigma_1(\alpha), \ldots, \sigma_n(\alpha)$$

which are elements of K but not necessarily distinct. Instead, we say the "distinct set" of $\beta_1, \ldots, \beta_r$ where every $\alpha = \beta_i$ for some i. We now hope to show :

$$m_{\alpha,F} = m(x) = \prod_{i=1}^{r}(x - \beta_i)$$

Now, $Gal(K/F)$ acts on $K[x]$ by acting on the coefficients. Given $\tau \in Gal(K/F)$, then

$$\tau(m(x)) = \tau\left(\prod_{i=1}^{r}(x - \beta_i)\right) = \prod_{i=1}^{r}(x - \tau(\beta_i)) = \prod_{i=1}^{r}(x - \beta_{\sigma(i)}) = \prod_{i=1}^{r}(x - \beta_i)$$

So $m(x) \in F[x]$ and is separable by construction. Therefore $m_{\alpha,F}(x)$ must divide but also $m(x)$ divides $m_{\alpha,F}(x)$. So $m(x) = m_{\alpha,F}(x) \implies$ all roots are in K. Therefore, K/F is separable and normal!

- (2) $\implies$ (3) Normal implies its the splitting field of a family of polynomials. If we replace that family with the set of irreducible factor polynomials, then we get (3).
- (3) $\implies$ (1) We can induct on $[K : F]$
  - *Basis:* If $[K : F] = 1 \implies K = F \implies$ clearly Galois
  - *Inductive Hypothesis:* Suppose $[K : F] = n$ and we know (3) $\implies$ (1) for extensions of degree less than n. Say K is the splitting field of a set $\{f_i(x)\}$ of separable polynomials in $F[x]$. We can assume the degree of f_i is greater than 1 since linear factors already split in F. Take $f(x)$ in this set, and let $\alpha \in K$ be a root. Let's look at the following tower:

$$\begin{array}{c} K \\ | \\ F(\alpha) \\ | \\ F \end{array}$$

    where $H = Aut(K/F(\alpha)) \leqslant Aut(K/F)$. Since K is the splitting field of $\{f_i(x)\}$ over $F(\alpha)$, then we know $|H| = [K : F(\alpha)] < n$ and therefore, we can apply the inductive hypothesis to see $K/F(\alpha)$ is Galois.

    What is $r = [F(\alpha) : F]$? We want $r := [Aut(K/F) : H]$! We know $f(x)$ is separable $\implies$ the minimum polynomial $m(x) = m_{\alpha,F}(x)$ is separable. $m(x)$ has exactly the same number of roots in K as the degree of the minimal polynomial. We denote the roots

$$\alpha_1, \ldots, \alpha_r$$

    Choosing $\alpha = \alpha_i$ for some i, we know there exists an isomorphism:

$$\begin{aligned} \tau_i : F(\alpha) &\xrightarrow{\sim} F(\alpha_i) \\ \tau_i(\alpha) &= \alpha_i \\ \tau_i|_F &= id \end{aligned}$$

    Moreover, by the uniqueness of splitting fields, $\exists \sigma_i : K \xrightarrow{\sim} K$ with $\sigma_i|_{F(\alpha)} = \tau_i$. Notice $\sigma_i \in Aut(K/F)$.

Looking at the cosets $\sigma_1 H, \ldots, \sigma_r H$ in $Aut(K/F)$. Observe these cosets are distinct because otherwise, if $\sigma_i H = \sigma_j H$

$$\implies \underbrace{\sigma_j^{-1}\sigma_i}_{\in H}(\alpha) = \alpha$$
$$\implies \sigma_j^{-1}(\alpha_i) = \alpha$$
$$\implies \alpha_i = \alpha_j$$
$$\implies i = j$$

Therefore, $[Aut(K/F) : H] \geq r$. If $[Aut(K/F) : H] > r$, then $|Aut(K/F)| > |H| \cdot r = [K : F(\alpha)] \cdot [F(\alpha) : F] = n$ which contradicts Theorem 7.16. Therefore

$$[Aut(K/F) : H] = r$$
$$\implies [Aut(K/F)] = |H|[Aut(K/F) : H] = [K : F(\alpha)] \cdot [F(\alpha) : F] = n = [K : F]$$

So K/F is Galois!

■

So all these definitions of Galois will come in handy for identifying Galois Groups.

