McGill Winter 2025 - MATH457 - Honors Algebra IV
Taught By: Prof. Henri Darmon
Notes By: Megan Millet

Contents

List of Definitions

List of Theorems, Propositions, Lemmas

1 Introduction

Recall that algebra 3 was a study of:

1. groups
2. rings and fields
3. modules and vector spaces

We will now focus on composite theories.
Things we will study in algebra 4:

1. Representation theory (which uses groups and modules and vector spaces)
2. Galois theory (this is the study of fields via the study of groups)

   - we study the quadratic equation

   - there are similar formulas for the general cubic and quartic equations

   - is there a general formula to find the roots of a general quintic equation involving the extraction of n-th roots? no! there is no general formula.

   - Galois associated to any equation $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ that one can associate a group G and one can see whether the roots can be expressed in terms of n-th roots from the properties of this group; i.e. whether or not $f(x) = 0$ can be solved by radicals

2 Representation Theory

2.1 Introduction

Why do we study representation theory? We want to find out, given a group G, all of the "representations" that G acts on. In representation theory, we are mostly interested in the following representations:

1. a set (permutation representation)
2. modules over a ring ($\mathbb{Z}$), or usually a field ($\mathbb{C}$, field of characteristics $p > 0$) (linear representations)

Example. Let G be the rotations of icosohedron (D20). It has 60 symmetries.

1. Permutation representations: 20 faces, 30 edges, 12 vertices, 6 diagonals.
2. Linear representations: $\mathbb{R}^3$ because it lives in 3D space.

One can learn a lot about the structure of a group G by understanding how it can act on other mathematical structures (e.g. a set).

Definition 2.1 (G-set)*.* Let X be a set. We say that X is a G-set if there is a binary map $G \times X \to X$ such that $(g, x) \mapsto gx$ for all $x \in X$, we also require $1x = x$ and $(g_1 g_2)x = g_1(g_2 x)$ for all $g_1, g_2 \in G, \forall x \in X$.

Definition 2.2 (Linear Representation)*.* A *linear representation* of a group G is a vector space V over a field F equipped with a map $G \times V \to V$ such that

1. $1v = v \quad \forall v \in V$
2. $(g_1 g_2)v = g_1(g_2 v) \quad \forall g_1, g_2 \in G, \forall v \in V$
3. $v \mapsto gv$ is a linear transformation $\forall g \in G$

Remark 2.3*.* Properties 1 and 2 together imply that V is a G-set.

Different ways of viewing representations of G:

1. Homomorphism $\rho : G \to Aut_F(V)$ (this is analogous to $\rho : G \to Aut(X) = Perm(X)$)
2. If $\dim_F(V) = n$ is finite, then $\rho : G \to \mathrm{GL}_n(F)$ (analogous to $\rho : G \to S_n$)
3. Modules over the group ring $F[G]$ which is the collection of all formal finite linear combinations of elements of the group G, i.e.

$$F[G] = \left\{ \sum_{g \in G} \lambda_g g \right\}$$

   We have that:

$$\left(\sum_{g \in G} a_g g \right) \left(\sum_{h \in G} b_h h \right) = \sum_{g,h \in G} a_g b_h (gh)$$

   We also have that:

$$\left(\sum_{g \in G} \lambda_g g \right) v = \sum_{g \in G} \lambda_g (gv)$$

Definition 2.4 (Irreducible representation)*.* A representation V of G is called *irreducible* if there is no G-stable

$$0 \neq W \subset V$$

where W is a proper subset of V (not equal to V).

Remark 2.5. A representation is never transitive.

Example. $G = \mathbb{Z}/2 = \{1, \tau\}$ where $\tau^2 = 1$. If V is a representation of G then V is determined by $\rho : G \to Aut_F(V)$, so we consider $\rho(\tau) \in Aut_F(V)$. We know that $\tau^2 = 1$, so $\rho(\tau^2) = 1 = \rho(\tau)^2$. What are the eigenvalues of $\rho(\tau)$? The eigenvalues are 1 or -1. The minimal polynomial of $\rho(\tau)$ divides $x^2 - 1 = (x-1)(x+1)$. Assume that $2 \neq 0$ in F. We have that $V = V_+ \oplus V_-$ such that:

$$V_+ = \{v \in V : \tau v = v\} \quad V_- = \{v \in V : \tau v = -v\}$$

Here, V is irreducible if and only if $(dim(V_+), dim(V_-)) = (0,1)$ or $(1,0)$.

Example. Let G be a finite abelian group. That is, $G = \{g_1, g_2, \ldots, g_n\}$. V is a representation of G. Consider $\{T_1, T_2, \ldots, T_N\}$ where $T_j = \rho(g_j) \in Aut_F(V)$. Assume F is of characteristic zero and F is algebraically closed (i.e. can think of $F = \mathbb{C}$). Every linear transformation in a complex space has an eigenvector. Fact: $\{T_1, \ldots, T_n\}$ have a simultaneous eigenvector $v \in V$. So the line that spans this vector is a one-dimensional vector space which stabilizes the entire group. Here the finite abelian group is irreducible if and only if it is one-dimensional.

General Assumptions:

1. G is a finite group
2. the vector space V is finite dimensional
3. the field F of a vector space is algebraically closed and of characteristic 0 (such as $\mathbb{C}$)

Theorem 2.6 (Abelian Group with Irreducible Representation)**.** *If G is an abelian group and V is an irreducible finite dimensional representation of G, then $dim(V) = 1$.*

Proof. Let $G = \{g_1, g_2, \ldots, g_N\}$. Let $\rho : G \to Aut_{\mathbb{C}}(V)$ and $\tau_j = \rho(g_j)$ for $\tau_j : V \to V$. Then $\tau_1, \ldots, \tau_N$ are pairwise commuting. We have that:

$$\begin{aligned} \tau_i \circ \tau_j &= \rho(g_i) \circ \tau(g_j) \\ &= \rho(g_i \cdot g_j) \\ &= \rho(g_j \cdot g_i) \\ &= \rho(g_j \cdot g_i) \\ &= \tau_j \circ \tau_i \end{aligned}$$

We have that $\tau_1, \ldots, \tau_N$ have a simultaneous eigenvector ν. That is, $\tau_j v = \lambda_j \nu \quad \forall j = 1, \ldots, N$. Then $\mathbb{C} \cdot \nu = span(\nu)$ is a subrepresentation of V, so $V = \mathbb{C}\nu$. □

Proposition 2.7 (Common Eigenvector)**.** *If $T_1, \ldots, T_N$ is a collection of commuting linear transformations on a complex vector space, then they have a common eigenvector.*

Proof. We will proceed by induction on N. For $N = 1$: The minimal or characteristic polynomial has a root λ, so λ is an eigenvalue and we can let v be the associated eigenvector (by def v is non-zero). Now we assume that this holds for N and will show it holds for $N+1$. Given $T_1, \ldots, T_N, T_{N+1}$. Let λ be an eigenvalue for T_{N+1}. Let $V_\lambda = \{v \in V : T_{N+1} v = \lambda v\}$ be the eigenspace such that $0 \neq V_\lambda \subset V$. Claim: each T_j maps V_λ to itself. Let $v \in V_\lambda$.

$$\begin{aligned} T_{N+1}(T_j v) &= T_j(T_{N+1} v) \\ &= T_j(\lambda v) \\ &= \lambda(T_j v) \\ &\implies T_j v \in V_\lambda \end{aligned}$$

This is not to say that T_jv is an eigenvector of V_λ, but it is certainly contained in V_λ. By the induction hypothesis, there is a simultaneous eigenvector $v \in V_\lambda$ for $T_1, \dots, T_N$. So v is also an eigenvector for T_{N+1} since it was chosen in V_λ. This does not mean that they have the same eigenvalue for each T_j either. It can vary by scalars. □

Remark 2.8. Every irreducible representation of an abelian group G is given as a homomorphism $\rho : G \to \mathbb{C}^*$.

2.2 Non Abelian Groups

Example. Let $G = S_3$ and let F be an arbitrary field with the assumption that $2 \neq 0$. Given $\rho : G \to Aut_F(V)$ we want to consider $T = \rho((23)) \implies T^2 = I$. T is diagonalizable with eigenvalues contained in the set $\{1, -1\}$.
Case 1: -1 is the only eigenvalue of T, i.e. (23) acts as $-I$. Then we can also claim that (12) acts as $-I$ because it is conjugate to (23). That is, $(12) = g(23)g^{-1}$ for some $g \in S_3$. So we have that:

$$\rho((12)) = \rho(g)\rho((23))\rho(g)^{-1} = -I$$

Similarily, $\rho((13)) = -I$. Now we can consider $\rho((123)) = \rho((13)(12)) = \rho((13) \circ \rho((12))) = (-I)(-I) = I$ Likewise for the other element of order 3 in S_3. So we have that $\rho : G \to Aut_{\mathbb{C}}(V) = \mathbb{C}^*$ and then $\rho(g) = sign(g)$.
Case 2: 1 is an eigenvalue of $t = \rho((123))$. Let e_1 be a non-zero vector fixed by T. So $Te_1 = e_1$. Let $e_2 = (123)e_1$ and $e_3 = (123)e_2$. We find that $\{e_1, e_2, e_3\}$ is preserved by S_3, so the representation V has dimension at most 3. $V = span\{e_1, e_2, e_3\}$.
Case 2a: Assume $w = e_1 + e_2 + e_3 \neq 0$. S_3 fixes w. That is, taking any element of S_3, say $(12)w = (e_2 + e_1 + e_3) = w$ is fixed (it is just permuted). So $V = span(w)$ so $dim(V) = 1$, i.e. $e_1 = e_2 = e_3$.
Case 2b: Assume $w = e_1 + e_2 + e_3 = 0$. Still have that $V = span(w)$ but there is a linear relation among the three vectors, so the dimension of the span is at most 2. So $dim(V) \leq 2$. We also know that each of the elements must be distinct because their sum equals 0, i.e. $e_1 \neq e_2 \neq e_3$. Consider $(23)e_1 = e_1$. If we take $(23)(e_2 - e_3) = e_3 - e_2 = -(e_2 - e_3)$, which implies that $dim(V) = 2$. Relative to the basis (e_1, e_2) for V, the representation of S_3 is given by

$$1 \leftrightarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad (12) \leftrightarrow \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad (13) \leftrightarrow \begin{pmatrix} -1 & 0 \\ -1 & 1 \end{pmatrix} \quad (23) \leftrightarrow \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix} \quad (123) \leftrightarrow \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$$

$$(132) \leftrightarrow \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$$

Conclusion: There are essentially three distinct irreducible representations of S_3.

1. sign: $S_3 \to \mathbb{C}^*$ by $\mathbb{C}^* = Aut_{\mathbb{C}}(\mathbb{C})$
2. triv: $S_3 \to \mathbb{C}^*$
3. 2-dim rep

Essentially we have shown that given $G = S_3$, if $6 \neq 0$ in F then G has two one-dimensional irreducible representations and one 2-dimensional irreducible representation.

Example. Let $G = D_8 = \{1, r, r^2, r^3, V_1, H_1, D_1, D_2\}$ permutations on a square. Consider the element r^2. It commutes with every element of G. We have a representation $\rho : D_8 \to Aut_F(V)$ such that in F, $2 \neq 0$. Now can can consider $T = \rho(r^2) \in Aut_F(V)$ and it is of order 2 so $T^2 = I$. The minimal polynomial of T

divides $x^2 - 1$, and hence it has distinct roots provided that $2 \neq 0$; thus it is diagonalizable. So we have that $V = V_+ \oplus V_-$ such that:

$$V_+ = \{v \in V : r^2 \cdot v = v\} \quad V_- = \{v \in V : r^2 \cdot v = -v\}$$

Key fact: V_+ and V_- are preserved by any element $g \in D_8$. We will now prove this fact.

Proof. Take $v \in V_+$. We want to see if $gv \in V_+$. We take:

$$\begin{aligned} r^2(gv) &= r^2 g \cdot v \\ &= gr^2 v \\ &= gv \quad \text{since } r^2 v = v \end{aligned}$$

Thus $gv \in V_+$. The proof for V_- is similar. Consider $v \in V_-$.

$$\begin{aligned} r^2(gv) &= r^2 gv \\ &= gr^2 v \\ &= g(-v) \\ &= -gv \end{aligned}$$

Thus $gv \in V_-$. □

From this, if V is irreducible then either $V = V_+$ or $V = V_-$. So $\rho(r^2)$ acts as a scalar that is either I or $-I$.
Case 1: $\rho(r^2) = I$. We have that $\rho : D_8 \to Aut_F(V)$ also factors as $\rho : D_8 \to D_8/\{1, r^2\}$ which is isomorphic to the Kleine four group, or two copies of $\mathbb{Z}/2 \times \mathbb{Z}/2$. I.e. $\rho : D_8 \to D_8/\{1, r^2\} \to Aut_F(V)$. So V is 1-dimensional. Now we have that $\rho : D_8/\{r^2\} \to F^*$ provided that $\rho(g_1), \rho(g_2) \in \{1, -1\}$. So there are four distinct representations in total for this.
Case 2: $\rho(r^2) = -I$.

Proposition 2.9 (Eigenvalues of H_1 in D_8). *$\rho(H_1)$ has both eigenvalues 1 and -1.*

Proof. If $\rho(H_1) = I$, then $\rho(V_1) = \rho(r^2 H_1) = \rho(r^2)\rho(H_1) = -I$. We also have that $V_1 = rH_1r^{-1}$. So $\rho(V_1) = \rho(rH_1r^{-1}) = \rho(r)\rho(H_1)\rho(r^{-1}) = I$. But then we have that $\rho(V_1) = I = -I$ a contradiction. So we cannot have that $\rho(H_1) = I$. Similarily, if $\rho(H_1) = -I$ we get a contradiction. □

Now to conclude Case 2: If $\rho(H_1) = -I$ then $\rho(V_1) = T(-I)T^{-1} = -I$ but $\rho(V_1 H_1) = I = \rho(r^2) = -I$ another contradiction. Thus $\rho(-1) \neq -I$.
Let $v_1 \in V$ satisfy $H_1 v_1 = v_1$ which exists by the previous proposition. Take also $v_2 \in V$ such that $v_2 = rv_1$.
Claim: the $span\{v_1, v_2\}$ is preserved by D_8 and $span\{v_1, v_2\} = V$.

Proof. Take $r \in D_8$. Then $rv_1 = v_2$. Also, $rv_2 = r^2 v_1 = -v_1$. Then $\{1, r, r^2, r^3\}$ preserves $span\{v_1, v_2\}$. Take $H_1 \in D_8$. Then $H_1 v_1 = v_1$. We consider: if v_1 is fixed by H_1 then rv_1 is fixed by $rH_1r^{-1} = V_1$. Thus know that $V_1 v_2 = v_2$. So if we apply r^2 to both identities, we get that $r^2 H_1 v_1 = r^2 v_1 \implies V_1 v_1 = -v_1$ and $r^2 v_2 = r^2 V_1 v_2 \implies Hv_2 = -v_2$.
Then we have that:

$$H_1 \leftrightarrow \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad V_1 \leftrightarrow \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

It follows that $span\{v_1, v_2\}$ is preserved by D_8. We can also show that

$$D_1 = rH_1 \leftrightarrow \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

□

Definition 2.10 (G-homomorphism). If V_1 and V_2 are two representations of a fixed group G. A *G-homomorphism* from V_1 to V_1 is a linear map $\rho : V_1 \to V_2$ such that $\rho(gv) = g\rho(v)$ for all $g \in G, v \in V_1$. Moreover, if ρ is a vector space isomorphism then V_1 and V_2 are said to be isomorphic.

Questions to Consider:

- Describe all the irreducible representations of the group G up to isomorphism
- How is a general representation of G made up of irreducible representations

Remark 2.11. If V_1 and V_2 are two representations of G, then $V_1 \oplus V_2$ is also a representation of G. The action is:

$$g(v_1, v_2) = (gv_1, gv_2)$$

will satisfy all the axioms of an action on a linear representation.

Proposition 2.12 (Finite G has G-stable complement). *Let V be a representation over a finite G over $\mathbb{C}$, and let W be a sub-representation. Then W has a G-stable complement W'. I.e. $V = W \oplus W'$.*

Proof. Let W_0' be any complementary subspace of W. We will consider a linear projection $\pi : V \to W$ such that $\pi^2 = \pi$ and $\Im(\pi) = W$, $\ker(\pi) = W_0'$. We are going to improve π to make it G-invariant by replacing it by

$$\tilde{\pi} : \frac{1}{\#G} \sum_{g \in G} \rho(g)\pi \cdot \rho(g)^{-1}$$

This is called the averaging trick. Key properties:

- $\tilde{\pi}$ is G-equivariant. I.e. $\tilde{\pi}(gv) = g\tilde{\pi}(v)$.
- $\tilde{\pi}$ is a projection onto the vector space W, i.e. $\tilde{\pi}^2 = \tilde{\pi}$ and $\Im(\tilde{\pi}) = W$.

Claim: $W' = \ker(\tilde{\pi})$. Consider $v \in W'$. Then we have that $\tilde{\pi}(gv) = g\tilde{\pi}(v) = g \cdot 0 = 0$. So it is stable under the group. Properties of $\tilde{\pi}$:

- $\tilde{\pi}$ is a projection onto W. We have that:

$$\begin{aligned}
\tilde{\pi}^2 &= (\frac{1}{\#G} \sum_{g \in G} g \circ \pi \circ g^{-1})(\frac{1}{\#G} \sum_{h \in G} h \circ \pi \circ h^{-1}) \\
&= \frac{1}{(\#G)^2} \sum_{g,h} g \circ \pi \circ g^{-1} \circ h\pi h^{-1} \\
&= \frac{1}{(\#G)^2} \sum_{g,h} g \circ g^{-1} \circ h\pi h^{-1} \\
&= \frac{1}{(\#G)^2} \sum_{g,h} \circ h\pi h^{-1} \\
&= \tilde{\pi}
\end{aligned}$$

- Similarily, the image of $\tilde{\pi} \subset W$. Take $w \in W$. Then

$$\tilde{\pi}(w) = \frac{1}{\#G} \sum_{g \in G} g \circ I \circ g^{-1}(w) = w$$

Also, we have that $\tilde{\pi}(hv) = h\tilde{\pi}(v)$ for all $h \in G$. We have that:

$$\begin{aligned}\tilde{\pi}(hv) &= \frac{1}{\#G}\sum_{g\in G} g \circ \pi \circ g^{-1}(hv)\\ &= \frac{1}{\#G}\sum_{g\in G} g \circ \pi \circ g^{-1}h(v)\\ &= \frac{1}{\#G}\sum_{g\in G} g \circ \pi \circ (h^{-1}g)^{-1}(v)\\ &= \frac{1}{\#G}\sum_{\tilde{g}\in G} h\tilde{g}\pi\tilde{g}^{-1}(v)\\ &= h\tilde{\pi}(v)\end{aligned}$$

We can now take W' to be the $\ker(\tilde{\pi})$. Then $V = W \oplus W'$ because $\tilde{\pi}$ is a projector, and W' is G-stable because for any $w \in W'$, we have that: $\tilde{\pi}(gw) = g\tilde{\pi}(w) = g \cdot 0 = 0$. So $gw \in W$. □

Remark 2.13. This proposition implies Matschke's Theorem.