Example 8.24. *Consider $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$, which is the splitting field of $x^3 - 2$ over $\mathbb{Q}$. Since $x^3 - 2$ is separable, we know by the previous theorem that $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ is Galois over $\mathbb{Q}$. Also,*

$$[\mathbb{Q}(\sqrt[3]{2}, \zeta_3) : \mathbb{Q}] = 6$$
$$\implies |Gal(\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q})| = 6$$

Let $\sigma \in Gal(\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$. Then we can for $\alpha = \sqrt[3]{2}$,

$$\begin{aligned}
id: &\quad \alpha \to \alpha &\quad \zeta_3 \to \zeta_3 \\
order2: &\quad \alpha \to \alpha &\quad \zeta_3 \to \zeta_3^2 \\
order3: &\quad \alpha \to \zeta_3\alpha &\quad \zeta_3 \to \zeta_3 \\
order6: &\quad \alpha \to \zeta_3\alpha &\quad \zeta_3 \to \zeta_3^2 \\
order3: &\quad \alpha \to \zeta_3^2\alpha &\quad \zeta_3 \to \zeta_3 \\
order6: &\quad \alpha \to \zeta_3^2\alpha &\quad \zeta_3 \to \zeta_3^2
\end{aligned}$$

Since there are 6 of these and $|Gal(\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q})| = 6$, then we have completely enumerated the group.

8.6 The Fundamental Theorem of Galois Correspondence

Theorem 8.25 (Galois Correspondence)**.** *Let K/F be finite and Galois. Let G be the set of subgroups of $Gal(K/F)$. Let $\mathcal{F}$ be the set of intermediate fields L with $F \subset L \subset K$. Then there exists an inclusion-reversing bijection*

$$\begin{aligned}
\mathcal{G} &\leftrightarrow \mathcal{F} \\
H &\to \mathcal{F}(H) &\quad \forall H \in \mathcal{G} \\
Aut(K/L) &\leftarrow L &\quad \forall L \in \mathcal{F}
\end{aligned}$$

Proof. If $\underbrace{H_1}_{\in\mathcal{G}} \neq \underbrace{H_2}_{\in\mathcal{G}}$, then $\mathcal{F}(H_1) \neq \mathcal{F}(H_2)$.

- So we have an injection of sets

$$\mathcal{G} \to \mathcal{F}$$
$$H \to \mathcal{F}(H)$$

- To see that it's a surjection, we let $L \in \mathcal{F}$. We recall K/F is Galois $\implies$ K is normal, separable over F. So K is normal and separable over L. So K/L is Galois with

$$L = \mathcal{F}(\underbrace{Gal(K/L)}_{\in \mathcal{G}})$$

  Therefore, we have a bijection.

- Now to see its inverse sends $L \to Aut(L)$, let $L \in \mathcal{F} \implies \mathcal{F}(Aut(K/L)) = L$. Also, if $H \in \mathcal{G}$, then $Aut(K/\mathcal{F}(H)) = H$ by Artin's Theorem.

$$G \to \mathcal{F}$$
$$H \to \mathcal{F}(H) \to Aut(K/\mathcal{F}(H)) = H$$

- Lastly, for this map to be inclusion reversing, suppose $\underbrace{H_1}_{\in \mathcal{G}} \subset \underbrace{H_2}_{\in \mathcal{G}}$. Clearly,

$$\mathcal{F}(H_1) \supset \mathcal{F}(H_2)$$

  Conversely, let $\underbrace{L_1}_{\in \mathcal{F}} \subset \underbrace{L_2}_{\in \mathcal{F}}$. Then $Aut(K/L_1) \supset Aut(K/L_2)$.

■

Note 8.26. *Suppose K/F is not Galois. $\implies$ $\mathcal{F}(Aut(K/F)) \supset F$. So there doesn't exist $H \in \mathcal{G}$ with $F = \mathcal{F}(H)$.*

Theorem 8.27. *Let K/F be Galois and finite. The Galois Correspondence has the following properties: If $L \in \mathcal{F}$ corresponds to $H \in \mathcal{G}$, then*

1. *$|H| = [K : L]$ and $[L : F] = [Aut(K/F) : H]$*
2. *H is a normal subgroup of $Aut(K/F)$ if and only if L is Galois over F and, in this case, $Gal(L/F) \cong Aut(K/F)/H$*

Note 8.28. *K/F Galois does not imply L/F is Galois. Consider $\mathbb{Q}(\sqrt[4]{2}, i)$, which has a the Galois group of D_8. Define the generators in the Galois Group:*

$$r(\sqrt[4]{2}) = i\sqrt[4]{2} \quad r(i) = i$$
$$s(\sqrt[4]{2}) = \sqrt[4]{2} \quad r(i) = -i$$

$$\begin{array}{c} \mathbb{Q}(\sqrt[4]{2}, i) \\ | \\ \mathbb{Q}(\sqrt[4]{2}) \\ | \\ \mathbb{Q} \end{array}$$

But notice, $Aut(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}) = \langle id, s \rangle$, which is not a normal subgroup of D_8.

Proof. (Of Theorem)

1. Let $L = \mathcal{F}(H)$. K/L is Galois so $|H| = [K : L]$. Since K/F is Galois, we have

$$[Aut(K/F) : H] \cdot [H] = |Aut(K/F)| = [K : F] = [K : L][L : F] = |H|[L : F]$$

$$\implies [Aut(K/F) : H] = [L : F]$$

2. ($\Leftarrow$) Suppose L/F is Galois. Let $H = Aut(K/L)$ and let $\sigma \in Aut(K/F)$, then consider $\sigma|_L$. Since L/F is Galois, we know it is a normal extension. So there exists a collection S of polynomials in $F[x]$ such that L is the splitting field of S over F.

   So what is $\sigma(L)$? It is a splitting field of

$$\{\sigma(f) : f \in S\} = S$$

   Since L and $\sigma(L)$ are both contained in K, they are both obtained by adjoining to F the roots (in K) of polynomials in S. Therefore,

$$L = \sigma(L)$$

$$\implies \sigma|_L \in Aut(L/F)$$

   Therefore, we have identified the restriction map:

$$\begin{aligned} Res : Aut(K/F) &\to Aut(L/F) \\ \sigma &\to \sigma|_F \qquad\qquad \forall \sigma \in Aut(K/F) \end{aligned}$$

   which is a homomorphism. Observe,

$$Ker(Res) = Aut(K/L) = H \implies H \trianglelefteq Aut(K/F)$$

   By the first isomorphism theorem,

$$Aut(K/F)/H \cong Im(Res)$$

   Investigating $Im(Res)$, we know by the uniqueness of splitting field, for all $\tau \in Aut(: /F)$, there exists $\sigma \in Aut(K/F)$ with $\sigma|_L = \tau$. Notice that K is a splitting field of some polynomial over K with coefficients in F. So

$$\begin{aligned} \tau : L &\to L \\ \{f\} &\to \{f\} \end{aligned}$$

   then there exists $\sigma : K \to K$ with $\sigma|_L = \tau$. Then every element of $Aut(L/F)$ can be reached by Res. Therefore,

$$Im(Res) = Aut(L/F)$$

   Therefore,

$$Aut(K/F)/H \cong Aut(L/F)$$

   ($\Rightarrow$) Suppose $H \trianglelefteq Aut(K/F)$. Let $L = \mathcal{F}(H)$ and let $\alpha \in L, \beta \in K$ be roots of the mimimal polynomial $m(x)$ of α over F. Notice, there exists $\sigma \in Aut(K/F)$ with

$$\sigma(\alpha) = \beta$$

because $\exists \phi : F(\alpha) \to F(\beta)$ such that $\phi|_F = id$ with $\phi(\alpha) = \beta$. So K is a splitting field of polynomials in $F[x]$ over $F \implies$ also a splitting field of this set of $F(\alpha)$. So $\exists \sigma : K \to K$ with $\sigma|_{F(\alpha)} = \phi$. Consider $\tau \in H$

$$\begin{aligned}\tau(\beta) &= \sigma \underbrace{\sigma^{-1}\tau\sigma}_{H \trianglelefteq Aut(K/F)} (\alpha) \\ &= \sigma(\alpha) && \text{since } L = \mathcal{F}(H), \alpha \in L \\ &= \beta\end{aligned}$$

So $\tau(\beta) = \beta \implies \beta \in \mathcal{F}(H) = L \implies$ all roots of $m(x)$ are in $L \implies m(x)$ splits in $L \implies L$ is the splitting field of

$$\{m_{\alpha,F}(x) : \alpha \in L\}$$

So L/F is separable because K/F is. Therefore L/F is Galois which we have shown implies $Gal(L/F) \cong Aut(K/F)/H$.

■

Example 8.29. *Let $K = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$, which we already demonstrated earlier is Galois over $\mathbb{Q}$. Moreover, we said*

$$|Gal(K/\mathbb{Q}| = 6 = 2 \cdot 3$$

Therefore, it is either isomorphic to $\mathbb{Z}_6$ or D_6. Notice, $\mathbb{Z}_6$ is abelian which implies all subgroups are normal. Now we actually have a theorem which demonstrates a correspondence between the normal subgroups of the Galois group and the Intermediate Fields being Galois. Since K here is Galois, it must follow that all intermediate fields $\mathbb{Q} \subset L \subset K$ are Galois over $\mathbb{Q}$. But $\mathbb{Q}(\sqrt[3]{2})$ is not normal and hence not Galois over $\mathbb{Q}$. Therefore,

$$Gal(K/\mathbb{Q}) \cong S_3 = D_6$$

Moreover, the generators of $Gal(K/\mathbb{Q})$

$$\begin{aligned}\sigma := \sqrt[3]{2} \to \zeta_3\sqrt[3]{2} \qquad \zeta_3 \to \zeta_3^2 \\ \tau := \sqrt[3]{2} \to \sqrt[3]{2} \qquad \zeta_3 \to \zeta_3^2\end{aligned}$$