Proposition 2.14 (Alternate Existence of G-stable complements)**.** *Let $W \subset V$ is a subrepresentation. Let $W' = W^{\perp} = \{v \in V :< v, w >= 0 \quad \forall w \in W\}$. Then $V = W \oplus W' = W \oplus W^{\perp}$ and is a G-stable subspace.*

Proof. Let $v \in W' = W^{\perp}$. $\forall w \in W$, $< gv, w >=< v, g^{-1}w >= 0$. So $gw \in W^{\perp}$. □

Theorem 2.15 (Matschke's Theorem)**.** *Any representation of a finite group G over $\mathbb{C}$ can be expressed as a direct sum of irreducible representations. I.e. If V is a representation of G then there exist $V_1, \ldots, V_t \subset V$ such that these are irreducible representations and $V = V_1 \oplus V_2 \oplus \ldots \oplus V_t$.*

Proof. Given V. Let W be any proper sub-representation of G in V. Let W' be the complementary subspace. We can write $V = W \oplus W'$, and we know that $dim(W) < dim(V)$ and $dim(W') < dim(V)$. We can proceed by induction on the $dim(V)$. □

Remark 2.16. This statement is analogous to the statement that every G-set is a union of transitive G-sets.

Remark 2.17. The assumption "G is finite" is essential. For a counter example, take $G = (\mathbb{Z}, +)$, $\rho : G \to GL_2(\mathbb{C})$ by $\rho(n) \to \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$. This ρ is a homomorphism. This representation is not irreducible because $span\{e_1\}$ is invariant (it has a non-trivial invariant subspace). So $\mathbb{C}\cdot e_1$ is an irreducible sub-representation of V. Are there any other invariant lines under the group G? Any other element not in the span will look like:

$$ae_1 | be_2, \quad b \neq 0$$

We can assume $b = 1$ wolog. I.e. consider $ae_1 + e_2$. The orbit of this vector under the action of G, i.e. $G \cdot (ae_1 + e_2)$. Take $1 \cdot (ae_1 + e_2) = (1 + a)e_1 + e_2$. Now take the difference of the two vectors to obtain $(ae_1 + e_2) - ((a+1)e_1 + e_2) \in G(ae_1 + e_2)$. Thus this representation is not the direct sum of two irreducible representations. (There is only one irreducible representation.)

Remark 2.18. $\mathbb{C}$ is necessary as well. Consider the counter example: $F = \mathbb{Z}/3/ZZ$, $V = Fe_1 \oplus Fe_2 \oplus Fe_3$. Take $G = S_3$ and let G act on the vector space according to permuting over the elements of the vector space. An obvious irreducible subrepresentation of the vector space V is $F \cdot (e_1 + e_2 + e_3)$. Let W be any G-stable subspace which is not equal to $F(e_1 + Fe_2 + Fe_3)$. Then there exist $ae_1 + be_2 + ce_3 \in W$ such that $(a, b, c) \neq (\lambda, \lambda, \lambda)$. If we apply (123) to this vector we obtain $ce_1 + ae_2 + be_3 \in W$. If we apply (132)

we obtain $be_1 + ce_2 + ae_3 \in W$. Then their sum is in W, i.e. $(a + b + c) \cdot (e_1 + e_2 + e_3) \in W$. We can apply (12) to the vector to obtain $be_1 + ae_2 + ce_3 \in W$. Taking the different of the two vectors we obtain: $(a - b) \cdot (e_1 - e_2) \in W$. Similarily, $(b - c) \cdot (e_2 - e_3) \in W$ and $(a - c) \cdot (e_1 - e_3) \in W$. We are assuming that the triple (a, b, c) are not all equal. That is, since at least one of $(a - b), (a - c), (b - c) \neq 0$, assume wolog $(a - b) \neq 0$, then this implies that $e_1 - e_2 \in W$, which implies that $e_2 - e_3, e_1 - e_3 \in W$. Then we can write $e_1 + e_2 + e_3$ as a linear combination of these three vectors by taking

$$(e_1 - e_2) - (e_2 - e_3) + (e_1 - e_3) + (e_2 + e_3) = e_1 + e_2 + e_3$$

Thus we have that $e_1 + e_2 + e_3 \in span\{(e_1 - e_2) - (e_2 - e_3) + (e_1 - e_3)\}$.

Definition 2.19 (Hermitian Inner Product). A *Hermitian Inner Product* of V is a Hermitian-bilinear function $V \times V \to \mathbb{C}$ by $(v, w) \mapsto < v, w >$ which satisfies:

1. $< v_1 + v_2, w >=< v_1, w > + < v_2, w >$
2. $< \lambda v, w >= \lambda \cdot < v, w > \quad \forall \lambda \in \mathbb{C}$
3. $< v, w_1 + w_2 >=< v, w_1 > + < v, w_2 >$
4. $< v, \lambda w >= \overline{\lambda} < v, w > \quad \forall \lambda \in \mathbb{C}$
5. Positivity Axiom: $< v, v >\in \mathbb{R}_{\geq 0}$ and $< v, v >= 0 \iff v = 0$

Theorem 2.20 (Existence of Hermitian Inner Product). *If V is a finite dimensional complex representation of a finite group G then there is a Hermitian inner product on V such that*

$$< gv, gw >=< v, w > \quad \forall g \in G, v, w \in V$$

Proof. Unitaraisability. Let $<, >_0$ be an arbitrary Hermitian inner product on V. That is, let $e_1, ldots, e_n$ be a basis for V. Define $< e_i, e_j >_0 \begin{cases} 0, & i = j \\ 1, & i \neq j \end{cases}$. Then we have that:

$$< \alpha_1 e_1 + \ldots + \alpha_n e_n, \beta_1 e_1 + \ldots + \beta_n e_n >_0 = \alpha_1 \overline{\beta_1} + \ldots + \alpha_n \overline{\beta_n} \in \mathbb{C}$$

Now we use the averaging trick:

$$< v, w >= \frac{1}{\#G} \sum_{g \in G} < gv, gw >_0$$

Claim: this is Hermitian linear, positive, and it is G-equivariant.
Positive: $< v, v >= \frac{1}{\#G} \sum_{g \in G} < gv, gv >_0 \subset \mathbb{R}_{\geq 0}$ and in particular, if $< v, v >= 0 \implies < v, v >_0 = 0 \implies v = 0$.
G-equivariant: $< hv, hw >= \frac{1}{\#G} \sum_{g \in G} < ghv, ghw >_0 = \frac{1}{\#G} \sum_{g \in G} < gv, gw >_0 =< v, w >$ □

Theorem 2.21 (Semisimplicity Matschke's Theorem). *If V is a representation of G, and $W \subset V$ is a subrepresentation, then there exists W' such that $V = W \oplus W'$ such that W' is also a subrepresentation.*

Definition 2.22 (Semisimplicity). A *semisimple* object is one which can be decomposed into *simple* objects.

Remark 2.23. Finite abelian groups are not semisimple in general.

Definition 2.24 (Simple Objects). Simple objects are represented by $\mathbb{Z}/p\mathbb{Z}$ for p prime.

Example. We have that $\mathbb{Z}/p^2\mathbb{Z}$ for p prime and C_4 are not semisimple abelian groups.

We consider the two following questions:

- Given G, give a complete list of the irreducible representations up to isomorphism, denoted $V_1, \dots, V_t$
- Given a general finite dimensional representation V of G,

  $$V = V_1^{m_1} \oplus V_2^{m_2} \oplus \dots \oplus V_t^{m_t}$$

  for m_j the multiplicity of V_j in V.

Definition 2.25 (Homomorphism subvector Space). Recall: If V, W are two G-representations, then we define:

$$Hom_G(V, W) = \{T : V \to W, T \text{ linear } : T(gv) = gT(w) \quad \forall g \in G, \forall v \in V\}$$

Remark 2.26. $Hom_G(V, W)$ is a $\mathbb{C}$-vector space.

Theorem 2.27 (Shur's Lemma)**.** *Let V and W be irreducible representations of a fixed group G. Then*

$$Hom_G(V, W) = \begin{cases} 0, & \text{if } V \not\simeq W \\ \mathbb{C}, & \text{if } V \simeq W \end{cases}$$

Proof. Suppose that $V \not\simeq W$. Let $T \in Hom_G(V, W)$. $\ker(T)$ is a subrepresentation of V because if $v \in \ker(T)$, then $gv \in \ker(T)$. That is: $T(gv) = gT(v) = g(0) = 0$. If $\ker(T) = 0$, then T would be injective, so we would have $W \simeq V$ which is a contradiction. Thus we have that $\ker(T) \neq 0$. Thus $\ker(T) = V$, so $V = 0$. Now we assume that $V \simeq W$. Let $T \in Hom_G(V, W) = End_G(V)$ because we have that $V \simeq W$. Since $\mathbb{C}$ is algebraically closed, T has an eigenvalue λ. We consider $T - \lambda I \in End_G(V)$. We have that $\ker(T - \lambda I) \neq 0$ because it contains an eigenvector. Thus it is a non-trivial subrepresentation of V. Thus $\ker(T - \lambda I) = V$ which implies that $T = \lambda I$. □

Corollary 2.28 (Shur's Corollary)**.** *Given V a general representation,*

$$m_j = \dim_{\mathbb{C}} Hom_G(V_j, V)$$

where m_j is the multiplicity of each V_j of V.

Proof. $Hom_G(V_j, V_1^{m_1} \oplus \dots \oplus V_t^{m_t}) = Hom_G(V_j, V)^{m_1} \oplus \dots \oplus Hom_G(V_j, V)^{m_t} = \mathbb{C}^{m_j}$. □

Definition 2.29 (Trace of an Endomorphism). Let $T : V \to V$. The *trace* of T is the Trace of any matrix representing T. The trace of $tr(PAP^{-1}) = tr(A)$, and $tr(AB) = tr(BA)$.

Proposition 2.30 (Trace of a Projection is Dimension of Space)**.** *Let $W \subset V$ be a subspace and π be a projection $V \to W$. Then $tr(\pi) = \dim(W)$.*

Proof. Let $v_1, \dots, v_d$ be a basis for W. Take $v_{d+1}, \dots, v_n$ be a basis for $\ker(\pi)$. We have that

$$\pi = \begin{pmatrix} \begin{pmatrix} 1 & \dots & 0 \\ 0 & 1 \dots & 0 \\ 0 & \dots & 1 \end{pmatrix} & \dots & 0 \\ 0 & \dots & 0 \end{pmatrix}$$

where the uppler block contains a $d \times d$ identity matrix. Thus $tr(\pi) = \dim(W)$. □

Example. Given $V_1 = \mathbb{C}$ with a trivial action of G, we have that:

$$Hom_G(V_1, \overline{V}) \simeq V^G = \{v \in V : gv = v \quad \forall g \in G\}$$

Recall Burnside's Lemma. Given X a permutation representation, we had that the number of orbits on G acting on X is equal to $\frac{1}{\#G}\sum_{g\in G}\#FP_X(g)$. The next theorem is a generalization of this lemma. Given a G-set X, we can consider a vector space V by considering $V = \mathbb{C}^x = \{\sum_{x\in X}\lambda_x : \lambda_x \in \mathbb{C}\}$. Then we have that $g(\sum_{x\in X}\lambda_x \cdot x) = \sum_{x\in X}\lambda_x(gx)$.

Example. Let $V =$\{set of functions on X\}. Then $V^G = \{f : X \to \mathbb{C} : gf = g\}$. Then we have if $f \in V^G$ that $gf(x) = f(g^{-1}x)\forall g \in G$. Thus $f(x) = f(g^{-1}x) \quad \forall g \in G$. So we find that $\dim(V^G)$ =the number of orbits of G on X. The trace of g acting on V is the number of fixed points of g acting on X.

Proposition 2.31 (Automorphisms over $\mathbb{C}$ are isomorphic to General Linear group)**.** *If V is a finite dimensional representation of a finite group G, then for $d = \dim_{\mathbb{C}}(V)$,*

$$\rho_V : G \to Aut_{\mathbb{C}}(V) \simeq GL_d(\mathbb{C})$$

for $V^G = \{v \in V : gv = v \quad \forall g \in G\}$.

Theorem 2.32 (Dimension represented by averages)**.** *If V is any representation of G, then*

$$\dim(V^G) = \frac{1}{\#G}\sum_{g\in G} tr(\rho(G))$$

for trivial subrepresentation $V^G = \{v \in V : gv = v \quad \forall g \in G\} = \bigcap_{g\in G}$(1-eigenspace for $\rho(g)$).

Proof. Recall that if you have a projector $\pi : V \to W$ (i.e $\pi^2 = \pi$) then the $\text{tr}(\pi) = \dim(W)$. Take $\pi = \frac{1}{\#G}\sum_{g\in G}\rho(g)$. Each individual row of G is an automorphism of this vector space. But the group of automorphisms of G is a group of units of the bigger ring (group of endomorphisms of the ring). So we have that $\pi \in End_{\mathbb{C}}(V)$. Some observations about π:

(i) $\Im(\pi) \subset V^G$:

$$\pi(v) = \frac{1}{\#G}\sum_{g\in G} g\cdot$$

Now if we take $h \in G$, then we have:

$$\begin{aligned} h(\pi(v)) &= \frac{1}{\#G}\sum_{g\in G} hg \cdot v \\ &= \pi \end{aligned}$$

(ii) If $v \in V^G$, then $\pi(v) = v$. So $\pi^2 = \pi$ and $\Im(\pi) = V^G$.

Thus π projects $V \to V^G$. Now we can apply our principle:

$$\dim(V^G) = \text{tr}(\pi) = \text{tr}\left(\frac{1}{\#G}\sum_{g\in G}\rho(g)\right) = \frac{1}{\#G}\sum_{g\in G}\text{tr}(\rho(g))$$

□

Remark 2.33. For each $g \in G$, $\rho(g)$ is of finite order and is hence diagonalizable.

Proof. $g^N = 1 \implies \rho(g)^N = 1 \implies$ the minimal polynomial of $\rho(g)|x^N - 1$. Recall that $x^N - 1 = (x-1)(x-\zeta)(x-\zeta^2)\ldots(x-\zeta^{N-1})$ for $\zeta = e^{2\pi i/N}$ is a primitive N-th root of unity. These factors are linear, algebraically closed, and distinct (which is a necessary and sufficient condition for the transformation to be diagonalizable). □

2.3 Characters of Representations

Definition 2.34 (Character)*.* If V is a finite dimensional representation of G then the *character* of V is the function $\chi_V : G \to \mathbb{C}$ defined by $\chi_V(g) = \mathrm{tr}(\rho_V(g))$.

Proposition 2.35 (Properties of χ_V)**.** *(i) χ_V is a class function conjugacy classes. That is,*

$$\chi_V(hgh^{-1}) = \chi_V(g)$$

(ii) $\chi_V(1) = \dim(V)$

(iii) $\frac{1}{\#G}\sum_{g\in G}\chi_V(g) = \dim(V^G)$

Proof. (i) $\chi_V(hgh^{-1}) = \mathrm{tr}(\rho_V(hgh^{-1})) = \mathrm{tr}(\rho_V(h)\rho_V(g)\rho_V(h^{-1})) = \mathrm{tr}(\rho_V(g)) = \chi_V(g)$.

(ii)

□

Example. Let $G = S_3$. Recall that S_3 has three irreducible representations:

(1) $V = \mathbb{C}$ with trivial action

(2) $V = sgn \simeq \mathbb{C}$ for $\rho(g) = sign(g)$

(3)

$$1 \leftrightarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad (12) \leftrightarrow \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad (13) \leftrightarrow \begin{pmatrix} -1 & 0 \\ -1 & 1 \end{pmatrix} \quad (23) \leftrightarrow \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix} \quad (123) \leftrightarrow \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$$

$$(132) \leftrightarrow \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$$

Now we can make a table:

	1	{(12), (13), (23)}	{(123), (132)}
χ_{triv}	1	1	1
χ_{sgn}	1	-1	1
χ_2	2	0	-1

Example. Let $G = D_8 = \{1, r, r^2, r^3, V, H, D_1, D_2\}$.

	$\{1\}$	$\{r^2\}$	$\{r, r^3\}$	$\{V, H\}$	$\{D_1, D_2\}$
χ_{triv}	1	1	1	1	1
χ_2	1	1	1	-1	-1
χ_3	1	1	-1	1	1
χ_4	1	1	-1	-1	1
χ_5	2	-2	0	0	0

Calculation for χ_5: We are considering $D/ < 1, r^2 >= \mathbb{Z}/2\mathbb{Z}$. We send $D_8 \to \mathbb{Z}/2\mathbb{Z}$. So V_5 corresponds to the matrices:

$$Id \leftrightarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad r \leftrightarrow \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad r^2 \leftrightarrow \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$r^3 \leftrightarrow \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad V = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \quad H = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$D_1 \leftrightarrow \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad D_2 \leftrightarrow = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$$

Patterns between the two examples:

1. It seems like the number of irreducible representations coincides with the number of conjugacy classes. $h(G) =$ the number of conjugacy classes.

2. Orthoginality of characters: if χ_i and χ_j are characters of irreducible representations of G, then we can take:
$$\frac{1}{\#G} \sum_{g \in G} \chi_i(g) \chi_j(g) = \delta_{ij} = \begin{cases} 1, & i \neq j \\ 0, & i = j \end{cases}$$

Theorem 2.36 (Isomorphic Representations and their Characters)**.** *If V_1 and V_2 are two representations then $V_1 \simeq V_2 \iff \chi_{V_1} = \chi_{V_2}$.*

Proof. Recall that if V is a representation, then $V \simeq V_1^{m_1} \oplus V_2^{m_2} \oplus \ldots \oplus V_t^{m_t}$ where $V_1, V_2, \ldots, V_t$ is a complete list of irreducible representations of G. V is determined by $(m_1, \ldots, m_t)$ for $m_i \geq 0$. We take $V_1 = \mathbb{C}$ with $gv = v \quad \forall g \in G$. Consider the space $V^G = V_1^{m_1} \simeq \mathbb{C}^{m_1}$. So we have that $m_1 = \dim(V^G)$. We also have that $m_1 = \frac{1}{\#G} \sum_{g \in G} \chi_V(g)$. We would now like to characterize the multiplicities m_j similarily. Consider $hom_G(V_j, V) = hom_G(V_j, V_1^{m_1} \oplus \ldots \oplus V_t^{m_t}) = hom_G(V_j, V_1)^{m_1} \oplus \ldots \oplus hom_G(V_j, V_t)^{m_t}$. Now we also know that
$$hom(V_j, V_i) = \begin{cases} 0, & \text{if } i \neq j \\ \simeq \mathbb{C}, & \text{if } i = j \end{cases}$$

by Shur's Lemma. So, this is isomorphic to $\mathbb{C}^{m_j}$. We then can say that:

$$m_j = \dim_{\mathbb{C}}(hom_G(V_j, V))$$

If $j = 1$, we have that $m_1 = \dim_{\mathbb{C}}(hom_G(\mathbb{C}, V))$. We call $hom_G(\mathbb{C}, V)$ the space of V^G. □

Remark 2.37. The passage from ρ_V to χ_i involves a great deal of loss on information.

Example. Recall the monster group: $\#G = 8 \cdot 10^{53}$. Its smallest non-trivial representation has dimension $d = 196883$. Then ρ_V is given as a collection of $8 \cdot 10^{53} \cdot 196883 \cdot 196883$ matrices. And the number of conjugacy classes $h(G) = 194$. So $\chi_V = 194$ conjugate numbers. This is characterized in "Atlas of Finite Groups" book.

If V and W are two G-representations then we can consider $hom(V, W)$ is also a vector space over $\mathbb{C}$. But it also carries a natural action of G. It is a representation of the group G. Given $T \subset hom(V, W)$ and $g \in G$. We want $g \star T \in hom(V, W)$. There are several actions:

(i) $(g \star T)(v) = T(g^{-1}v)$ which only depends only on the action on V

(ii) $(g \star T)(v) = g \cdot T(v)$ which depends only on the action on W

(iii) $(g \star T)(v) = gT(g^{-1}v)$ which combines both

These actions are:

(i) $hom(V, W) = hom(V, \mathbb{C})^{d_2}$ where $d_2 = \dim W$

(ii) $hom(V, W) = W^{d_1}$ where $d_1 = \dim V$

We always view $hom(V, W)$ as endowed by action (iii).
Key Property: $hom(V, w)^G = \{T : V \to W | g \star T = T\}$. Then $gT(g^{-1}v) = T(v)$. Then this is equivalent to saying that $T(g^{-1}v) = g^{-1}T(v)$.
This gives us the crucial formula:

$$hom(V, W)^G = \hom_G(V, W)$$

Recall that

$$m_j = \dim_{\mathbb{C}}(hom_G(V_j, V)) = \dim_{\mathbb{C}}(hom_G(V_j, V)^G) = \frac{1}{\#G} \sum_{g \in G} \chi_{hom(V_j,V)}(g)$$

2.4 Further Properties of Characters

(1) Given two G-representations V, W, then $V \oplus W$ is a G-representation. Then $g(v, w) = (gv, gw)$. We have that $\chi_{V \oplus W} = \chi_V + \chi_W$.

(2)

Theorem 2.38 (Character of Hom). $\chi_{hom(V,W)} = \overline{\chi_V} \chi_W$

Proof. Let $g \in G$. We know that $\rho_V(g)$ is a finite order linear representation so it is diagonalizable on V. Let $e_1, e_2, \ldots, e_m$ be an eigenbasis (basis of eigenvectors for $\rho_V(g)$) such that $m = \dim(V)$. We have that $g \cdot e_i = \alpha_i e_i$, for $\alpha_i \in \mathbb{C}$ and where $\alpha_i^N = 1$ for some N (N-th root of unity). Let $f_1, \ldots, f_n$ be a basis of eigenvectors for $\rho_W(g)$ acting on the space W where $n = \dim(W)$. We have that $g \cdot f_j = \beta_j f_j$ for $\beta_j \in \mathbb{C}$ which are also roots of unity. We can write:

$$\chi_V(g) = \sum_{i=1}^{m} \alpha_i \quad \text{and} \quad \chi_W = \sum_{j=1}^{n} \beta_j$$

We take $T_{ij} \in hom(V, W)$ for $i \in [1, m]$ and $j \in [1, n]$. We define it by:

$$T_{ij}(e_k) = \begin{cases} 0, & \text{if } k \neq i \\ f_j, & \text{if } k = i \end{cases}$$

So T_{ij} is a basis for $hom(V, W)$. Now we consider:

$$\begin{aligned} (g \star T_{ij})(e_i) &= gT_{ij}(g^{-1}e_i) \\ &= gT_{ij}(\alpha_k^{-1}e_i) \\ &= \alpha_k^{-1}gT_{ij}e_i \\ &= \alpha_k^{-1}gf_j \\ &= \alpha_k^{-1}\beta_j f_j \end{aligned}$$

Thus we have that:

$$(g \star T_{ij}) = \alpha_i^{-1}\beta_j T_{ij}$$

So $\rho_{Hom(V,W)}(g)$ is represented as a diagonal $mn \times mn$ matrix with entries equal to $\{\alpha_i^{-1}\beta_j\}_{i \in [1,m]; j \in [1,n]}$.
So we get that:

$$\chi_{hom(V,W)}(g) = \sum_{i \in [1,m]; j \in [1,n]} \alpha_i^{-1}\beta_j$$

We can then rewrite this as:

$$\begin{aligned}\chi_{hom(V,W)}(g) &= \sum_{i\in[1,m];j\in[1,n]} \alpha_i^{-1}\beta_j \\ &= \left(\sum_{i\in[1,m]} \alpha_i^{-1}\right)\left(\sum_{j\in[1,n]} \beta_j\right) \\ &= \left(\sum_{i=1}^{m} \overline{\alpha_i}\right)\left(\sum_{j=1}^{n} \beta_j\right) \\ &= \overline{\chi_V(g)}\chi_W(g)\end{aligned}$$

□

We now consider the orthogonality of irreducible group characters. Let $V_1, V_2, \dots, V_t$ be a complete list of distinct irreducible representations of G. Call $\chi_1, \chi_2, \dots, \chi_t : G \to \mathbb{C}$ are the association characters. $\chi_j \in L^2(G)$ (a Hilbert space with a Hermitian inner product). Given $f_1, f_2 \in L^2(G) \simeq \mathbb{C}^{\#G}$, we define

$$< f_1, f_2 >= \frac{1}{\#G}\sum_{g\in G} \overline{f_1(g)} f_2(g)$$

And $< f, f > \in \mathbb{R}^{\geq 0}$ and is equal to zero iff $f = 0$.

Theorem 2.39 (Orthogonality of Characters). $< \chi_i, \chi_j >= \begin{cases} 0, & \textit{if } i = j \\ 1, & \textit{if } i \neq j \end{cases}$

Proof.

$$\begin{aligned}< \chi_i, \chi_j > &= \frac{1}{\#G}\sum_{g\in G} \overline{\chi_i(g)}\chi_j(g) \quad \text{by defn} \\ &= \frac{1}{\#G}\sum_{g\in G} \chi_{hom(V_i,V_j)} \quad \text{by previous theorem} \\ &= \dim_{\mathbb{C}}(hom(V_i, V_j))^G \quad \text{by the generalization of burnside} \\ &= \dim_{\mathbb{C}}(hom(V_i, V_j)) \quad \text{by defn of the } G \text{ action} \\ &= \dim_{\mathbb{C}} = \begin{cases} \mathbb{C}, & \text{if } i = j \\ 0, & \text{if } i \neq j \end{cases} \quad \text{by Shur's lemma}\end{aligned}$$

□

Corollary 2.40 (Orthonormal system). *$\chi_1, \dots, \chi_t$ are an orthonormal system of vectors in $L^2(G)$.*

Corollary 2.41 (Linear Independence of characters). *$\chi_1, \dots, \chi_t$ are linearly independent*

Corollary 2.42 (Number of characters smaller than dimension of space). *$t \leq \#G = \dim(L^2(G))$*

Corollary 2.43 (Number of characters smaller than number of conjugacy classes). *$t \leq h(G) =$ number of distinct conjugacy classes*

Proof. $\underbrace{\{f : G \to \mathbb{C} : f(hgh^{-1}) = f(g)\}}_{\text{dim}=h(G)} = \text{class functions} = L^2_{\text{class}}(G) \subset \underbrace{L^2(G)}_{\text{dimension}=\#G}$ □

We now know that if $V_1, \dots, V_t$ is a full list of irreducible representations, then $t \leq h(g)$.
Recall: For $G = S_3$, there are exactly 3 irreducible representations ($t = 3$) such that $d_1 = d_2 = 1$ and $d_3 = 2$. We also had that $h(g) = 3$.
Also recall that for $G = D_8$, we had $t = 5$, $d_1 = d_2 = d_3 = d_4 = 1$ and $d_5 = 2$.
We observe that $t = h(g)$ in these examples. We also have that the sum of the squares of the dimensions is equal to cardinality of G.

Definition 2.44 (Regular representation of G). $\mathbb{C}[G] = \{\sum_{g \in G} \lambda_g \cdot g : \lambda_g \in \mathbb{C}\}$ where G acts on $\mathbb{C}[G]$. This $\mathbb{C}[G]$ is called the regular representation.

Proposition 2.45 (Formula for χ of regular representations). $\chi_{\mathbb{C}[g]}(g) = \#\{h \in G : gh = h\} = \begin{cases} \#G & \text{if } g = 1 \\ 0, & \text{if } g \neq 1 \end{cases}$

2.5 Orthogonality of Irreducible Characters

Let G be a finite group, $V_1, \dots, V_t$ be irreducible representations of G. Set $p_j : G \to Aut_{\mathbb{C}}(V_j)$. Let $\chi_1, \dots, \chi_t$ be the associated characters. Let $\chi_j(g) = tr(p_j(g))$.

Theorem 2.46 (Isomorphic Representations Implies Same Characters). *If V and W are two representations of G, then V is isomorphic to $W \iff \chi_V = \chi_W$.*

Proof. The proof is by Maschke's Theorem. Let $V \simeq V_1^{m_1} \oplus \dots \oplus V_t^{m_t}$. Then we have that $\chi_V = m_1\chi_1 + m_2\chi_2 + \dots + \mu_t\chi_t$. We have that $\langle \chi_V, \chi_j \rangle = m_j \implies V$ is determined by χ_V. □

Consider $\chi_1, \dots, \chi_t$ an orthonormal system in $L^2_{class}(G) \subset L^2(G) \implies t \leq h(G)$. Our goal is to show that $t = h(G)$.

2.6 Regular Representation

Consider $V_{reg} = \mathbb{C}[G] = L^2(G)$ with left multiplication by G given by $(gf)(x) = f(g^{-1}x)$.
We have that $\chi_{V_{reg}}(g) = \begin{cases} \#G, & \text{if } g = id \\ 0, & \text{if } g \neq id \end{cases}$
$V_{reg} = V_1^{m_1} \oplus \dots \oplus V_t^{m_t}$. We now compute:

$$\begin{aligned} m_j &= \langle \chi_{V_{reg}}, \chi_j \rangle \\ &= \frac{1}{\#G} \sum_{g \in G} \overline{\chi_{V_{reg}}(g)} \chi_j(g) \\ &= \frac{1}{\#G} \#G \chi_j(id) \\ &= \dim(V_j) \end{aligned}$$

Corollary 2.47 (Irreducible reps). *Every irreducible representation occurs in V_{reg} with multiplicity equal to its dimension.*

Proof. $d_j = \dim_{\mathbb{C}}(V_j)$ and $V_{reg} = V_1^{d_1} \oplus \dots \oplus V_t^{d_t}$. Then taking $\dim_{\mathbb{C}}$ of both sides we get that $\#G = d_1^2 + d_2^2 + \dots + d_t^2$. □

Theorem 2.48 ($t = h(G)$). $t = h(G)$.

Proof. $\mathbb{C}[G] \simeq V_1^{d_1} \oplus \ldots \oplus V_t^{d_t}$. Key remark: $\mathbb{C}[G]$ is not just a G-representation but also a ring. We have that:

$$\left(\sum_{g\in G} \alpha_g \cdot g\right)\left(\sum_{h\in G} \beta_h \cdot h\right) = \sum_{g\in G}\left(\sum_{h_1,h_2} \alpha_{h_1}\beta_{h_2}\right) g$$

Let $p = (p_1, \ldots, p_t) : G \to Aut(V_1) \times \ldots \times Aut(V_t)$. Then $p : \mathbb{C}[G] \to End_{\mathbb{C}}(V_1) \oplus \ldots \oplus End_{\mathbb{C}}(V_t) \simeq M_{d_1}(\mathbb{C}) \oplus \ldots \oplus M_{d_t}(\mathbb{C})$. Observe that $\dim_{\mathbb{C}} \mathbb{C}[G] = \#G$. Then we have that $\dim(End_{\mathbb{C}}(V_1) \oplus \ldots \oplus End_{\mathbb{C}}(V_t)) = d_1^2 \oplus \ldots \oplus d_t^2$.
Claim: p is an injective ring homomorphism.

Proof. Let $\theta = \sum a_g \cdot g \in \ker(p)$ for $a_g \in \mathbb{C}[G]$. Then $p_h(\theta) = 0 \implies \theta$ act as 0 on V. This implies that θ acts as 0 on all irreducible representations $V_1, \ldots, V_t$. So θ acts as 0 on all representations. So θ acts as 0 on $\mathbb{C}[G]$. Thus we have that:

$$\theta(\sum_{g\in G} a_g \cdot g) = 0 \quad \forall \sum a_g \cdot g \in \mathbb{C}[G]$$

In particular, $\theta \cdot 1 = 0 \implies \theta = 0$. □

Now since $\dim(\mathbb{C}[G]) = \dim(End_{\mathbb{C}}(V_1) \oplus \ldots \oplus End_{\mathbb{C}}(V_t))$ we have that p is surjective.
Thus $p : \mathbb{C}[G] \simeq M_{d_1}(\mathbb{C}) \oplus \ldots \oplus M_{d_t}(\mathbb{C})$ as $\mathbb{C}$-algebras. Calculate the centers of these rings: $Z(\mathbb{C}[G]) = \{\sum \lambda_g \cdot g : (\sum \lambda_g \cdot g)\theta = \theta(\sum \lambda_g \cdot g) \text{ for all } \theta \in \mathbb{C}[G]\}$. Thus $\sum \lambda_g \cdot g \in Z(\mathbb{C}[G]) \iff h \cdot (\sum \lambda_g \cdot g) = (\sum \lambda_g \cdot g)h \quad \forall h \in G$. Then we have that: $(\sum \lambda_g \cdot hg) = (\sum \lambda_g \cdot gh) \quad \forall h \in G$. Thus $(\sum \lambda_g \cdot hgh^{-1}) = (\sum \lambda_g \cdot g)$. We also have that $(\sum \lambda_{h^{-1}gh} \cdot g) = (\sum \lambda_g \cdot g) \quad \forall h \in G$. So $\lambda_{h^{-1}gh} = \lambda_g$. This implies that $g \mapsto \lambda_g$ is a class function. So $\dim(Z(\mathbb{C}[G])) = h(G)$ and recall that $\dim(Z(End_{\mathbb{C}}(V_1) \oplus \ldots \oplus End_{\mathbb{C}}(V_t))) = t$. □

Some consequences of this include:

- Compare dimensions: $\#G = d_1^2 + \ldots d_t^2$.
- Comparing the dimensions of the centers

$$Z(\mathbb{C}[G]) = \{\sum_{g\in G} \lambda_g \cdot g : \lambda_g \text{ is a class function}\} = h(G) = \text{number of conjufacy classes}$$

$$Z(M_{d_1}(\mathbb{C}) \times \ldots \times M_{d_t}(\mathbb{C})) \simeq \underbrace{\mathbb{C} \oplus \mathbb{C} \oplus \ldots \mathbb{C}}_{t} = t$$

- $t = h(G)$

2.7 Abelian Groups

Let G be abelian. We have that $\dim(V_j) = 1$ for $j = 1, \ldots t \cdot h$ which has cardinality G. We can then conclude that the number of irreducible representations is equal to the cardinality of G.

Proposition 2.49 ($t = \#G$). *The number of irreducible representations $t = \#G$.*

Proof. We know that $G \simeq \mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_r\mathbb{Z}$ where $d_1 | \ldots | d_r$. If ρ is an irreducible representation of G then $\rho : G \to Aut(\mathbb{C}v) = \mathbb{C}^*$. G is generated by elements $g_1, \ldots, g_r$ with $g_1^{d_1} = \ldots = g_r^{d_r}$. Then we have that $G = \{g_1^{a_1} g_2^{a_2} \ldots g_r^{a_r} : 0 \leq a_1 \leq d_1 - 1, \ldots, 0 \leq a_r \leq d_r - 1\}$. So ρ is completely determined by the elements $\rho(g_1), \ldots, \rho(g_r)$. Thus $\rho(g_1^{a_1} \ldots g_r^{a_r}) = \rho(g_1)^{a_1} \ldots \rho(g_r)^{a_r}$. Then we have that $\mu_d = \{\zeta \in \mathbb{C}^* : \zeta^d = 1\}$. We then have that $Hom(G, \mathbb{C}^*) \simeq \mu_{d_1} \times \ldots \times \mu_{d_r}$. Then we have that $\rho \to (\rho(g_1), \ldots, \rho(g_r))$. We also have that $Hom(G, \mathbb{C}^*)$ is alos a group such that $\rho_1, \rho_2 \to \rho_1\rho_2(g) = \rho_1(g)\rho_2(g) \quad \forall g \in G$. Then $Hom(G, \mathbb{C}^*) = \mu_{d_1} \times \ldots \times \mu_{d_r}$ is an isomorphism of abelian groups. Let $\hat{G}$ = set of irreducible representations of G= set of irreducible characters of G. □

Remark 2.50. As a group, $\hat{G} \simeq G$ but this identification is not natural.

The key objective of Fourier Analysis: $L^2(G) = \{\text{square integrable functions from } G \to \mathbb{C}\}$. $f \in L^2(G) \iff ||f||^2 = \frac{1}{\#G}\sum_{g\in G}|f(g)|^2 < \infty$.

Note that $L^2(G)$ is a Hilbert space, with

$$\langle f_1, f_2\rangle = \frac{1}{\#G}\sum_{g\in G}\overline{f_1(g)}f_2(g)$$

Key Fact: The elements of $\hat{G}$ are an orthonormal basis of $L^2(G)$.

Suppose that $\#G = N$ and $\hat{G} = \{\chi_1, \ldots, \chi_N\}$. For given $f \in L^2(G)$, we write: $f =< \chi_1, f > \chi_1 + \ldots + < \chi_N, f > \chi_N$.