Then we see:

$$\begin{aligned}&\sigma^{-1}\tau = \sigma^2\tau \\ \implies &\sigma^2\tau(\sqrt[3]{2}) = \zeta_3^2\sqrt[3]{2} \\ \implies &\sigma^2\tau(\zeta_3) = \zeta_3^2\end{aligned}$$

On the other hand,

$$\begin{aligned}\tau\sigma(\sqrt[3]{2}) = \zeta_3^2\sqrt[3]{2} \\ \tau\sigma(\zeta_3) = \zeta_3^2\end{aligned}$$

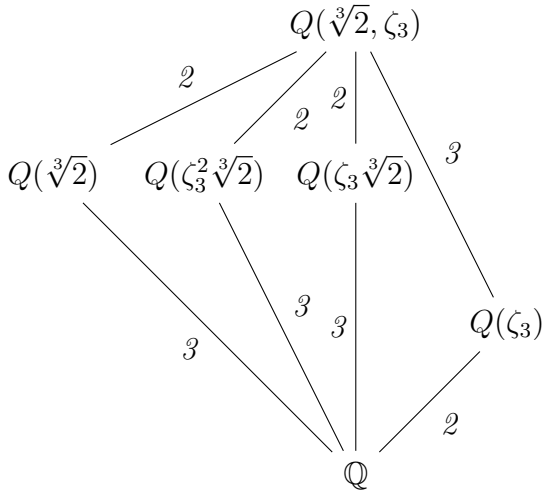
So we see $\sigma^2\tau = \tau\sigma$. Therefore,

$$Gal(K/\mathbb{Q}) = \langle \sigma, \tau : \tau^2 = \sigma^2 = e, \quad \sigma^2\tau = \tau\sigma \rangle \cong D_6$$

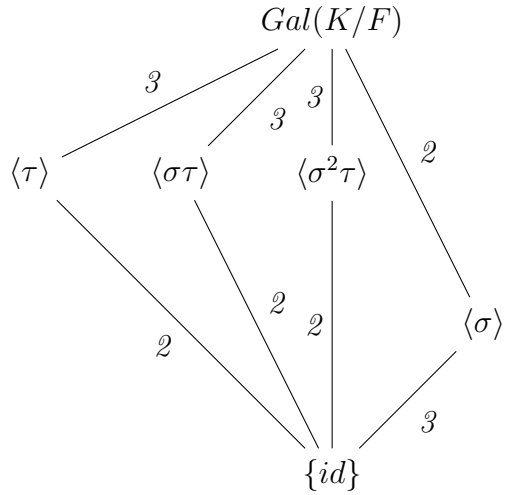
Now, the subgroups of D_6 and the corresponding intermediate fields are:

$$\begin{aligned}H_1 = \{id\} &\iff K \\ H_2 = \{id, \sigma, \sigma^2\} &\iff \mathbb{Q}(\zeta_3) \\ H_3 = \{id, \tau\} &\iff \mathbb{Q}(\sqrt[3]{2}) \\ H_4 = \{id, \sigma\tau\} &\iff \mathbb{Q}(\zeta_3^2\sqrt[3]{2}) \\ H_5 = \{id, \sigma^2\tau\} &\iff Q(\zeta_3\sqrt[3]{2}) \\ H_6 = D_6 &\iff \mathbb{Q}\end{aligned}$$

Then the subfield diagram is given by:



with corresponding subgroup lattice:



Example 8.30. *Let K be the splitting field of $(x^2-5)(x^2-7)$ over $\mathbb{Q}$. Observe,*

$$K = \mathbb{Q}(\sqrt{5},\sqrt{7}) \qquad [K:\mathbb{Q}] = 4$$

We have $\sigma,\tau \in Gal(K/\mathbb{Q})$ where

$$\sigma : \sqrt{5} \to -\sqrt{5} \quad \sqrt{7} \to \sqrt{7}$$
$$\tau : \sqrt{5} \to \sqrt{5} \quad \sqrt{7} \to -\sqrt{7}$$

Then $Gal(K/\mathbb{Q}) = \{id,\sigma,\tau,\sigma\tau\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. The subgroups are:

$$\begin{aligned} \{id\} &\iff K \\ \{\sigma\} &\iff \mathbb{Q}(\sqrt{7}) \\ \{\tau\} &\iff \mathbb{Q}(\sqrt{5}) \\ Gal(K/\mathbb{Q}) &\iff \mathbb{Q} \end{aligned}$$

9 Application of Galois Theory - Solving Polynomial Equations

Solving linear polynomials was developed significantly long ago. Quadratic polynomials are suspected to have been solved around 1600 BC during the rule of the Babylonians. Cubic equations were found to be solvable with a general formula in 1545 AD by Cardono, and his student Ferrari found the solution for quartic polynomials shortly after. Abel showed in 1827 demonstrated that quintic equations can't always have a nice formula. Galois's theory demonstrated that solving general polynomial equations relies on a strict group criterion in 1830.
While exploring applications for solving Polynomial Equations, we shall go about this in the following roadmap of topics:

- Describe "cyclic" field extensions
- Describe "radical" field extensions
- Prove the Galois Criterion.