2.8 Fourier Analysis on Finite Abelian Groups

Given G an abelian group, we define $\hat{G} = \{\text{irreducible representations of } G\} = hom_{\text{group}}(G, \mathbb{C}_1^*)$. In general, for a non-abelian group they have no additional structure, but for abelian groups we can multiply two homomorphisms to get another. So $\hat{G}$ is a group, not just a set.

We want to analyze $f \in L^2(G)$ and we have an inner product on it defined by:

$$< f_1, f_2 >= \frac{1}{\#G}\sum_{g\in G}\overline{f_1(g)}f_2(g)$$

Definition 2.51 (Fourier Transform). Given $f \in L^2(G)$, the function $\hat{f} : \hat{G} \to \mathbb{C}$ defined by

$$\hat{f}(\chi) = \frac{1}{\#G}\sum_{g\in G}\overline{\chi(g)}f(g)$$

is called the Fourier Transform of G. Because $\hat{G}$ is an orthonormal basis of $L^2(G)$, we have that $f = \sum_{\chi\in\hat{G}}\hat{f}(\chi)\cdot\chi \quad$ in $L^2(G)$. We get the identity:

$$f(g) = \sum_{\chi\in\hat{G}} f\hat{(\chi)}\cdot\chi(g)$$

This is called the Fourier Inversion.

Example. This is a non-example (it is not finite). Let $G = \mathbb{R}/\mathbb{Z}$. $L^2(G)$ is the space of $\mathbb{C}$ valued, periodic functions on $\mathbb{R}$ which are square integrable on [0,1]. We also have that $f(x+1) = f(x)$. Then the inner product will look like:

$$< f_1, f_2 >= \int_{\mathbb{R}/\mathbb{Z}}\overline{f_1(x)}f_2(x)dx = \int_0^1\overline{f_1(x)}f_2(x)dx$$

In this case, $\hat{G} = Hom(G, \mathbb{C}^*)$ by $\mathbb{R} \to \mathbb{C}^*$ given by $x \mapsto e^{\lambda x}$ for λ satisfying $e^{\lambda n} = 1$ for all $n \in \mathbb{Z}$, so $\lambda = 2\pi ik$ for $k \in \mathbb{Z}$. Thus $\hat{G} = Hom(G, \mathbb{C}^*) = \{\chi_j : j \in \mathbb{Z}\}$ for $\chi_j(x) = e^{2\pi ijx}$. We have that $e^{2\pi ij} = 1$ for all j. Then we have that:

$$\chi_n : \mathbb{R}/\mathbb{Z} \to \mathbb{C}^*$$

Now if we consider:

$$< \chi_n, \chi_m >= \int_0^1 e^{-2\pi i(m-n)}dx = \int_0^1 cos(2\pi i(m-n)x) - isin(2pii(m-n)x) = \begin{cases} 0, & \text{if } m \neq n \\ 1, & \text{if } m = n \end{cases}$$

So we have that $\hat{f} : G = \mathbb{Z} \to \mathbb{C}$ where it is defined by

$$\hat{f}(n) = \hat{f}(\chi_n) = \int_0^1 e^{-2\pi inx}f(x)dx$$

Remark 2.52. For finite groups, $G \simeq \hat{G}$ when G is finite.

Remark 2.53. If G is finite, then $\hat{G}$ is an orthonormal basis of $L^2(G)$.

Question to think about: How does this extend to $G = \mathbb{R}/\mathbb{Z}$?

Formally, we want to relate

$$f \leftrightarrow \sum_{n=-\infty}^{\infty} \hat{f}(n)e^{2\pi inx} = \lim_{N\to\infty} \sum_{n=-N}^{N} \hat{f}(n)e^{2\pi inx}$$

Example. Let $G = \mathbb{Z}/N\mathbb{Z}$ be finite abelian (cyclic group of order N under addition). We can write $\hat{G} = \{\chi_0, \chi_1, \ldots, \chi_{N-1}\} \simeq \mathbb{Z}/N\mathbb{Z}$. We will define

$$\chi_j(k) = e^{2\pi ijk/N} \in M_1 \subset \mathbb{C}^*$$

We have that:

$$\begin{aligned} \chi_{j_1} \cdot \chi_{j_2} &= e^{2\pi j_1 k} \cdot e^{2\pi i j_2} \\ &= e^{2\pi i(j_1+j_2)} \\ &= \chi_{j_1 j_2}(k) \quad \forall k \end{aligned}$$

Now if we take $f \in L^2(G)$ we have that

$$\hat{f}(n) = \frac{1}{N}\sum_{k=0}^{N-1} e^{-2\pi ink/N} \cdot f(k)$$

And we should think of $\hat{f} \in L^2(\mathbb{Z}/N\mathbb{Z}) = L^2(\widehat{\mathbb{Z}/N\mathbb{Z}})$. So we have that:

$$f = \sum_{n=0}^{N-1} \hat{f}(n)\chi_n$$

We now want to think about the application of these ideas. Consider the harmonic series $1 + \frac{1}{2} + \frac{1}{3} + \ldots$. Now take the odd reciprocals: $1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \ldots$. We get that:

$$\sum_{n=0}^{\infty}(\frac{1}{4n+1} - \frac{1}{4n-3}) = \sum_{n=0}^{\infty}(\frac{2}{(4n+1)(4n-3)})$$

More general question to consider: Let $f \in L^2(\mathbb{Z}/N\mathbb{Z})$. We now want to study

$$S(f) = \sum_{n=1}^{\infty} \frac{f(n)}{n}$$

when this exists (theres no guarantee this limit converges).
Key remarks:

1. The function $f \mapsto S(f)$ is linear, so it is enough to understand $S(f)$ for a basis of $L^2(G)$ (if we can evaluate it on a basis, then we have evaluated it on a general function)

2. $S(\chi_j)$ can be evaluated in closed form. By definition,

$$\begin{aligned} S(\chi_j) &= \sum_{n=1}^{\infty} \frac{\chi_j(n)}{n} \\ &= \sum_{n=1}^{\infty} \frac{e^{2\pi ijn/N}}{n} \\ &= \sum_{n=1}^{\infty} \frac{x^n}{n} \quad x = e^{2\pi ij/N} \\ &= -\log(1-x) \quad x = e^{2\pi ij/N} \end{aligned}$$

If $j = 0$, i.e. $\chi_j = 1$, then $S(\chi_j) = \infty$ at $j = 0$. Then $S(\chi_j) = -\log(1 - e^{2\pi ij/N})$ so $S(f) = S(\hat{f}(0)\chi_0 + \ldots + \hat{f}(N-1)\chi_{N-1})$. if $\hat{f}(0) \neq 0$ then $S(f) = 0$. But if $\hat{f}(0) = 0$ we get that

$$\begin{aligned} S(f) &= S(\sum_{j=1}^{N-1} \hat{f}(j)\chi_j) \\ &= \sum_{j=1}^{N-1} \hat{j} S(\chi_j) \\ &= \sum_{j=1}^{N-1} \hat{f}(j)(-\log(1-x)) \end{aligned}$$

Example. Let $f \in L^2(\mathbb{Z}/4\mathbb{Z})$. Then we have that

$$f(n) = \begin{cases} 0, & \text{if } n \text{ is even} \\ 1, & \text{if } n = 1 + 4k \\ -1, & \text{if } n = 3 + 4k \end{cases}$$

where $f = \frac{1}{2i}(\chi_1 - \chi_3)$ and we get that

$$\begin{aligned} S(f) &= \frac{1}{2i}(S(\chi_1) - S(\chi_3)) \\ &= \frac{1}{2i}(-\log(1-i) + \log(1+i)) \\ &= \frac{1}{2i}(-\log(\sqrt{2}) + \frac{\pi i}{4} + \log(\sqrt{2}) + \frac{\pi i}{4}) \\ &= \frac{\pi}{4} \end{aligned}$$

With the identity that $e^{2\pi i/4} = i$.

We will now go over the character table of S_4: We have that $\#S_4 = 4! = 24$. We will compute the conjugacy classes.

Number	Shape	Name
1	1	1A
6	(12)	2B
3	(12)(34)	2A
8	(123)	3A
6	(1234)	4A
24		

So we have $h = 5$, we are looking for 5 distinct irreducible representations. We have that:

	1	3	6	8	6
	1A	2A	2B	3A	4A
χ_1	1	1	1	1	1
χ_2	1	1	-1	1	-1
χ_3	2	2	0	-1	0
χ_4	3	-1	1	0	-1
χ_5	3	-1	-1	0	1

We will now go over the character table for A_5. We have that $\#A_5 = 60$. Here is the conjugacy class table:

Number	Shape	Name
1	1	1A
15	(12)(34)	2A
20	(123)	3A
12	(12345)	5A
12	(21345)	5B
60		

So we have $h = 5$, we are looking for 5 distinct irreducible representations. We have that:

	1	15	20	12	12
	1A	2A	3A	5A	5B
χ_1	1	1	1	1	1
χ_2	4	0	1	-1	-1
χ_3	5	1	-1	0	0
χ_4	3	-1	0	$(\sqrt{5}+1)/2$	$(-\sqrt{5}+1)/2$
χ_5	3	-1	0	$(-\sqrt{5}+1)/2$	$(\sqrt{5}+1)/2$

If G is abelian, then $\mathbb{C}[G]$ is a commutative ring. As a ring, $\mathbb{C}[G] \simeq \oplus_{\chi\in\hat{G}}\mathbb{C}$ by

$$\sum_{g\in G}\lambda_g g \mapsto (\sum \lambda_g \cdot \chi(g))_{\chi\in\hat{G}}$$

Say we have that $\lambda \in \mathbb{C}^G$ such that $\lambda(g) = \lambda_g$. Then we have that $\sum_{g\in G}\lambda_g\chi(g) = \#G\cdot\langle\overline{\chi},\lambda\rangle = \#G\cdot\hat{\lambda}(\overline{\chi})$. Recall the Fundamental Isomorphism of rings: Let G be a general finite group. with $V_1,\ldots,V_h$ be the irreducible representations of G. We showed that

$$\Phi : \mathbb{C}[G] \simeq \oplus_{j=1}^{h} End_{\mathbb{C}}(V_j) \simeq \oplus_{j=1}^{h} M_{d_j}(\mathbb{C})$$

where d_j is the dimension of the j-th irreducible representation. Recall that $\rho_j : G \to Aut_{\mathbb{C}}(V_j)$. Then

$$\Phi(\sum_{g\in G}\lambda_g\cdot g) = (\sum \lambda_g\rho_1(g),\ldots,\sum\lambda_g\rho_h(g))$$

Definition 2.54 (Fourier Transform). If $f : G \to \mathbb{C}$ is a complex-valued function and $\theta_f = \sum_{g\in G} f(g)\cdot g$ is the corresponding element in the group ring $\mathbb{C}[G]$. Then its image in $\oplus End_{\mathbb{C}}(V_j)$ is called the Fourier Transform of f. That is, we can write:

$$\hat{f} = (T_1, T_2, \ldots T_h)$$

for $T_i \in End_{\mathbb{C}}(V_i)$. (We normally think of them as a collection of matrices of different sizes).

An application of Fourier Transforms is random products in groups: When you have a finite group, you can define a probability measure.

Definition 2.55 (Probability Measure). A probability measure/distribution on G is a function $\mu : G \to \mathbb{R}^{\geq 0}$ such that $\sum_{g\in G} \mu(g) = 1$. We can think of $\mu \in \mathbb{R}^{\geq 0}$ or $\mu \in \mathbb{R}[G]$. The advantage of thinking of $\mu \in \mathbb{R}[G]$ is that it has a product in the group ring.

The product in $\mathbb{R}[G]$ corresponds to a natural product on the space of functions called the convolution of $\mathbb{R}^G$. This convolution uses the group's structure (underlying product).

Definition 2.56 (Convolution). Given μ_1, μ_2, the convolution is given by:

$$\mu_1 \star \mu_2 = \sum_{(g_1 g_2)\in G\times G; g=g_1g_2} \mu_1(g_1) \cdot \mu_2(g_2)$$

From a probability point of view, this is the probability of finding the probability of picking g_1 at random in μ_1 and picking g_2 in μ_2. This space of probability measures is closed under convolution. In particular, $\mu\star\mu(g)$ is the probability of obtaining g as a product g_1g_2 where g_1 and g_2 are picked at random according to the probability measure μ.
Question: What is the limit as $n \to \infty$ of $\mu^{\star}N$? Does it exist?

Definition 2.57 (Support). The support of μ is $supp(\mu) = \{g \in G : \mu(g) \neq 0\}$.
We can consider G_μ =subgroup of G generated by element in the support. We also have G_μ^+ = subgroup of G generated by $\{g^{-1}h : g, h \in supp(\mu)\}$. Note that $G_\mu^+ \subseteq G_\mu \subseteq G$.

Example. Take $G = S_n$. And $\mu = \frac{2}{n(n-1)} \sum_{i<j}(ij)$. Then $supp(\mu) = \{(ij)\}$ So $G_\mu = S_n$ but $G_\mu^+ = A_n$.

Let $\mu_{unif} : G \to \mathbb{C}$ where $\mu_{unif}(g) = \frac{1}{\#G} \quad \forall g \in G \leftrightarrow \frac{1}{\#G}\sum_{g\in G} g$.

Theorem 2.58 (Important Probability Result). *If $G_\mu^+ = G$ then $\lim_{n\to\infty} \mu^{\star n}$ exists and is equal to μ_{unif}.*

Proof. Let $T_1, \ldots T_h$ be the Fourier Transforms of $FT\mu = FT(\theta_\mu)$ where $\theta_\mu = \sum_{g\in G} \mu(g) \cdot g$. We have that $T_j \in End_{\mathbb{C}}(V_j)$. We assume that $V_1 = \mathbb{C}$ with the trivial action. Recall that each representation V_j is equipped with a G invariant Hermition inner product.

Lemma 2.59 (Contracting Operators). *(a) T_j is a contracting operator. Claim: when you apply T_j to a vector, you contract its length. That is,*

$$||T_j(v)|| \leq ||v|| \quad \forall v \in V_j$$

(b) T_j is strictly contracting. That is,

$$||T_j(v)|| < ||v|| \quad \forall v \neq 0 \in V_j$$

and $j \geq 2$.

Proof. This is a standard application of the triangle inequality.

(a) $||T_j(v)|| = ||\sum_{g\in G} \mu(g)\rho_j(g)(v)|| \leq \sum_{g\in G} |\mu(g)|||\rho_j(g)(v)|| = \sum_{g\in G} \mu(g)||v|| = ||v||$

(b) In the triangle inequality, equality occurs if and only if all the vectors involved in the sum point in the same direction. That is, if and only if $\rho_j(g)(v)$ for $g \in supp(\mu)$ are equal. Thus we find that $||T_j(v)|| = ||v||$ then $\rho_j(g)v = \rho_j(h)v \quad \forall g, h \in supp(\mu)$. This tells us that $\rho_j(h^{-1}g)v = v \quad \forall g, h \in supp(\mu)$. So we find that $\rho_j(g)v = v$ for all $g \in G_\mu^+ = G$ by assumption. This means that $v \in V_j^G$. This implies that if $j \geq 2$, $v = 0$.

□

Note that $T_1 = \sum \mu(g)\rho_1(g) = \sum \mu(g) = 1$ since ρ_1 is the identity matrix. But we have that $T_2, \dots, T_h$ are strictly contracting. From this, we find that

$$\Theta = \lim_{N \to 0} \theta_\mu^N \in \mathbb{C}[G] = \lim(T_1^n, \dots, T_h^n) = (1, 0, \dots, 0)$$

We find that this is $FT(\theta_{\mu_{unif}}) = FT(\frac{1}{\#G} \sum_{g \in G} g)$. □

We are considering the group $G = GL_3(\mathbb{F}_2)$ and we know that $\#G = 168 = 2^3 \cdot 3 \cdot 7$. Let us go over the character table for G:

	1	21	56	42	24	24
	1A	2A	3A	4A	7A	7B
χ_1	1	1	1	1	1	1
χ_2	6	2	0	0	-1	-1
χ_3	7	-1	1	-1	0	0
χ_4	8	0	-1	0	1	1
χ_5	3					
χ_6	3					

We also have that

$$\mathbb{C}[V^*] = \left\{ \sum_{w \in V^*} \lambda_v[w] | \lambda_w \in \mathbb{C} \right\}$$

This action is given by for all $g \in G$, $g(\sum_{w \in V^*} \lambda_w[w]) := \sum_{w \in V^*} \lambda_w[gw]$. So we have that $dim_{\mathbb{C}}(\mathbb{C}[V^*]) = 7$.
So we have that $\chi_{\mathbb{C}[V^*]}(g) =$ number of fixed points of g acting on V^*.
Let $H = N_G(O_7)$ where H is the normalized sylow-7 subgroup for $GL_3(\mathbb{F}_2)$.
We will now motivate induced representations. Let us first revisit permutation representations.
We have that $V = \{f : G/H \to \mathbb{C}\}$ by $g \cdot f(x) = f(g^{-1}(x))$. We can actually rewrite this by $\{f : G \to \mathbb{C}\}$ by $f(xh) = f(x) \quad \forall h \in H$.
Consider $H \subset G$ and let $\chi \in Hom(H, \mathbb{C}^*)$. Now consider the set

$$V_\chi = \{f : G \to \mathbb{C} | f(xh) = \chi(h) \cdot f(x) \quad \forall h \in H\}$$

Key facts about V_χ:

1. G acts linearly on V_χ by the rule

$$gf(x) = f(g^{-1}x) \quad \forall x \in G$$

Proof. We need to verify if $f \in V_\chi$ then $gf \in V_\chi$. We take:

$$\begin{aligned} gf(hx) &= f(g^{-1}(xh)) \\ &= f(g^{-1}x \cdot h) \\ &= \chi(h)f(g^{-1}x) \\ &= \chi(h)(gf)(x) \quad \forall x \in G, h \in H \end{aligned}$$

Thus $gf \in V_\chi$. □

2. $dim(V_\chi) = [G : H]$. We now show this: Let $a_1, \dots, a_t$ be a set of coset representatives. That is,

   $$G = a_1H \sqcup a_2H \sqcup \dots \sqcup a_tH$$

   We claim that the function $f \mapsto (f(a_1), f(a_2), \dots, f(a_t)) \in \mathbb{C}^t$ is an isomorphism of $\mathbb{C}$ vector spaces from V_χ to $\mathbb{C}^t$. This is injective by computing the kernel. Suppose that $f(a_1) = \dots = f(a_t) = 0$ is in the kernal. Then since $f \in V_\chi$, we have that $f(a_jh) = \chi(h)f(a_j) = 0$. Therefore, we have that $f \equiv 0$ since every element in g can be written as $f(a_jh)$. For surjectivity: Given a collection $\lambda_1, \dots, \lambda_t \in \mathbb{C}^t$, we define a function:

   $$f(a_jh) = \chi(h)\lambda_j$$

   This gives us the preimage recipe.