9.1 Cyclic Field Extensions

Definition 9.1. *A finite Galois extension K/F is cyclic if $Gal(K/F)$ is cyclic.*

Lemma 9.2. *Let K/F be a finite, cyclic (Galois) extension. Suppose F contains a primitive n-th root of unity ζ_n, with $n = [K : F]$. Write*

$$Gal(K/F) = \langle \sigma \rangle$$

Then

1. *There exists $0 \neq \alpha \in K$ with $\zeta_n = \frac{\sigma(\alpha)}{\alpha}$*
2. *$K = F(\alpha)$ and $\alpha^n = a \in F \implies K = F(\sqrt[n]{a})$.*

Proof. 1. We want to show that $\sigma(\alpha) = \zeta_n \alpha$. We can interpret this from a linear algebra perspective as σ has an eigenvector α with eigenvalue ζ_n. Notice, σ is an endomorphism $K \to K$ of the F-vector space K, and we want to show ζ_n is an eigenvalue. Since $n = [F/F]$, we can interpret σ as an $n \times n$ matrix with coefficients in F. Further, we know $\sigma^n = id$ since $|Gal(K/F)| = n$. So σ satisfies the matrix polynomial equation:

$$X^n - I = 0$$

In fact, $id, \sigma, \sigma^2, \ldots, \sigma^{n-1}$ are all distinct K-valued characters. Now, trying to recall Dedekind's Lemma, we know the distinct K-valued characters are linearly independent, and therefore there does not exist a smaller degree polynomial equation that $X^n - I = 0$ that σ satisfies.

Now, consider the characteristic polynomial

$$P_\sigma(\lambda) = 0$$

of $\sigma_{n \times n}$. By Cayley-Hamilton, we have $P_\sigma(\sigma) = 0$ and it is degree n.

$$\implies P_\sigma(\sigma) = \sigma^n + a_{n-1}\sigma^{n-1} + \ldots + a_0 I = 0$$

Subtracting $\sigma^n - I = 0$ from both sides, we get:

$$a_{n-1}\sigma^{n-1} + \ldots + (a_0 - 1)I = 0$$

But σ cannot satisfy any smaller degree polynomial equation with coefficients in F. Therefore,

$$a_{n-1} = a_{n-1} = \ldots = a_1 = (a_0 - 1) = 0$$

Therefore,

$$P_\sigma(\lambda) = \lambda^n - 1$$

and $\zeta_n \in F$ is a root. So there exists an eigenvector in K with eigenvalue ζ_n. Now consider $\sigma - \zeta_n I$, which has determinant 0. Then $\sigma - \zeta_n I$ has a nontrivial kernel in K. Taking $\alpha \in Ker(\sigma - \zeta_n I) \setminus \{0\}$, then we get

$$\sigma(\alpha) - \zeta_n \alpha = 0 \implies \zeta_n = \frac{\sigma(\alpha)}{\alpha}$$

2. $\sigma^i(\alpha) = \zeta_n^i \alpha$ from (1). Now,

$$Gal(K/F) = \{id, \sigma, \sigma^2, \ldots, \sigma^{n-1}\}$$

Notice, the only element of $Gal(K/F)$ fixing α is the identify. So

$$Gal(K/F(\alpha)) = \{id\}$$

By Galois Correspondence, $F(\alpha) = K$. Moreover, $\sigma(\alpha^n) = (\sigma(\alpha))^n = (\zeta_n \alpha)^n = \alpha^n \in \mathcal{F}(Gal(K/F)) = F$ So there exists an $a \in F$ with $\alpha = \sqrt[n]{a}$.

■

Lemma 9.3. *Let F be a field and let $\zeta_n \in F$ be a primitive n-th root of unity. Suppose $K = F(\sqrt[n]{a})$ for some $a \in F$. Then K/F is a cyclic (Galois) extension of F.*

Proof. Consider the homomorphism

$$\begin{aligned} Aut(K/F) &\to \mathbb{Z}_n \\ \sigma &\to i \ (mod\ n) \end{aligned}$$

where $\sigma(\alpha) = \zeta_n^i \alpha$. The proof entails showing this is in fact an isomorphism, which is relatively easy to do on your own. ■

9.2 Radical Field Extensions

We usually call quantities such a $\sqrt{2}$ and $\frac{1}{2}\sqrt[3]{3 + \sqrt[10]{7}}$ as radicals.