The representation V_χ is called the induced representation of χ from h to G. We call V_χ the induced representation and denote it by $ind_H^G\chi$. The dimension of this induced representation is equal to $[G : H]$.

Remark 2.60. If H is a quotient of G, then any representation of H gives a representation of G by composing the natural homomorphism of H to the representation of H.
If H is a subgroup of G then any character of H gives a representation of G.

Given a homomorphism $\psi : H \to \mathbb{C}^*$ and V_ψ be an induced representation of G. What is χ_{V_ψ}?
As a basis for V_ψ, we consider for each $a \in G$, we construct $f_a \in V_\psi$ such that $f_a : G \to \mathbb{C}$ by $f_a(ah) = \psi(h)$ and $f_a(g) = 0$ if $g \notin aH$.
If $a_1, \dots, a_t$ are coset representatives for $H \subset G$ then $f(a_1), \dots, f(a_t)$ is a basis for V_ψ.
Given $g \in G$, what is the matrix of g in the basis $f(a_1), \dots, f(a_t)$?
We will see what g does to the function:

$$\begin{aligned} g \cdot f_{a_j}(x) &= f_{a_j}(g^{-1}x) \\ &= f_{ga_j}(x) \end{aligned}$$

We also have that

$$g \cdot f_{a_j}(ga_j) = f_{a_j}(g^{-1}ga_j) = f_{a_j}(a_j) = 1$$

If $a_1, \dots, a_t$ are coset representations, then $ga_jH = a_iH$ and $ga_j = a_ih_{ij}$ for some $h_{ij} \in H$. Then we have that

$$gf_{a_j} = f_{a_ih_{ij}} = \psi(h_{ij})f_{a_i}$$

Thus we have that:

$$\chi_{V_\psi}(g) = \sum_i \psi(h_i) = \sum_{i=1}^t \tilde{\psi}(a_i^{-1}ga_i)$$

where $\tilde{\psi}(x) = 0$ when $x \notin H$ and $h_i = a_i^{-1}ga_i$.
The final formula we have for the character of the induced representation is:

Theorem 2.61 (Character of Induced Rep Formula). $\chi_{\overline{V}_\psi}(g) = \sum_{aH \in G/H; a^{-1}ga \in H} \tilde{\psi}(a^{-1}ga)$ *where* $\tilde{\psi} : G \to \mathbb{C}$ *is the function on* G *defined by:*

$$\psi(g) = \begin{cases} 0, & \textit{if } g \notin H \\ \psi(g), & \textit{if } g \in H \end{cases}$$

Proof. Introduce a basis for V_ψ. For $a \in G$, let δ_a be the unique function in V_ψ satisfying

$$\delta_a(a) = \begin{cases} \delta_a(a) = 1 \\ \delta_a(x) = 0, & \text{not on } H \end{cases}$$

The functions $\delta_{a_1}, \dots, \delta_{a_t}$ are a basis for the representation V_ψ and are linearly independent because they have disjoint supports.
Properties of δ_a:

- $g\delta_a = \delta_{ga}$
- $\delta_{ah} = \psi(h)\delta_a$

We have that

$$g\delta_{a_j} = \delta_{ga_j} = \psi(h_j)\delta_{a'_j}$$

So we have that $g\delta_{a_j} = \psi(h_j)\delta_{a'_j}$ for $ga_j = a_{j'}h_j$.
We have that

$$\chi_{V_\psi}(g) = \sum_{j=j'} \psi(h_j) = \sum_{j'=j} \psi(a_j^{-1}ga_j) = \sum_{a\in G/H; gaH=aH} \psi(a^{-1ga})$$

Finally, this is equivalent to:

$$\chi_{\overline{V}_\psi}(g) = \sum_{aH\in G/H; a^{-1}ga\in H} \psi(a^{-1}ga)$$

□

Remark 2.62. $\psi(a^{-1}ga)$ depends only on the cosets aH not on a. If $a' = ah$ for $h \in H$. Then

$$(a')^{-1}ga' = h^{-1}(a^{-1}ga)h$$

Taking this over ψ, we get:

$$\psi((a')^{-1}ga') = \psi(h^{-1}(a^{-1}ga)h) = \psi(a^{-1}ga)$$

Theorem 2.63 (Irreducible Reps)**.**

$$\chi_{V_\psi(g)} = \frac{\#G}{\#H} \times \frac{1}{\#C(g)} \sum_{\gamma\in C(g)\cap H} \psi(\gamma)$$

Proof. We begin with

$$\begin{aligned}
\chi_{\overline{V}_\psi}(g) &= \sum_{aH\in G/H; a^{-1}ga\in H} \psi(a^{-1}ga) \\
&= \frac{1}{\#H} \sum_{a\in G; a^{-1ga\in H}} \psi(a^{-1}ga) \\
&= \frac{\#Z(g)}{\#H} \sum_{a\in Z(g\backslash G)} \tilde{\psi}(a^{-1}ga) \\
&= \frac{\#G}{\#H} \frac{1}{\#C(g)} \sum_{\gamma\in C(g)\cap H} \psi(\gamma)
\end{aligned}$$

with stabilizer $Z(g) = \{\alpha \in G : \alpha g = g\alpha\} \subseteq G$ of g under conjugation. By the Orbit Stabilizer Theorem, $\#Z(g) \times \#C(g) = \#G$. And $\tilde{\psi} = \psi(g)$ if $g \in H$ and 0 otherwise. □

2.9 Motivation

Let X be a mathematical object. G be a group of symmetrics (i.e. $G = Aut(X)$). And $V = L^2(X)$ be $\mathbb{C}$-valued functions on X. Our basic assumptions:

- X is finite
- G is finite
- V is finite dimensional

Let $T : L^2(X) \to L^2(X)$ such that T is defined in a natural way from the structure on X.

Example. X is a G-set. X is a set of vertices, edges, or faces of a regular sided object. X is a graph. We have that since $L^2(X) = \mathbb{C}$-valued functions on a graph, then $\rho : L^2(X) \to L^2(X)$ is given by

$$(T\rho)(x) = \sum_{y \text{ adj to } x} \rho(y)$$

Claim: T commutes with all actions of G. $T \circ g = g \circ T$ for all $g \in G$.

Proof. $(T \circ g)(\rho) - T(g\rho)$ in $L^2(X)$ for all $\rho \in L^2(X)$. Then $\forall x \in X$:

$$\begin{aligned}(T \circ g)(\rho)(x) &= T(g\rho)(x) \\ &= \sum_{y \sim x} (g\rho)(y) \\ &= \sum_{y \sim x} \rho(g^{-1}y) \\ &= \sum_{g^{-1}y \sim g^{-1}x} \rho(g^{-1}y) \\ &= \sum_{y \sim g^{-1}x} \rho(y)\end{aligned}$$

Then we must have that:

$$((g \circ T)\rho)(x) = g(T(\rho))(x) = T(\rho)(g^{-1}x) = \sum_{g \sim g^{-1}x} \rho(y)$$

□

Example. Let X be the factors of a cube, and $V = L^2(X)$. Then $T\rho(F) = \frac{1}{4}(\sum_{F' \text{ adj}} \rho(F'))$

Problem: What is the spectrum of T?

Theorem 2.64 (L^2)**.** *If $L^2(X) = V_1 \oplus \ldots \oplus V_t$ where V_j's are distinct irreducible representations of G, then T maps V_j to itself. Moreover, T acts as a scalar on V_j.*

Proof. T can be represented by a $t \times t$ matrix (T_{ij}) such that $T_{ij} : V_j \to V_i$. Now for $v \in V_1 \oplus \ldots \oplus V_t$, and setting $V = (V_1 \ldots V_t)^T$, we have that:

$$(T_{ij})(V_1 \ldots V_t)^T = \begin{pmatrix} T_{11}(v_1) & + \ldots & + T_{1t}(V_t) \\ & \vdots & \\ T_{t1}(V_1) & + \ldots & + T_{tt}(V_t) \end{pmatrix}$$

for each $T_{ij} \in Hom_G(V_j, V_i)$. By Shur's Lemma, $Hom_G = 0$ for $i \neq j$ and its equal to $\mathbb{C}$ otherwise. This implies that our matrix only has diagonal entries, with all others zero. So set $T_{ii} = \lambda_i \in \mathbb{C}$. Since $Tg = gT$, we have that $(T_{ij})g = g(T_{ij})$. □

We have the general principle: If V is a representation of G, and $T : V \to V$ for $T \in End_G(V)$ then we have that $T(gv) = gT(v)$ for all $v \in V, g \in G$. Then if $V = V_1 \oplus \ldots \oplus V_T$ where the V_j are irreducible representations and non-isomorphic, then $T(V_j) \subseteq V_j$ and $T(v) = \lambda_j v$ for all $v \in V_j$.

If we consider $\eta_j \in Hom_G(V - j, V)$ and take $\pi_i \in Hom_G(V, V_i)$, then we have that for $v = v_1 + \ldots + v_t$,

$$gv = gv_1 + \ldots + gv_t$$

and so

$$g\pi_i(v) = gv_i \quad \text{and} \quad \pi_i g(v) = gv_i$$

And last class we considered:

$$T \in Hom_G(V,V) = (T_ij) = \pi_i T \eta_j \in Hom_G(V_j, V_i)$$

and then by Schur's Lemma we know that: $T_ij = 0$ for $i \neq j$ and λ_i along the diagonal. Now, we claim that if $v \in V_j$ then $T(v) \in V_j$. This is because:

$$\begin{aligned} T(v) &= \pi_1 T(v) + \ldots + \pi_t T(v) \\ &= T_{1j}(v) + T_{2j}(v) + \ldots + T_{tj}(v) \\ &= T_{jj}(v) \\ &= \lambda_j v \end{aligned}$$

Remark 2.65. Whenever $T : V \to V$ is a linear transformation and $V = V_1 \oplus \ldots \oplus V_t$, then we have that:

$$v = (v_1 \ldots v_t)^T$$

for $v_j \in V_j$ which means that $v = v_1 + \ldots + v_t$. In this notation, an application of T becomes mutliplication by a square matrix whose entries consist of homomorphisms of the V_j's. We have that

$$T(v) = \begin{pmatrix} T_{11} & T_{12} & \ldots & T_{1t} \\ T_{21} & T_{22} & \ldots & T_{2t} \\ \vdots & & & \vdots \\ T_{t1} & T_{t2} & \ldots & T_{tt} \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_t \end{pmatrix}$$

So then $T_{ij} \in Hom(V_j, V_i)$.

Example. Let X =set of faces of the cube. Let $V = L^2(X) \leftarrow G = S_4$ (G acts linearly on V). Define $T : V \to V$ by

$$T(\psi)(x) = \frac{1}{4} \sum_{y \sim x} \psi(y)$$

for $y \sim x$ meaning that y is the face adjacent to x.
Question: How to decompose $L^2(X)$ into a sum of irreducible representations of S_4?

	1 1A	6 2A	3 2B	8 3A	6 4A
χ_1	1	1	1	1	1
χ_1	1	-1	1	1	-1
χ_3	2	0	2	-1	0
χ_4	3	1	-1	0	-1
χ_5	3	-1	-1	0	1
$L^2(X)$	6	0	2	0	2

We can write $L^2(X) = \chi_1 \oplus \chi_3 \oplus \chi_5$. This is equal to the constant functions $\oplus L^2(X)_{+,0} \oplus L^2(X)_-$.

Definition 2.66 (even). $\rho : X \to \mathbb{C}$ is even if $\rho(x) = \rho(x')$ where x' =face opposite to x. So $L^2(X)_+$ = space of even functions. Thus for $\rho \in L^2(X)_+$, g preserves $L^2(X)_+$.

Definition 2.67 (odd). $L_2(X)_-$ =space of odd functions $= \{\rho : X \to \mathbb{C} | \rho(x') = -\rho(x)\}$.

Consider the space $L^2(X)_{+,0} = \{\rho : X \to \mathbb{C} | \rho \text{ is even and } \sum_{x \in X} \rho(x) = 0\}$.
T preserves V_1, V_3, V_5:

- $T(\mathbb{1}_x) = \mathbb{1}_x$ so eigenvalue of 1 with multiplicity 1
- For $\rho \in V_5$, $T(\rho) = 0$ so eigenvalue of 0 with multiplicity 3
- For $\rho \in V_3$, and x the top face, $T(\rho)(x) = \frac{1}{2}(a + c) = -\frac{1}{2}b = -\frac{1}{2}\rho(x)$ so eigenvalue of $-1/2$ with multiplicity 2

3 Galois Theory

Galois Theory is the study of fields via their symmetries. Note that all of the fields are commutative unless stated otherwise.

Definition 3.1 (Extension)*.* If E and F are fields, we say that E is an extension of F if F is a subfield of E.

IF E is an extension of F, then its also a vector space over F. When you have a vector space over a field we have a size of the object.

Definition 3.2 (Degree)*.* We define the degree of E over F as the dimension of the field viewed as an F-vector space. Notation: $[E : F] = dim_F E \in \mathbb{N} \cup \{\infty\}$. E/F is a finite extension if the degree $[E : F] < \infty$.

Example. Let $E = \mathbb{C}$ and $F = \mathbb{R}$. Then $[E : F] = 2$. Basis (1,i).

Example. $E = \mathbb{C}$ and $F = \mathbb{Q}$. Then $[E : F] = \infty$.

Example. Let $E = F[x]/(p(x))$ where $p(x)$ is an irreducible polynomial of dimension n. Then $E = \{f(x) + (p(x))\} = \{a_0 + a_1x + \ldots + a_{n-1}x^{n-1} : a_i \in F\} \supset \{a_0 : a_0 \in F\}$. This is also closed under both multiplication and addition. So E is an extension of the field F. $[E : F] = n = deg(p(x))$.

Example. Take $E = F(x) = \{\frac{f(x)}{g(x)} : f, g \in F[x], g(x) \neq 0\}$=fraction field of the polynomial ring $F[x]$. E is an extension of F. $[E : F] = \infty$.

Theorem 3.3 (Multiplicativity of the Degree)**.** *Given $K \subset F \subset E$ all finite extensions and commutative fields. Then we have that*

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

Proof. Denote $[E : F] = n$ and $[F : K] = m$. Let $\alpha_1, \ldots, \alpha_n$ be a basis for E as an F-vector space. Let $\beta_1, \ldots, \beta_m$ be a basis for F as a K-vector space. If we have an element $a \in E$, then the fact that $\alpha_1, \ldots, \alpha_n$ is a basis for E as a vector space means that $a = \lambda_1\alpha_1 + \ldots + \lambda_n\alpha_n$ uniquely with scalars $\lambda_i \in F$. Since λ_i are in F, we can write each of these as a combination of the β_i. That is, each $\lambda_i = \lambda_{i1}\beta_1 + \ldots + \lambda_{im}\beta_m$ where each $\lambda_{ij} \in K$ for $i = 1, \ldots, n$ and $j = 1, \ldots, m$. Finally, we can write any element $a \in E$ as

$$a = (\lambda_{11}\beta_1 + \lambda_{12}\beta_2 + \ldots + \lambda_{1m}\beta_m)\alpha_1 + \ldots + (\lambda_{n1}\beta_1 + \ldots + \lambda_{nm}\beta_m)\alpha_n$$

That is,

$$a = \sum_{i=1}^{n}\sum_{j=1}^{m} \lambda_{ij}\alpha_i\beta_j$$

So $\{\alpha_i\beta_j\}$ forms a K-basis for E. Hence $dim_K(E) = nm$. □

Ruler and compass constructions:

Definition 3.4 (Ruler and compass construction)*.* A complex number is constructible by ruler and compass if it can be obtained by rational numbers by successive applications of field operations plus extraction of square roots.

The set of elements which are constructible by ruler and compass is an extension of the rationals of infinite degree.
Lore Drop: It was called constructible by ruler and compass because they were interested in ancient greece in making numbers using only rulers and compasses.
Question: To characterize the set of numbers which are constructible by the ruler and compass.

Theorem 3.5 (Not Constructible)**.** *If $\alpha \in \mathbb{R}$ satisfies an irreducible cubic polynomial over $\mathbb{Q}$ then α is not constructible by ruler and compass.*

Proof. Suppose toward a contradiction that α is constructible by ruler and compass. Then α belongs to a field which is obtained by a finite sequence of adjunctions of square roots. That is, $\exists \mathbb{Q} \subset F_1 \subset \ldots \subset F_n$ fields with the $[F_{i+1} : F_i] = [F_i : \mathbb{Q}] = 2$. This means that

$$F_{i+1} = F_i(\sqrt{a}) = \{a + b\sqrt{a_i} : a, b \in F\}$$

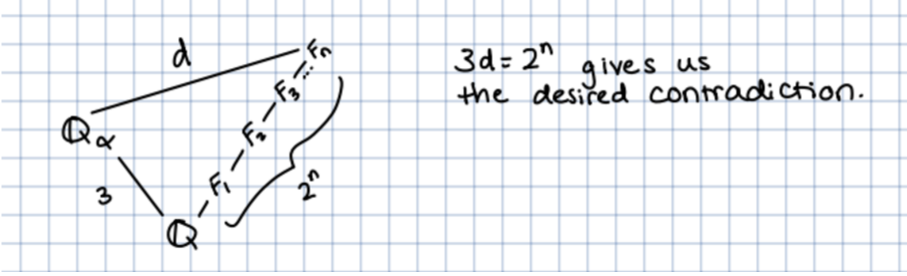
But $[F_n : \mathbb{Q}] = 2^n$. Note that $\mathbb{Q}[\alpha] = \mathbb{Q}(\alpha) = \mathbb{Q}[x]/p(x)$ where $p(x)$ is the minimal polynomial of α with degree 3. We can see this by taking

$$ev_\alpha : \mathbb{Q}[x] \to \mathbb{Q}(\alpha) \quad \text{by} f(x) \mapsto f(\alpha)$$

Then ker(ev_α)=(p(x)). So then

$$\overline{ev_\alpha} : \mathbb{Q}[x]/(p(x)) \to \mathbb{Q}(\alpha)$$

Note that this quotient $\mathbb{Q}[x]/(p(x))$ is a field. So this is an isomorphism. On the otherhand, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}[x]/(p(x)) : \mathbb{Q}] = 3$ given by basis $(1, x, x^2)$. Now we can draw a field diagram which gives us our contradiction.



□

Example. Let $p(x) = x^3 - 2$ and $\alpha = 2^{3/2}$. This is called duplicating the cube. It cannot be achieved by a ruler and compass construction.