Definition 9.4. *A finite extension K/F is <u>radical</u> if $K = F(\alpha_1, \ldots, \alpha_r)$ and there exists integers $n_1, \ldots, n_r$ with $\alpha_i^{n_i} \in F(\alpha_1, \ldots, \alpha_{i-1})$ for all $i \geq 2$.*
If $n_1 = n_2 = \ldots = n_r = n$, then K/F is an <u>n-radical extension</u>.

In essence, we can raise every element in the field extension K/F to some power in order to return the element to the original field F.

Example 9.5. *Consider $\mathbb{Q}(\sqrt[4]{2})$. This is clearly a 4-radical extension of $\mathbb{Q}$, but it's also 2-radical since*

$$\mathbb{Q}(\sqrt[4]{2}) = \mathbb{Q}(\sqrt{2}, \sqrt[4]{2}) \quad \text{because} \quad (\sqrt[4]{2})^2 \in \mathbb{Q}(\sqrt{2})$$

Definition 9.6. *Let K/F be a finite extension. The <u>normal closure</u> of K/F is the splitting field over F of*

$$\{\text{minimal polynomial of } \alpha \text{ over } F : \alpha \in K\}$$

Lemma 9.7. *Let K/F be a finite, n-radical extension of F. Then the normal closure N/F of K/F is also n-radical.*

Lemma 9.8. *Let K/F be a finite Galois extension. Let L/F be a finite extension. Then*

$$KL/L$$

is Galois and $Gal(KL/L) \cong Gal(K/K \cap L)$.

Note 9.9. *Clearly this lemma is analogous to the Second Isomorphism from Group Theory. In particular,*

$$Gal(KL/L) \cong \text{ subgroup of } Gal(K/F)$$

Lemma 9.10. *Let K/F be a finite extension, and let $\zeta \in K$ be a root of unity (not assuming it's primitive). Then $F(\zeta)/F$ is Galois with an abelian Galois group.*

9.3 Galois Criterion for Polynomial Solvability

Definition 9.11. *Let F be a field, and let $f(x) \in F[x]$. Then f is solvable by radicals if there exists a radical extension L of F such that $f(x)$ splits over L.*

Theorem 9.12 (Galois Solvability)**.** *Let F be a field of characteristic 0. Let $f(x) \in F[x]$. Let K be a splitting field of $f(x)$ over F. Then $f(x)$ is solvable by radicals if and only if $Gal(K/F)$ is solvable.*

Note 9.13. *This is why we defined certain groups as solvable.*

Proof. ($\Rightarrow$) Suppose for some n, there exists an n-radical extension M of F such that the polynomial f splits over M. Let ζ be a primitive n-th root of unity in some extension of M. *You should check that there is some extension of M that will possess this root, which comes as the result of M being characteristic 0 as well as the separability of the polynomial $x^n - 1$.* Then $M(\zeta)$ is an n-radical extension of F, since M is an n-radical extension of F and $\zeta^n = 1 \in F$.

Let L be the normal closure of $M(\zeta)/F$. That is L is the splitting field of the collection of minimal polynomials

$$\{m_{\alpha,F} : \alpha \in M(\zeta)\}$$

Notice, as a result from the homework, that L/F is a finite extension. By Lemma 9.7, we know L/F is an n-radical extension since $M(\zeta)/F$ is n-radical. Now consider the chain:

$$\begin{array}{c} F_r = L \\ | \\ F_{r-1} \\ | \\ \vdots \\ | \\ F_1 = F(\zeta) \\ | \\ F_0 = F \end{array}$$

where $F_{i+1} = F_i(\alpha_i)$ for $i \geq 1$ and some α_i with $\alpha_i^n \in F_i$. Now, using Lemma 9.10, we know that each extension

$$F_{i+1}/F_i \text{ is cyclic and Galois}$$

for $i \geq 1$. Moreover, F_1/F_0 is abelian and Galois.

Now, because $char(F) = 0 \implies L/F$ is Galois since we get separability from $char(F) = 0$. Now define

$$H_i = Gal(L/F_i)$$

So $\{id\} = H_r \subset H_{r-1} \subset \ldots \subset H_1 \subset H_0 = Gal(L/F)$. Since F_{i+1}/F_i is Galois for all i, then we must have

$$H_{i+1} \trianglelefteq H_i \quad \text{and} \quad H_i/H_{i+1} \cong \underbrace{Gal(F_{i+1}/F_i)}_{abelian}$$

So $Gal(L/F) = H_0 \trianglerighteq H_1 \trianglerighteq \ldots \trianglerighteq H_r = \{id\}$ is an abelian series. Therefore $Gal(L/F)$ is solvable! Observe, $Gal(K/F) \cong Gal(L/F)/Gal(L/K)$. Since $Gal(K/F)$ is the quotient of solvable groups, it must also be solvable!