Example. $p(x) = x^3 - 3x + 1/2 = 0$. This is irreducible. So a root of it is not constructible by ruler and compass. $r = \cos(2\pi/9)$ is a root of it, which comes from the fact that $\cos(3\theta) = \cos(\theta)^3 - 3\cos(\theta)\sin(\theta)^2$.

Definition 3.6 (Constructible). $\alpha \in \mathbb{R}$ is constructible if $\exists \mathbb{Q} \subset F_1 \subset \ldots \subset F_n$ such that $[F_{i+1} : F] = 2$ with $\alpha \in F_n$.

If α satisfies an irreducible cubic equation over F, then α is not constructible.

- Duplicating cube $2^{1/3}$ is not constructible
- Trisection of an angle is not constructible
- $\cos \frac{2\pi}{9}$ is not constructible

Definition 3.7 (Algebraic). Let E/F be finite extensions. An element $\alpha \in E$ is algebraic over F if α is the root of a polynomial in $F[x]$.

- $\sqrt{2}$ is algebraic over $\mathbb{Q}$
- 2 is algebraic over $\mathbb{R}$ or $\mathbb{Q}$
- π is not algebraic over $\mathbb{Q}$, but it is algebraic over $\mathbb{Q}(\pi^2)$

Remark 3.8. The set of $\alpha \in \mathbb{R}$ which are algebraic over $\mathbb{Q}$ is countable.

Lemma 3.9 (Finite extensions produce algebraic)**.** *If E/F is finite then every $\alpha \in R$ is algebraic over F.*

Proof. Take $a_0 + a_1\alpha + \ldots + \alpha_n\alpha^n$. Then we have that for each $1, \alpha, \ldots, \alpha^n$ such that $n = [E : F]$ cannot be linearly independent. □

Definition 3.10 (Automorphism Group). The automorphism group E/F is

$$Aut(E/F) = \{\sigma : E \to E | \sigma(x+y) = \sigma(x) + \sigma(y); \sigma(xy) = \sigma(x)\sigma(y); \sigma|_F = Id\}$$

Consequences: If $\sigma \in Aut(E/F)$ then

- $\sigma(1) = 1$
- $\sigma(0) = 0$
- $\sigma(\alpha^{-1}) = \sigma(\alpha)^{-1}$

Proposition 3.11 (Acting on Finite Orbits)**.** *If $[E : F]$ is finite then $G = Aut(E/F)$ acts on E with finite orbits.*

Proof. Let $\alpha \in E$. Since α is algebraic, there is a polynomial $a_nx^n + \ldots + a_1x + a_0$ such that $a_i \in F$ are satisfied by α, so

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

Let $\sigma \in Aut(E/F)$. Then we have that:

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

$$\implies \sigma(a_n\alpha^n) + \ldots + \sigma(a_1\alpha) + \sigma(a_0) = 0$$

$$\implies a_n\sigma(\alpha^n) + \ldots + a_1\sigma(\alpha) + a_0 = 0$$

If α is a root of $f(x) \in F[x]$, then $\sigma(\alpha)$ is a root of $f(x)$. So we have that

$$Orbit_G \subset \{\text{roots of } f(x) \in E\}$$

□

Remark 3.12. If E/F is an algebraic extension, then $Aut(E/F)$ acts with finite orbits.

Theorem 3.13 (Finite implies Finite)**.** *If $[E : F] < \infty$ then $\#Aut(E/F) < \infty$*

Proof. Let $\alpha_1, \ldots, \alpha_n$ be generators for E over F. Then $E = F(\alpha_1, \ldots, \alpha_n)$. Key Remark: If $\sigma \in Aut(E/F)$ then σ is completely determined by $(\sigma(\alpha_1), \ldots, \sigma(\alpha_n)) \subset Orbit_G(\alpha_1) \times \ldots \times Orbits_G(\alpha(n))$. □

Example. Suppose that E is generated over F by a single element α such that $E = F(\alpha)$. Let $p(x) \in F[x]$ be the minimal polynomial of α. Consider the evaluation map:

$$ev_\alpha = F[x] \to F[\alpha] \quad \text{by } x \mapsto \alpha \implies f(x) \mapsto f(\alpha)$$

We have that $\ker(ev_\alpha) = (p(x))$.

$$\overline{ev_\alpha} : F[x]/(p(x)) \xrightarrow{injection} F[\alpha]$$

$F[x]/(p(x))$ is an integral domain, hence a field. So $F[\alpha] = F(\alpha)$. Then $[F(\alpha) : F] = deg(p(x))$. $\sigma \in Aut(E/F)$ is determined.

$$\sigma\alpha \in \{\text{roots of } p(x)\}$$

This implies that $\#\{\text{roots of } p(x)\} < deg(p(x)) = [F(\alpha : F)]$. If E is generated by a single element over F, then

$$\#Aut(E/F) \leq [E : F]$$

We previously defined $Aut(E/F)$ = field automorphisms which fix F pointwise.
An automorphism is a bijection $E \to E$ which is a homomorphism of rings. Thus it is automatically injective as its a homomorphism of rings.
Any homomorphism $\phi : E \to E$ is automatically injective.
If $[E : F] < \infty$, then ϕ being injective automatically implies that ϕ is surjective.

Remark 3.14. Find an example of a field E and a homomorphism $\phi : E \to E$ which is not surjective.

We saw that $\#Aut(E/F)$ is a finite group. We also saw that if $E = F(\alpha)$, then $\#Aut(E/F) \leq [E : F]$.

Theorem 3.15 (Cardinality of Auts at least size of extensions)**.** *If E/F is any finite extension of fields then $\#Aut(E/F) \leq [E : F]$.*

Proof. A natural strategy is to do induction on the generators of E/F. So we will do induction on the number of generators for E over F. Namely, $E = F(\alpha_1, \dots, \alpha_n)$. Note that (for the homomorphisms in the category of fields)

$$Aut(E/F) = Hom_F(E, E)$$

Let M be any arbitrary extension of F (possibly infinite) which is fixed. We will consider:

$$Hom_F(E, M)$$

Claim: $\#Hom_F(E, M) \leq [E : F]$. This is a more general statement than what we originally want to prove. We will prove this claim by induction on the number of generators of M.

Base case ($n = 1$): This is essentially what we proved last class, but we will go over it again. We have that $E = F(\alpha) = F[\alpha]$. Thus for $p_\alpha(x) \in F[x]$ the minimal polynomial of F satisfied by α, we have that $[E : F] = deg(p_\alpha(x))$. Let d denote the degree of $p_\alpha(x)$. By considering $Hom_F(E, M)$ we can write any element as

$$\phi(a_0 + \ldots + a_{d-1}\alpha^{d-1}) = a_0 + \ldots + a_{d-1}\phi(\alpha)^{d-1}$$

Then we see that the map $\phi \mapsto \phi(\alpha)$ is an inclusion from $Hom_F(E, M)$ into the collection of all the roots of $p_\alpha(x)$ in M.

Inductive Step ($n \implies n + 1$): We write $E = F(\alpha_1, \dots, \alpha_{n+1})$. Let $F' = F(\alpha_1, \dots, \alpha_n)$. If $F' = E$ then we are done with the argument. So we can write $E = F'(\alpha_n)$. Let $g(x) \in F'[x]$ be the minimal polynomial of α_{n+1} with $deg(g(x)) = d_2$. We consider the restriction map

$$Hom_F(E, M) \to Hom_F(F', M)$$

Then $\#Hom_F(F', M) \leq d_1 = [F' : F]$ by the induction hypothesis. Given $\phi_0 \in Hom_F(F', M)$, how many $\phi : E \to M$ are there which satisfy the condition such that

$$\phi|_{F'} = \phi_0$$

We know that α_{n+1} is the root of $g(x) = \lambda_{d_2}x^{d_2} + \ldots + \lambda_1 x + \lambda_0$ where $\lambda_i \in F'$. Then $\phi(\alpha_{n+1})$ is a root of

$$\phi(\lambda_{d_2}x^{d_2} + \ldots + \lambda_1 x + \lambda_0) = \phi(\lambda_{d_2})\phi(\alpha_{d_2})^{d_2} + \ldots + \phi(\lambda_0)$$

But note that we can replace all of the ϕ by ϕ_0. So we have that

$$\phi_0(\lambda_{d_2})\phi_0(\alpha_{d_2})^{d_2} + \ldots + \phi_0(\lambda_0)$$

Then $\phi(\alpha_{n+1})$ is a root of the polynomials $\phi_0(g(x)) \in M[x]$. There are at most d_2 choices of roots. Hence $\#Hom_F(E, M) \leq d_1 d_2 = [E : F]$. □

Definition 3.16 (Galois extension)*.* An extension E/F is said to be Galois if $\#Aut(E/F) = [E : F]$. We write $Gal(E/F) = Aut(E/F)$ when E/F is Galois.

Example. Take $E = \mathbb{C}$ and $F = \mathbb{R}$. We know $[E : F] = 2$. We claim this is Galois. We need to find a field automorphism of ϕ which is the identity on $\mathbb{R}$. Conjugation forms an automorphism. We take $c : \mathbb{C} \to \mathbb{C}$ by $(x + iy) \mapsto x - iy$. Then $Aut(\mathbb{C}/\mathbb{R}) = \{1, c\}$ which has order 2, so $[E : F] = \#Aut(E/F)$ so this is a Galois extension.

Example. An example of a field extension which is not Galois is given by $F = \mathbb{Q}$ and $E = \mathbb{Q}(2^{1/3}) = \mathbb{Q}[x]/(x^3 - 2) \subset \mathbb{R}$. $Aut(E/F) \leftrightarrow x^3 - 2$ over the field $\mathbb{Q}(2^{1/3}) \subset \mathbb{R}$. We have that $Aut(E/F) = \{2^[1/3]\}$ so it has order 1, which is strictly less than $3 = [E : F]$. Thus E/F is not a Galois extension.

Example. $F = \mathbb{Q}$. and $E = \mathbb{Q}(2^{1/3}, \zeta)$ such that $\zeta^3 = 1$, i.e. ζ satisfies $x^2 + x + 1$ (so there are two choices for ζ, since

$$\zeta = \frac{-1 \pm \sqrt{-3}}{2})$$

We have that $[E : F] = 6$ because $[\mathbb{Q}(\zeta) : F] = 2$ and $[\mathbb{Q}(2^{1/3}) : F] = 3$. So we have that

$$\{1, 2^{1/3}, 2^{2/3}, \zeta, \zeta 2^{1/3}, \zeta 2^{2/3}\}$$

forms the basis of $[E : F]$. So $x^3 - 2$ is irreducible over $\mathbb{Q}(\zeta)$ as well. It is either $\mathbb{Z}_6$ or S_3. We can show it is in fact S_3 by writing it as the field generated by $\{r_1, r_2, r_3\}$ which are the roots of $x^3 - 2$.

Assume E/F is a finite Galois extension. Then set $G = Gal(E/F)$ so that $E^G = \{\alpha \in E : g\alpha = \alpha \forall g \in G\}$. E^G is a subfield of E.

Theorem 3.17 ($E^G = F$)**.** $E^G = F$

Proof. We know that $[E : F] = \#G \leq [E^G : E]$. We also know that $[E : E^G]$ divides $[E : F]$. So $[E : E^G] = [E : F]$, so $[E^G : F] = 1$ which means $E^G = F$. □

Terminology: One says that E/F is normal. Galois $\implies$ normal.

Theorem 3.18 (Splits into Factors)**.** *If $f(x)$ is an irreducible polynomial in $F[x]$, which has a root in E, then $f(x)$ splits completely into linear factors in $E[x]$.*

Proof. Let $r \in E$ be a root of $f(x)$. Let $\{r_1, r_2, \ldots, r_n\}$ be the orbit of r under the action of $Gal(E/F)$. Consider

$$g(x) = (x - r_1)(x - r_2) \cdots (x - r_n) \in E[x]$$

When expanding, we get:

$$x^n - \sigma_1 x^{n-1} + \ldots + (-1)^n \sigma_n$$

where $\sigma_1, \ldots, \sigma_n$ are the elementary symmetric functions in $r_1, \ldots, r_n$. So

$$\sigma_1 = r_1 + r_2 + \ldots + r_n$$

$$\sigma_2 = r_1 r_2 + r_1 r_2 + \ldots + r_1 r_{n-1} = \sum_{j=1}^{n} r_i r_j$$

$$\sigma_3 = \sum_{1 \leq i,j < k \leq n} r_i r_j r_k$$

Thus we have

$$\sigma_n = r_1 \cdots r_n$$

So each $\sigma_j \in E^G$ for $G = Gal(E/F)$ which permuts $r_1, \ldots, r_n$. But then $\sigma_j \in F$ from our previous theorem. Then $g(x) \in F[x]$. So $f(x)$ is the minimal irreducible polynomial of r over F. We have that $f(x)|g(x)$, so $f(x)$ splits completely into linear factors in $E[x]$. □

3.1 Splitting Fields

Let F be a field, with $f(x)$ a polynomial in $F[x]$, not necessarily irreducible.

Definition 3.19 (Splitting Field). A splitting field of $f(x)$ is an extension E/F satisfying:

1. $f(x)$ factors into linear factors in $E[x]$ so $f(x) = (x - r_1) \cdots (x - r_n)$.
2. E is generated as a field by the roots $r_1, \dots, r_n$.

Construction of a splitting field:

- We do induction on $deg(f(x)) = n$.
- If $n = 1$ then $E = F$.
- In general, we want to show $n \implies n + 1$. Take $f(x)$ and let $deg(f(x)) = n + 1$. Let $p(x)$ be an irreducible factor of $f(x)$. Take
$$L = F[x]/(p(x))$$
L is a field containing F and a root of $p(x)$ hence of $f(x)$. Let r be the root of $p(x)$ in L, so $r = x + (p(x))$. $x - r$ divides $f(x)$ because r is a root of $f(x)$. This occurs in $L[x]$. Then $f(x) = (x - r)g(x)$ where $deg(g(x)) = n$. Let E be the splitting field of $g(x)$ over L.

Remark 3.20. It is very hard to compute the degree of a spllitting field of $f(x)$.

If $f(x)$ is irreducible of degree n and E is the splitting field of $f(x)$, then $n \leq [E : F] \leq n!$.

Theorem 3.21 (Splitting Fields Isomorphic)**.** *If $f(x) \in F[x]$ and E and E' are two splitting fields of $f(x)$ over F, then $E \simeq E$ are isomorphic as extensions of F.*

Proof. We will do induction on $deg(f(x)) = n$. For $n = 1$, $E = E' = F$. Assume that the theorem holds for all polynomials of degree n. We will show $n \implies n + 1$: Let $p(x)$ be an irreducible factor of $f(x)$. Let r be a root of $p(x)$ in E. Let r' be a root of $p(x)$ in E'. We have that $F(r)$ and $F(r')$ are isomorphic over F because:
$$F(r) = F[x]/p(x) \quad \text{and } F(r') = F[x]/p(x)$$
Let ϕ be the isomorphism from $F(r)$ to $F(r')$. Let $L = F(r) = F(r')$ where this equality is achieved by ϕ. So E and E' are both splitting fields of $g(x)$ where $g(x)(x - r) = f(x)$. We apply the induction hypothesis to $g(x)$ over L. We get that E and E' are isomorphic as extensions of L as desired. □

Proposition 3.22 (Galois isomorphic to splitting field of polynomial)**.** *If E/F is Galois, then E is isomorphic to the splitting field of a polynomial $f(x) \in F[x]$.*

Proof. Since $[E : F] < \infty$, then we can let $\alpha_1, \dots, \alpha_n$ be a finite set of generators for E/F. Let $f_1, \dots, f_n$ be irreducible polynomials in $F[x]$ having $\alpha_1, \dots, \alpha_n$ as roots. Take $f(x) = f_1(x) \cdots f_n(x)$. By the normality of the extension, in $E[x]$, all the polynomials f_j factor completely into linear factors in $E[x]$. Hence, so does F. So the roots of $f(x)$ generate the extension E/F. Thus E is the splitting field of $f(x)$. □

3.2 Finite Fields

If F is a finite field then it contains $\mathbb{Z}/p\mathbb{Z}$ for some prime p the characteristic of F. Moreover, we can write $n = dim_{\mathbb{F}_p}(F)$ so we have that $\#F = p^n$.

Theorem 3.23 (Field of cardinality p^n)**.** *Given a prime p and an integer $n \geq 1$, there is a field of cardinality p^n. Furthermore, this field is unique up to isomorphism.*

Proof. Possible approach: find a polynomial $f(x) \in \mathbb{F}_p[x]$ which is irreducible of degree n. Then after finding this polynomial, set $F = \mathbb{F}_p[x]/(f(x))$ is the desired field. The problem with this, is that it is not clear if there exists an irreducible polynomial of degree n.

This is where splitting fields are useful. If F is a field of cardinality p^n, then F^* is an abelian group of cardinality $p^n - 1$. This means that $\forall x \in F^x$, we have that

$$x^{p^n-1} = 1$$

But then we can write

$$x^{p^n-1} = 0 \quad \forall x \in F^x$$

$$x^{p^n} - x = 0 \quad \forall x \in F = F^x \cup \{0\}$$

So F is the collection of roots of the polynomial $x^{p^n} - x$. Let F be the splitting field of $x^{p^n} - x$.
Claim: F has cardinality p^n. Note that $x^{p^n} - x$ has distinct roots in any extension of the field of $\mathbb{F}^p$. So if you have $f(x) = x^{p^n} - x$ then $f'(x) = -x$. So $gcd(f(x), f'(x)) = 1$. We find that $\#F \geq p^n$. Exercise: Show that $\#F = p^n$. Key remark: The set of roots of this polynomial $x^{p^n} - x$ is itself a field. So $\#F \leq p^n$. Thus $\#F = p^n$. □

The field with p^n elements is unique up to isomorphism.
F is an extension of $\mathbb{F}_p$. Is F Galois over $\mathbb{F}_p$? $Aut(F/\mathbb{F}_p) =?$.

Definition 3.24 (Frobenius Homomorphism). The map $\phi : F \to F$ defined by $\phi(a) = a^p$ is called the frobenius homomorphism. We will show its actually an automorphism.

Since ϕ is a homomorphism of fields, we have that $\phi : F \hookrightarrow F$ is injective. So ϕ is an $\mathbb{F}_p$-linear transformation from $F \to F$. By the finite dimensionality of F, this implies that ϕ is an automorphism of the field F. This is the frobenius automorphism.
The frobenius automorphism gives $\phi \in Aut(F/\mathbb{F}_p)$. What is the order of ϕ?

$$\phi^k(a) = (a^p)^{p^{\cdots}} = a^{p^k}$$

When is this the identity? What is the smallest k such that $a^{p^k} = a$ for all $a \in F$? If this is true, then $x^{p^k} - x$ has at least p^n roots. We know that $\phi^n = id$ since $a^{p^n} = a$ for all $a \in F$. So ϕ is of order n in $Aut(F/\mathbb{F}_p)$. Thus we get that $\mathbb{Z}/n\mathbb{Z} \subset Aut(F/\mathbb{F}_p)$. So we know that $\#Aut(F/\mathbb{F}_p) \leq [F : \mathbb{F}_p] = n$.