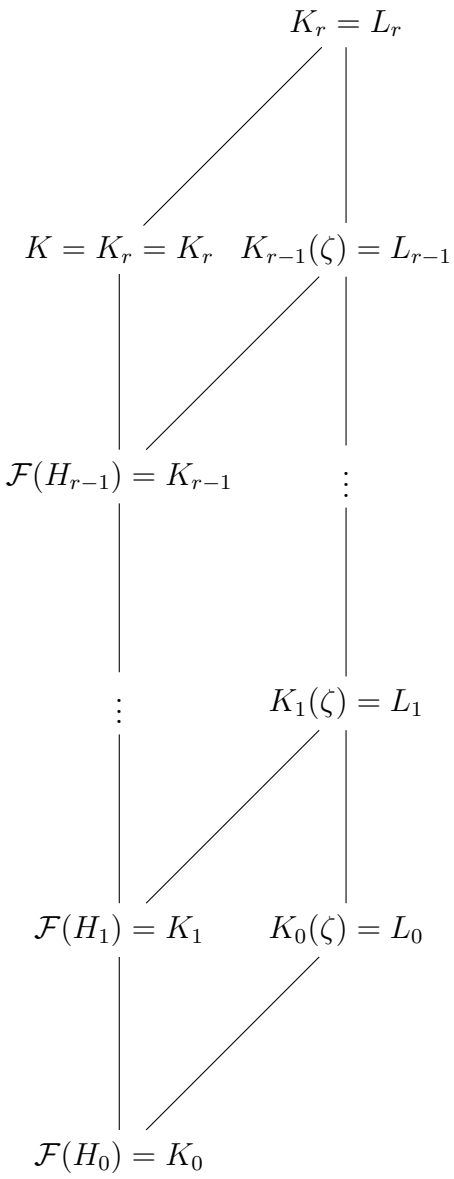
($\Leftarrow$) Suppose $Gal(K/F)$ is solvable. Then there exists

$$Gal(K/F) = H_0 \trianglerighteq H_1 \trianglerighteq \ldots \trianglerighteq H_r = \{id\}$$

where H_i/H_{i+1} is cyclic (since every abelian series admits a cyclic refinement). Now let $K_i = \mathcal{F}(H_i)$ and let $n = lcm([K_{i+1} : K_i])$. Let ζ be a prime n-th root of unity. For each $0 \leq i \leq r$, let

$$L_i = K_i(\zeta)$$

We can depict the subfield lattice as:



Trying to interpret this diagram, from Galois correspondence, we have K_{i+1}/K_i is a Galois extension since $H_{i+1} \trianglelefteq H_i$. Also,

$$L_{i+1} = L_i K_{i+1}$$

Now we can leverage Lemma 9.8 to conclude

$$L_{i+1}/L_i = L_i K_{i+1}/L_i$$

is a Galois extension with $Gal(L_{i+1}/L_i) \cong$ a subgroup of $Gal(K_{i+1}/K_i) \cong H_i/H_{i+1}$ which is abelian / cyclic. So

$$d_i := [L_{i+1} : L_i] \text{ divides } [K_{i+1} : K_i] \text{ divides } n$$

So a suitable power of ζ, specifically $\zeta^{n/d}$, is a primitive d_i-th root of unity and L_i contains it. So L_{i+1}/L_i is radical. Notice L_0/F is also radical. So L_r is a radical extension of F. So the splitting field K of $f(x)$ is contained in a radical extension of F. Therefore, $f(x) = 0$ is solvable by radicals. ■

Example 9.14. *$x^5 - 1$ is solvable by radicals with solutions:* $1, \frac{-1}{4} - \frac{1}{4}\sqrt{5} \pm \frac{1}{4}\sqrt{-10 + 2\sqrt{5}}, \frac{-1}{4} + \frac{1}{4}\sqrt{5} \pm \frac{1}{4}\sqrt{-10 - 2\sqrt{5}}$

Example 9.15. *$x^5 - 2x + 1$ is NOT solvable by radicals.*

9.4 Implications of Galois' Criterion

Definition 9.16. *Let F be of characteristic 0 and $f(x) \in F[x]$. The Galois group of $f(x)$, denoted $Gal(f)$, is the Galois group of a splitting field of $f(x)$ over F.*

Lemma 9.17. *Let $f(x) \in F[x]$ be a separable polynomial of degree n. Then there exists an injection*

$$Gal(f) \to S_n$$

Moreover, if f is irreducible, then the image is a transitive subgroup of S_n.

Definition 9.18. *A transitive subgroup $H \leqslant S_n$ is a group such that given $1 \leq i, j \leq n$, there exists $\sigma \in H$ such that $\sigma(i) = j$.*

Proof. Let $\sigma \in G$. Then σ takes any of the n roots of f in K to another unique root fo f. That is, it gives rise to a permutation in S_n. It's easy to check that the corresponding map $G \to S_n$ is a group homomorphism with trivial kernel, and therefore an injection.

To demonstrate the transitivity of this subgroup, if $f(x)$ is irreducible, we have for all roots α, β of $f(x)$, there exists $\sigma \in G$ with $\sigma(\alpha) = \beta$. ■

Question 9.19. *When is it a Galois group actual becomes the Symmetric Group S_n?*

There is, in a sense, a "typical" degree n polynomial that has a Galois group S_n.

Theorem 9.20. *Let F be of characteristic 0. Then every polynomial of degree less than 4 is solvable by radicals, and a "typical" polynomial of degree greater than or equal to 5 is not solvable by radicals.*

Example 9.21. *$x^5 - 4x + 2 \in \mathbb{Q}[x]$ is not solvable by radicals. By Eisenstein's Criterion for $p = 2$, we see this polynomial is irreducible. Graphing this polynomial, you would see this has 3 roots in $\mathbb{R}$. Clearly there must then be 2 roots in $\mathbb{C}/\mathbb{R}$. More over, these complex roots are complex conjugates of each other.*

Let $K/\mathbb{Q}$ be a splitting field of f over $\mathbb{Q}$. Let $\alpha \in K$ be a root of f. Then

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5 \implies 5 | [K : \mathbb{Q}] = |Gal(K/\mathbb{Q})|$$

by the Tower Theorem. By Cauchy's Theorem, $Gal(K/\mathbb{Q})$ has an element of order 5. Viewing $Gal(K/\mathbb{Q}) \leqslant S_5 \implies \sigma$ is a 5-cycle. But by complex conjugation is an element of $Aut(\mathbb{C}/\mathbb{Q})$, and restricting it to K, we get $\tau \in Gal(K/\mathbb{Q})$, which is a transposition.
But we know a subgroup of S_5 containing a 5-cycle and a 2-cycle is all of S_5. Therefore,

$$Gal(K/\mathbb{Q}) \cong S_5$$

which is not solvable. Therefore $f(x)$ is not solvable by radicals.

9.4.1 Solving Cubics and Quartics

Definition 9.22. *Let F be a field, $f(x) \in F[x]$ of degree n, and let $\alpha_1, \ldots, \alpha_n$ be the roots of f in some splitting field. Let*

$$\Delta = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)$$

Then the discriminant of $f(x)$ is $D = \Delta^2$.

Lemma 9.23. *Let F be of characteristic $\neq 2$, let $f(x) \in F[x]$ be separable, and let K be a splitting field of $f(x)$ over F. Then $D \in F$ and if $\sigma \in Gal(K/F)$ then σ is an even permutation if and only if $\sigma(\Delta) = \Delta$ and odd if and only if $\sigma(\Delta) = -\Delta$.*

Corollary 9.23.1. *$Gal(K/F) \leqslant A_n$ if and only if D is a square in $F \implies \exists y \in F$ such that $D = y^2$.*

Proof. $Gal(K/F) \leqslant A_n \iff \sigma(\Delta) = \Delta \forall \sigma \in Gal(K/F) \iff \Delta \in F$. ■

Remark 9.24. *So $Gal(K/F) = \{id\}$ if D is a square and order 2 if D is not.*

Theorem 9.25. *Let F be a field of characteristic 0, and let $f(x) \in F[x]$ be irreducible and degree 3. Let $G = Gal(f)$. Then*

- *$G \cong A_3 \cong Z_3$ if and only if D is a square in F.*
- *$G \cong S_3$ if and only if D is not a square in F.*

Proof. We only need to check is that the transitive subgroups of S_3 are S_3 and A_3. ■

Lemma 9.26. *Let $f(x) = x^3 + ax + b \in F[x]$. Then $D = -4a^3 - 27b^2$. Then the solutions of this polynomial are given by*

$$\sqrt[3]{-\frac{b}{2} + \sqrt{\left(\frac{b}{2}\right)^2 + \left(\frac{a}{3}\right)^3}} + \sqrt[3]{-\frac{b}{2} - \sqrt{-\left(\frac{b}{2}\right)^2 + \left(\frac{a}{3}\right)^3}}$$