Theorem 3.25 (Galois and Frobenius Aut). *F is a Galois extension of $\mathbb{F}_p$ whose Galois group is cyclic with a canonical generator: the frobenius automorphism. $Gal(F/\mathbb{F}_p) = \{1, \phi, \phi^2, \ldots, \phi^{n-1}\}$.*

Example. Take $q = 8 = 2^3$. $\mathbb{F}_2[x]/(x^3 + x + 1)$. We also have F is the splitting field of $x^8 - x$.

Goal: A more general definition of "Galois" (so that it applies to infinite degrees).

Definition 3.26 (Normal). An extension E/F is normal if every irreducible polynomial in $F[x]$ with a root in E splits into linear factors in $E[x]$.

Theorem 3.27 (Galois implies normal). *If E/F is Galois then E/F is normal over F.*

Proof. Let $f(x)$ in $F[x]$ be an irreducible polynomial, let $r \in E$ such that $f(r) = 0$. Let $\{r_1, \ldots, r_n\}$ be the orbit of r under $G = Gal(E/F)$. Consider the polynomial

$$\tilde{f}(x) = (x - r_1) \cdots (x - r_n) \in E^G[x] = F[x]$$

Since $f(x)$ is the minimal polynomial (because its irreducible) vanishing on r, we find that $f(x)|\tilde{f}(x)$. □

Definition 3.28 (Separable). An extension E/F is separable if every irreducible polynomial with a root in E has no multiple roots in E. Every root occurs with multiplicity 1.

Proposition 3.29 (Character 0 implies separable)**.** *If $char(f) = 0$ then every extension of F is separable.*

Proof. Let $f(x)$ be an irreducible polynomial. Suppose that $f(x) = (x-r)^e g(x)$ in $E[x]$. Take the derivative:

$$f'(x) = e(x-r)^{e-1}g(x) + g'(x)(x-r)^e$$

If $e > 1$ then $f'(r) = 0$. Hence r is a root of the $gcd(f(x), f'(x)) \in F[x]$.
If we are in characteristic 0 we have:

$$f(x) = a_n x^n + \ldots + a_1 x + a_0 \quad \text{for } a_i \in F$$

Then we have

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

This implies that $gcd(f(x), f'(x)) = 1$ so we can deduce that $f(x)$ has no multiple roots. □

Remark 3.30. If $char(F) = p$ then there are plenty of non-constant polynomials with derivative zero. Namely, any polynomial in x^p. In that case, $gcd(f(x), f'(x)) = f(x)$.

Proposition 3.31 (Finite Galois implies separable)**.** *If E/F is finite Galois then it is separable.*

Proof. Same idea as before (in the normal proof). □

Theorem 3.32 (Normal and Separable implies Galois)**.** *If E/F is a finite extension, normal, and separable, then E/F is Galois.*

Proof. Recall the proof that $\#Aut(E/F) \leq [E : F]$. We will retrace this proof using the hypotheses normal and separable to replace the inequalities by equalities throughout the proof. We will prove by induction: Consider $\#Hom_F(K, E)$ where $F \subseteq K \subseteq E$. We will show

$$\#Hom_F(K, E) = [K : F]$$

by induction on the $deg(K/F)$.
Let $n = [K : F] = 1$:
This case is trivial, it is always satisfied.

Now for general n:
Suppose K is generated by $F(\alpha) = F[x]/(p(x))$ where $p(x)$ is an irreducible polynomial with root α, and $deg(p(x)) = deg(K/F)$. Then we have that

$$Hom_F(k, E) = Hom_F(F(\alpha), E) = \{\text{roots of } p(x) \text{ in } E\} = deg(p(x)) \text{ by the normality and separability}$$

We are trying to construct a ring homomorphism $\phi : F[x]/(p(x)) \to E$. This is equivalent to $\phi : F[x] \to E$ such that $p(x) \in ker(\phi)$, that is, $\phi(x)$ is a root of $p(x)$. For the general case, we assume

$$K = F(\alpha_1, \ldots, \alpha_t) = F(\alpha_1, \ldots \alpha_{t-1})(\alpha_t) = K_{t-1}(\alpha_t) \quad K_{t-1} \subsetneq K$$

Then we know that

$$[K_{t-1} : F] < [K : F] = n$$

We apply the induction hypothesis on K_{t-1}. We have that

$$\#Hom_F(K_{t-1}, E) = [K_{t-1} : E]$$

We observe that there are exactly $[K : K_t]$ extensions of any $\phi_0 : K_{t-1} \to E$. Let $p(x)$ be the minimal polynomial of α_t over K_{t-1}. So we have that

$$deg(p(x)) = [K : K_{t-1}]$$

Identify $K = K_{t-1}[x]/(p(x))$. We know that $p(\alpha_t) = 0$ so $\phi(p(\alpha_t)) = 0$. This is the same as $p_{\phi_0}((\phi(\alpha_t))) = 0$. That is,

$$p_{\phi_0}(x) = \phi_0(a_n)x^n + \ldots + \phi_0(a_1)x + \phi_0(a_0) \in E[x]$$

If $\phi|_{K_{t-1}} = \phi_0$, then $\phi(\alpha_t) = 0$.

Claim: $p_{\phi_0}(x)$ splits into distinct linear factors in $E[x]$. We know that $p(x)$ has a root in E, namely α_t. By normality, $p(x)|g(x)$ where $g(x)$ is the minimal polynomial of α_t over F. Then $g(x)$ factors into distinct linear factors over E by normality and separability. This implies that $p_{\phi_0}(x)|g_{\phi_0}(x) = g(x)$. So $p_{\phi_0}(x)$ has exactly K/K_{t-1} roots. We put this all together:

$$\#Hom_F(K,E) = \#Hom_F(K_{t-1},E) \times \{\text{extensions } \phi \text{ of any } \phi_0 : K_{t-1} \to E\} = [K_{t-1} : F][K : K_{t-1}] = [K : F]$$

Then we apply this to the case $K = E$, so we find that $\#Aut_F(E) = [E : F]$. □

For finite extensions, being Galois is equivalent to being normal and separable. This also applies to infinite extensions. We can rewrite the definition:

Definition 3.33 (Galois Reworked). An extension E/F is Galois if it is normal and separable over F.

Proposition 3.34 (Finite Extension Equivalencies). *If E/F is a finite extension, then TFAE:*

- $\#Aut(E/F) = [E : F]$
- *E is normal and separable over F*
- *E is the splitting field of a separable polynomial over F*

Remark 3.35. The second property also makes sense for infinite extensions.

Proposition 3.36 (Tower Galois property). *If E/F is a Galois extension, and K is any subfield of E containing F*

$$F \subset K \subset E$$

Then E is Galois over K.

Proof. This is obvious with the third property of Galois extensions. By property two, if $\alpha \in E$, given that E/F is normal and separable, we have that there exists a polynomial $f(x) \in F[x]$ which is irreducible, and it splits into distinct linear functions in E, and satisfies $f(\alpha) = 0$. Let $g(x)$ be the min polynomial of α over K. This $g(x) \in K[x]$ and $g(\alpha) = 0$ and g is irreducible. Then we have that $g(x)$ must divide $f(x)$ in $K[x]$ because it is the minimal polynomial. Hence this divisibility also holds in $E[x]$. But in $E[x]$, $f(x)$ factors into distinct linear factors. This implies that E/K is normal and separable. Hence Galois by our earlier proposition. We now want to see this from the perspective of property one. Property one asserts that $\#Aut(E/K) = [E : K]$. Let $G = Gal(E/F)$. Let $X = Hom_F(K,E)$. Recall that $\#X = [K : F]$. X is naturally a G-set under the rule: if $\phi \in X$ and $\sigma \in G = Aut(E)$ then $\sigma \star \phi = \sigma \circ \phi$. Furthermore, X is a transitive G-set. We showed that any $\phi : K \to E$ extends to $\tilde{\phi} : E \to E$. If $\phi_1, \phi_2 : K \to E$, then

$$\sigma = \tilde{\phi_1} \circ \tilde{\phi_2}^{-1} \in G$$

$$\sigma\phi_2 = \phi_1$$

By the Orbit Stabilizer Theorem, we have that

$$\#X \cdot \#Stab_G(Id : K \to E) = \#G$$

This implies that

$$[K : F]\#Aut(E/K) = [E : F]$$

By multiplicativity of the degree, $\#Aut(E/K) = [E : F]/[K : F] = [E : K]$. This is exactly what we wanted to show. □

Caveat: K need not be Galois over F.

Remark 3.37. If $E/\mathbb{F}_p$ is a finite extension, then $E/\mathbb{F}_p$ is Galois and cyclic with a canonical generator $\sigma : x \mapsto x^p$. If we let $K = \mathbb{F}_{p^t}$, then $\mathbb{F}_p \subset K \subset E$, then E is Galois over K. The Galois group of E/K is generated by σ^t where $\sigma^t : x \mapsto x^{p^t} = x^{\#K}$. This σ^t is the relative Frobenius element over K.

Theorem 3.38 (Injections between sets)**.** *The map $K \mapsto Gal(E/K)$ is an injection from*

$$\{\textit{subfields } F \subset K \subset E\} \to \{\textit{subgroups of } Gal(E/F)\}$$

Proof. We can show that it is injective by showing that it has a left-inverse. If you know $H = Gal(E/K)$, how can you recover K from H? Claim: $K = E^H$. □

Corollary 3.39 (Finitely many subfields)**.** *If E/F is finite Galois then there are finitely many subfields*

$$F \subset K \subset E$$

Proof. The number of subgroups is finite because the Galois group is finite, and so there are at most as many subfields as subgroups of the Galois group E/F. □

Corollary 3.40 (More finitely many subfields)**.** *If E/F is any finite separable extension, then there are finitely many subfields*

$$F \subset K \subset E$$

Proof. E is separable. Then it is generated by a collection $\alpha_1, \dots, \alpha_t$ where α_j is the root of a separable polynomial $g_j(x) \in F[x]$. Let $\tilde{E}$ be the splitting field of $g_1(x) \cdots g_t(x)$. So $\tilde{E} \supset E$ and $\tilde{E}/F$ is a Galois extension. By the previous corollary, there are finitely many K such that

$$F \subset K \subset \tilde{E}$$

Hence the same conclusion holds for E. □

Remark 3.41. E/F separable is essential for this to work.

Example. Take $F = \mathbb{F}_p(u, v) = \{\text{rational functions } u, v\}$. Let $E = \mathbb{F}_p(u^{1/p}, v^{1/p})$. We have that $[E : F] = p^2$. We claim there is no number $R(u, v)^p = u$, because otherwise it would have the root p in E. For $\alpha \in E$, take

$$\alpha = R(u^{1/p}, v^{1/p}) = \frac{f(u^{1/p}, v^{1/p})}{g(u^{1/p}, v^{1/p})}$$

We have that

$$\alpha^p = (\frac{f(u^{1/p}, v^{1/p})}{g(u^{1/p}, v^{1/p})})^p = \frac{f(u, v)}{g(u, v)} \in F$$

This implies that $[F(\alpha) : F] = 1$ or p for all $\alpha \in F$. This means $F(\alpha) \neq E$. So the Primitive Element Theorem does not hold here. This is because E/F has infinitely many distinct subfields.

Theorem 3.42 (Primitive Element Theorem)**.** *If E/F is finite, separable then $\exists \alpha \in E$ such that $E = F(\alpha) = F[\alpha] \simeq F[x]/(p_\alpha(x))$ where $p_\alpha(x)$ is the minimal polynomial which vanishes at α.*

Proof. We know that $E = F(\alpha_1, \dots, \alpha_n)$. We will proceed by induction on the number of generators. If F is finite then the result is clear because a finite field can always be generated by a single element. That is, $E^\star = E \setminus \{0\}$ is cyclic so there exists $\alpha \in E$ such that $E^* = \{1, \alpha, \alpha^2, \dots, \alpha^n, \dots\}$. The $n = 1$ case is also trivial. For the $n = 2$ case we assume we work in infinite dimensions. Let $E = F(\alpha, \beta)$. Consider

$$E_t = F(\alpha + t\beta) \quad t \in F$$

There are infinitely many t but there are finitely many E_t because there are finitely many subfields of E/F. So $\exists t_1 \neq t_2 \in F$ such that $E_{t_1} = E_{t_2}$ by pigeonhole principle. This means that

$$F(\alpha + t_1\beta) = F(\alpha + t_2\beta)$$

We claim that this extension is equal to E. So we have that $\alpha + t_1\beta \in E$ and $\alpha + t_2\beta \in E$. Since fields are closed under addition and subtraction, we can subtract one from the other to get rid of α, we are also allowed to divide:

$$\frac{(\alpha + t_1\beta) - (\alpha + t_2\beta)}{t_1 t_2} \in E_{t_1} \implies \beta \in E_0 \text{ and } \exists \alpha \in E_0$$

Now for the $n > 2$ case: We have that

$$\begin{aligned} E &= F(\alpha_1, \dots, \alpha_{n+1}) \\ &= F(\alpha_1, \dots, \alpha_n)F(\alpha_{n+1}) \\ &= F(\beta)F(\alpha_{n+1}) \\ &= F(\beta, \alpha_{n+1}) \\ &= F(\alpha) \quad \text{by n=2 case} \end{aligned}$$

□

Remark 3.43. The separability assumption is key in the statement.

Our goal: $\forall H \subset G$, we recover $Gal(E/E^H) = H$.

Proposition 3.44 ($(E : E^H) = \#H$)**.** $[E : E^H] = \#H$

Proof. By the Primitive Element Theorem, we know that for some $\alpha \in E$ we have that $E = E^H(\alpha)$. Consider $H\alpha$ = orbit of α under the action of H. $H\alpha = \{\alpha_1, \dots, \alpha_n\}$. We claim $\#H = \#H\alpha$. This is because $stab_H(\alpha) = 1$ since $g\alpha = \alpha \implies g = id$ on $E = E^H(\alpha)$. Consider $p(x) = (x - \alpha_1)\cdots(x - \alpha_n) \in E^H[x]$, and $p(\alpha) = 0$, and $p(x)$ is irreducible over E^H because H acts transitively on its roots. This implies that $[E : E^H] = deg(p(x)) = n = \#H$. □

Corollary 3.45 ($H = Gal(E/E^H)$)**.** $H = Gal(E/E^H)$

Theorem 3.46 (Galois Correspondence)**.** *$\{$subfields $F \subset K \subset E\}$ and $\{$subgroups of $H \subset G\}$ are mutual inverse bijections.*

Proof. Not covered □

Remark 3.47. Galois correspondence is inclusion reversing.

Example. $F = \mathbb{Q}$ and $E = \mathbb{Q}(2^{1/4})$ be the splitting field of $x^4 - 2$. Let $r = 2^{1/4}$ and consider $\mathbb{Q}[r]/r^4 - 2$.

Complements:

- Take $\sigma \in Gal(E/F)$ and $F \subset K \subset E$. We can observe that $\sigma K = \{\sigma x : x \in K\}$ is also a subfield of E/F.
- If H corresponds to K under the Galois correspondence, then $\sigma H \sigma^{-1}$ corresponds to σK under the Galois correspondence.

So $Gal(E/(\sigma K)) = \{\alpha \in Gal(E/F) : \alpha(\sigma x) = \sigma x \quad \forall x \in K\}$. Then we have that

$$\alpha(\sigma x) \iff \sigma^{-1}\alpha\sigma(x) \in Gal(E/K) = H$$

Thus $\alpha \in \sigma H \sigma^{-1}$.

Theorem 3.48 (Equivalencies for Galois)**.** *Given $F \subset K \subset E$. The following are equivalent:*

(i) $\sigma K = K \quad \forall \sigma \in Gal(E/F)$

(ii) K *is Galois over* F

(iii) $Gal(E/K)$ *is a normal subgroup of* $Gal(E/F)$.

Proof. ($(i) \implies (iii)$): Let $H = Gal(E/K)$. Then $\sigma K = K$ for all $\sigma \in G = Gal(E/F)$ implies that $\sigma H \sigma^{-1} = H$ for all $\sigma \in G$ by Galois correspondence. This implies that H is a normal subgroup of G.

($(i)\&(iii) \implies (ii)$): Restriction gives a homomorphism from $\eta : Gal(E/F) \to Aut(K/F)$. $ker(\eta) = Gal(E/K)$. Then by the isomorphism theorem we have an injection from $Gal(E/F)/Gal(E/K) \hookrightarrow Aut(K/F)$. Then we have that

$$\#Gal(E/F)/Gal(E/K) = [E : F]/[[E : K]] = [K : F]$$

Thus we have that K/F is Galois. Moreover, $Gal(K/F) = G/H$.

($(iii) \implies (i)$): exercise

($(ii) \implies (i)$): exercise □

3.3 Radical Extensions

Definition 3.49 (Radical Extensions). An extension E/F is called a radical extension if $\exists n > 1$ and an element $a \in F$ such that $E = F(a^{1/n}) = F[x]/(x^n - a)$ where $x^n - a$ is irreducible. If $x^n - a$ is not irrecible, then we can take $F[x]/(g(x))$ where $g(x)$ is an irreducible factor of $x^n - a$.

Definition 3.50 (Tower). A tower of radical extensions of E/F is a sequence

$$F = E_0 \subset E_1 \subset \ldots \subset E_n = E$$

where each E_i/E_{i-1} is a radical extension for all $i = 1, \ldots, n$. That is, $E_i = E_{i-1}(a_i^{n_i})$ for $a_i \in E_{i-1}$ and $n_i \geq 1$.

Question: Is every finite extension of $\mathbb{Q}$ contained in a tower of radical extensions?
Classical question: Given a polynomial $f(x) \in \mathbb{Q}[x]$, can its roots be expressed in terms of radicals?
Not all algebraic α are constructible. We showed that if $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ then α is not constructible. If α is constructible, then $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^t$ some power of 2.
Goal: Find a structural invariant of $\mathbb{Q}(\alpha)/\mathbb{Q}$ when α is constructible by radicals. The degree is too crude. The idea is to replace the degree by the atuomorphism of $\mathbb{Q}(\alpha)/\mathbb{Q}$.
Consider automorphism groups of radical extensions.
Let $E = F(a^{1/n})$ for $a \in F$. What is $Aut(E/F)$?

Remark 3.51. E/F need not be Galois.

Example. $\mathbb{Q}(2^{1/3})$ is not Galois but $Aut(\mathbb{Q}(2^{1/3})/\mathbb{Q}) = 1$.

We want to make a further assumption on F to ensure that it is Galois.
We can adjoin it with the primitive roots of unity, that is:

$$\mathbb{Q}(a^{1/n}, a^{1/n}\zeta, a^{1/n}\zeta^2, \ldots, a^{1/n}\zeta^{n-1}) = \mathbb{Q}(\zeta, a^{1/n})$$

Theorem 3.52 (Abelian Galois)**.** *Suppose F contains n distinct n-th roots of unity, and let $\mu_n(F) = \{x \in F^\times : x^n = 1\} \simeq \mathbb{Z}/n\mathbb{Z}$. We get that $F(a^{1/n})$ is Galois with abelian Galois. Moreover, this group is a subgroup of $\mu_n(F)$.*

Proof. Consider $\eta : Aut(E/F) \to \mu_n(F)$ by $\sigma \mapsto \sigma(a^{1/n})/a^{1/n} \in \mu_n(F)$. We can check that η is a homomorphism.

$$\begin{aligned}\eta(\sigma_1\sigma_2) &= \sigma_1\sigma_2(a^{1/n})/a^{1/n}\\ &= \sigma_1(\eta(\sigma_2)a^{1/n})\\ &= \eta(\sigma_2)\sigma_1(a^{1/n})/a^{1/n}\\ &= \eta(\sigma_2)\eta(\sigma_1)\end{aligned}$$

We claim η is injective. If $\eta(\sigma) = 1$ then $\sigma(a^{1/n}) = a^{1/n}$ which implies that $\sigma = id$ on E. We have $Image(\eta) \simeq Gal(E/F)$ where E is the splitting field of $x^n - a$. □

Definition 3.53 (Solvable). A finite group G is solvable if there is a sequence of $1 =\subset G_0 = G_1 \subset G_2 \subset \ldots \subset G_n = G$ such that

(1) $G_{i-1} \triangleleft G_i$ so that G_{i-1} is normal in G_i

(2) G_i/G_{i-1} is abelian gorup for all i

Example. An ablian group $1 \triangleleft G$

Example. S_3 is solvable, $1 \triangleleft A_3 \triangleleft S_3$

Example. S_4 is solvable. $V = \{1, (12)(34), (13)(24), (14)(23)\}$, then $1 \triangleleft V \triangleleft S_4$. And we know that so $S_4/V = S_3$. $1 \triangleleft V \triangleleft A_4 \triangleleft S_4$.

Example. S_5 is NOT solvable. $A_5 \triangleleft S_5$ is the only normal subgroup of S_5. But A_5 is not abelian. Then S_5 and A_5 is NOT solvable.

Remark 3.54. A polynomial $f(x) \in F[x]$ is solvable by radicals if its splitting field is contain in a tower of radical extensions.

Theorem 3.55 (Tower of extensions contained in Gal extensions)**.** *If E/F is a tower of radical extensions, then it is contained in a Galois extensions $\tilde{E}/F$ with solvable Galois group. Some assumptions: $char(F) = 0$.*

Proof. Suppose $F = E_0 \subset E_1 \subset \ldots \subset E$ where $E_i = E_{i-1}(a_i^{1/n})$ for $a_i \in E_{i-1}$. We prove the claim by induction on n. $n = 1$ case: $E = F(\alpha)$ $\alpha^m = a \in E$. Let $\tilde{E}$ be the splitting field of $x^m - a$. So $\tilde{E} = F(\zeta, a) = F(\zeta)(a)$. $F \subset F(\zeta) \subset F(\zeta)(a)$ where ζ is the primitive mth root of unity ($\zeta^m = 1$). Then consider $\sigma \in Gal(F(\zeta)/F)$

$$\sigma_a : \zeta \mapsto \zeta^a$$

where $gcd(a, m) = 1$, $a \in (\mathbb{Z}/m\mathbb{Z})^\times$.

$$\sigma_a \circ \sigma_b = \sigma_{ab} \text{ as } \sigma_a \circ \sigma_b(\zeta) = \sigma_a(\zeta^b) = (\zeta^a)^b = \zeta^{ab}$$

So there is an injection from

$$Gal(F(\zeta)/F) \hookrightarrow (\mathbb{Z}/m\mathbb{Z})^\times$$

$F(\zeta)/F$ is an abelian extension. If $\sigma \in Gal(F(\zeta, \alpha)/F(\zeta))$ then

$$\sigma(\alpha) = \zeta_\sigma \alpha$$

where ζ_σ is determined by σ. Moreover,

$$\begin{aligned}\sigma_{\zeta_1} \circ \sigma_{\zeta_2}(\alpha) &= \sigma_{\zeta_1}(\sigma_{\zeta_2}(\alpha))\\ &= \sigma_{\zeta_1}(\zeta_2\alpha)\\ &= \zeta_2\sigma_{\zeta_1}(\alpha)\\ &= \zeta_2\zeta_1\alpha\end{aligned}$$

so there is an injection.

$$Gal(F(\zeta,\alpha)/F(\zeta)) \hookrightarrow \mu_m \simeq \mathbb{Z}/m\mathbb{Z}$$

where μ_m is the set of roots of unity. This implies that $Gal(F(\zeta,\alpha)/F(\zeta)) \subset \mu_m$. Let $G_1 = Gal(F(\zeta,\alpha)/F(\zeta))$ and $G = Gal(F(\zeta)/F)$. G_1 is normal in G since $F(\zeta,\alpha)^{G_1} = F(\zeta)$ is Galois over F. $G_1 \subset \mu_m \simeq \mathbb{Z}/m\mathbb{Z}$. Also, $G/G_1 \subset (\mathbb{Z}/m\mathbb{Z})^\times$. Since $G \leftrightarrow F$ and $G_1 \leftrightarrow F(\zeta)$, and $1 \leftrightarrow F(\zeta,\alpha)$. $F(\zeta)/F$ Galois implies that G_1 is normal. Then $G/G_1 = Gal(F(\zeta)/F) \subset (\mathbb{Z}/m\mathbb{Z})^\times$ so then $G_1 = Gal(F(\zeta,\alpha)/F(\zeta)) \subset \mathbb{Z}/m\mathbb{Z}$. $F \subset F(\alpha) \subset F(\alpha,\zeta)$ implies that H is abelian and H need not be normal. Cont next lecture. □

Proposition 3.56 (Solvable implies quotient is solvable)**.** *If G is a solvable group, then any quotient $\overline{G}$ of G is solvable.*

Proof. $1 \triangleright G_1 \triangleright \ldots \triangleright G_n = G$. Then $1 \subset \overline{G_1} \subset \ldots \subset \overline{G_{n-1}} \subset \overline{G}$. There is a surjective homomorphism $\eta : G \to \overline{G}$. By definition, $\eta(G_i) = \overline{G_i}$ and so η induces a well defined map

$$\overline{\eta_i} : G_i/G_{i-1} \to \overline{G_i}/\overline{G_{i-1}}$$

by $aG_{i-1} \mapsto \eta(a)\overline{G_{i-1}}$. Note: $G_i \supset G_{i-1}$ implies that $\eta(G_i) \supset \eta(G_{i-1})$. Also, $\overline{\eta_i}$ is surjective by construction. Then $\overline{G_i}/\overline{G_{i-1}}$ are abelian, so we have that $1 \triangleright \overline{G_1} \triangleright \ldots \triangleright \overline{G}$. □

Theorem 3.57 (Solvable by radicals implies Gal solvable group)**.** *If $f(x) \in F[x]$ is solvable by radicals, then $Gal(f)$ is a solvable group.*

Proof. Let $F = E_0 \subset E_1 \subset \ldots \subset E_n = E$ be a tower with $E_i = E_{i-1}(a^{1/m_i})$, $a_i \in E_{i-1}$, and $m_i \geq 1$. Now do induction on n. $E = F(a^{1/m})$. $\tilde{E}$ = normal closer of E over F which is a subset of the splitting field. Then we have that

$$x^m - a = F(\zeta, a^{1/m}), \zeta^m = 1$$

Let $G = Gal(\tilde{E}/F)$ is solvable, in two stages it has an abelian normal subgroup with abelian quotient $H \triangleleft G$. Let $H = Gal(F(\zeta, a^{1/m})/F(\zeta)) \subseteq \mathbb{Z}/m\mathbb{Z}$ and $G/H \subseteq (\mathbb{Z}/m\mathbb{Z})^\times$. Done. Now for the $n-1 \implies n$ case. □

Theorem 3.58 (Tower of radicals contained in Gal extensions)**.** *If E/F is a tower of radical extensions, then it is contained in a Galois extension $\tilde{E}/F$ with $Gal(\tilde{E}/F)$ solvable.*

Proof. If $f(x)$ is solvable then E= splitting field of F is contained in the tower of radical extensions. Therefore, E is contained in a subgroup extension of F, say $\tilde{E}$. Then G is a quotient of $Gal(\tilde{E}/F)$ so G is solvable. □

Theorem 3.59 (Quintic polynomial not solvable by radicals)**.** *If $f(x)$ is a quintic polynomial and $Gal(f) = S_5$ then $f(x)$ is not solvable by radicals.*

Proposition 3.60 (Transitive subgroup of S_5)**.** *Let G be a transitive subgroup of S_5 containing a transposition. Then $G = S_5$.*

Proof. G transitive $\implies 5|\#G$. We can assume without loss of generality that $\sigma : (12345) \in G$ and that $\tau : (12) \in G$. Conjugating τ by $\sigma^1, \sigma^2, \ldots, \sigma^n$, we have that $(23), (34), (45), (51) \in G$. Then we have that $(12)4(24) \implies (13) \in G$. So all 10 transpositions belong to G. □

Proposition 3.61 (Degree 5 has $Gal(f) = S_5$)**.** *Let $f(x)$ be a polynomial of degree 5 over $\mathbb{Q}$ satisfying*

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

2. *$f(x)$ has exactly 3 real roots*

Then we can get many $f(x)$ with $Gal(f) = S_5$.

3.4 Main Theorem of Galois Theory

If $f(x)$ is solvable by radicals then $Gal(f)$ is solvable group. Conversely, every solvable extension of F is constructible by radicals.

Remark 3.62. (1) It is enough to show this for abelian E/F. If E is solvable, then write $F \subset E_1 \subset \ldots \subset E_n = E$. We have that E_i/E_{i+1} is abelian.

(2) We can assume that F contains n-th roots of unity, so $n = [E : F]$.

We can view E as a F-linear representation of $G = Gal(E/F)$. So if $\sigma \in G$, $x, y \in E$, then $\sigma(x + y) = \sigma(x) + \sigma(y)$. Also for $\lambda \in F$, $x \in E$, then $\sigma(\lambda x) = \lambda\sigma(x)$. We can write

$$E = \oplus_{\chi \in G}$$

$$\widehat{G} = Hom(G, F^\times)$$

$$E[x] = \{v \in E : \sigma v = \chi(\sigma) \cdot v, \forall \sigma \in G\}$$

So $dim_F E[\chi] \leq 1$. Suppose $v \in E[\chi]$ for $v \neq 0$. Take $w \in E[\chi]$. Consider $w/v \in E$. Then $\sigma(w/v) = \sigma(w)/\sigma(v) = \chi(\sigma)w/\chi(\sigma)v = w/v$ for all $\sigma \in G$. So we can conclude that $w/v \in E^G = F$. This implies that $w = \lambda v$ with $\lambda \in F$. This implies that $E[\chi] = Fv$. Thus $\dim_F E = [E : F] = \#G$. This implies that $\dim_F(\oplus_{\chi \in G} E[\chi]) \leq \#\widehat{G} = \#G$. This implies that $\dim_F(E[\chi]) = 1$. Thus E is isomorphic to $F[G]$ as a G-representation (regular representation) Fact: this is also true for G non-abelian. For each $\chi \in \widehat{G}$, let $y_\chi \in E[\chi]$ be a basis. Then $F = F(y_\lambda : \chi \in \widehat{G})$. But what about y_χ^n? We apply $\sigma \in G$ to it:

$$\sigma(y_\lambda^n) = [\sigma(y_\chi)]^n = (\chi(\sigma)y_\lambda)^n = \chi(\sigma)^n y_\chi^n = y_\lambda^n \quad \forall \sigma \in G$$

This implies that $y_\lambda^n = a_\chi \in F$ and we can write $y_\chi = a_\chi^{1/n}$. Thus $E = F(a_\chi^{1/n}, \chi \in \widehat{G})$.

We showed that $f(x)$ is solvable by radicals $\iff$ $Gal(f)$ is solvable. Application to understanding the cubic equation (Cardano's Approach). Let E=splitting field of f.
We now want to consider the quartic equations of degree 4. S_4 is a solvable group (and any transitive subgroup of S_4 is solvable). This implies that there is always a solution to quartic equations. We have that

$$S_4 \underbrace{\triangleright}_{\mathbb{Z}/2\mathbb{Z}} A_4 \underbrace{\triangleright}_{\mathbb{Z}/3\mathbb{Z}} V \quad \underbrace{\triangleright}_{\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}} \quad 1$$

where V is the Klein 4 group. We can further write:

$$S_4 \underbrace{\triangleright}_{\mathbb{Z}/2\mathbb{Z}} A_4 \underbrace{\triangleright}_{\mathbb{Z}/3\mathbb{Z}} V \underbrace{\triangleright}_{\mathbb{Z}/2\mathbb{Z}} \{1, \tau\} \underbrace{\triangleright}_{\mathbb{Z}/2\mathbb{Z}} 1$$

We have that $\mathbb{Q} \subset K \subseteq L \subset L' \subset E$
Then we have by adjoining these operations we can get to our splitting field

$$\mathbb{Q} \underbrace{\subset}_{\sqrt{\cdot}} K \underbrace{\subset}_{(\cdot)^{1/3}} K(\zeta) \underbrace{\subseteq}_{\sqrt{\cdot}} L(\zeta) \underbrace{\subset}_{\sqrt{\cdot}} E(\zeta)$$

The fact that V is normal in S_4 tells us that L is Galois over $\mathbb{Q}$. $Gal(L/\mathbb{Q}) = S_4/V = S_3$. The idea is to take $f(x) = (x - r_1)(x - r_2)(x - r_3)(x - r_4)$. Question: Construct a cubic polynomial in $\mathbb{Q}(x)$ called $g(x)$ such that the splitting field of g is L. We know that:

$$V = \{1, (12)(34), (13)(24), (14)(23)\}$$

$r_1r_2 + r_3r_4$ is fixed under V. We find the distinct conjugates now:

$$\{r_1r_2 + r_3r_3, r_1r_3 + r_2r_4, r_1r_4 + r_2r_3\}$$

The cubic resolvant:

$$g(x) = (x - (r_1r_2 + r_3r_4))(x - (r_1r_3 + r_2r_4))(x - (r_1r_4 + r_2r_3)) \in E^{S_4}[x] = \mathbb{Q}[x]$$

Assume that $f(x) = x^4 + ax^2 + bx + c = 0$ (can always do this), where $a, b, c \in \mathbb{Q}$. Now have to figure out what the coefficients are.

$$x^3 - (r_1r_2 + r_3r_4 + r_1r_3 + r_2r_4 + r_1r_4 + r_2r_3)x^2 + \dots$$

$$\begin{aligned} f(x) &= (x - r_1)(x - r_2)(x - r_3)(x - r_4) \\ &= x^4 - (r_1 + r_2 + r_3 + r_4)x^3 + (\sum_{1 \leq i < j \leq 4} r_ir_j)x^2 \end{aligned}$$

So we find that $(\sum_{1 \leq i < j \leq 4} r_ir_j) = a$.
Then $g(x) = x^3 - ax^2 + \dots$.

3.5 Back to Constructible Numbers

At the beginning we proved this

Theorem 3.63 (Contructible implies 2^t)**.** *α is constructible by ruler and compass implies that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^t$ for some $t \geq 0$.*

Remark 3.64. The converse is not true for this theorem.

Example. This is a counter example to the converse of this theorem. Let $f(x)$ be any irreducible polynomial of degree 8 over $\mathbb{Q}$. We know that this contains an 8-cycle. Assume that $f(x)$ has a Galois gorup equal to S_8. Then $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 8$. But we claim that it is not constructible by ruler and compass. We apply Galois correspondence. We find that S_7 corresponds to $\mathbb{Q}(\alpha)$, and we claim that it contains no quadratic extension. If there were a quadratic extension K then it would have to correspond to a subgroup H under the Galois correspondence which would contain S_7 and 4. But can there be such a group?

Remark 3.65. In general, for $n \geq 4$ S_{n-1} is a maximal subgroup of S_n. So there is no subgroup which contains S_{n-1} properly in S_n.

Thus there cannot be such an H whose index is strictly less than n. This would mean that there is an action of S_n on a set of cardinality t, which would give a homomorphism from $S_n \to S_t$ for $t < n$ which cannot happen.

If we want an if and only if for this theorem, we need more restrictions.

Theorem 3.66 (Constructible iff Gal)**.** *α is constructible by ruler and compass $\iff$ $\mathbb{Q}(\alpha)$ is contained in a Galois extension $E/\mathbb{Q}$ with $Gal(E/QQ) = 2^t$ for $t \geq 0$.*

Proof. Think about □

Remark 3.67. This suggests that every group whose cardinality is a power of p is solvable when p is prime.

We take

$$\#G = Z(G) + \sum_{\#C_i} \#C_i$$

where $Z(G) = \{g \in G : gh = hg \quad \forall h \in G\}$
This suggests that $Z(G)$ would be a good candidate for the first step of normal subgroups of G. Now you can proceed by induction. Taking $G/Z(G)$, it has a non-trivial center $\overline{G_1} = Z(G/Z(G))$ and let $G_1 =$ inverse image in G. Then $1 \lhd Z(G) \lhd G$. Now we can iterate this process.
f solvable by radicals $\iff$ $Gal(f)$ is solvable.
f is constructible $\iff$ $Gal(f)$ is a 2-group.
Can find a sequences $G \rhd G_1 \rhd \ldots \rhd$ such that $G_i/G_{i+1} = \mathbb{Z}/2\mathbb{Z}$.

3.6 Fundamental Theorem of Algebra

Theorem 3.68 (Fund Thm of Algebra)**.** *$\mathbb{C}$ is algebraically closed.*

Facts:

- Every polynomial of odd degree in $\mathbb{R}[x]$ has a root in $\mathbb{R}$. This follows from the intermediate value theorem.
- Every quadratic equation in $\mathbb{C}[x]$ has roots in $\mathbb{C}$

Proof. Let K be a finite extension of $\mathbb{C}$. Let K' be the Galois closure of K over $\mathbb{R}$. Sylow theorem $\implies$ G has a subgroup of cardinality 2^t. The field $F = (K')^s$ is invariant under the action of Sylow subgroup and so is of odd degree over $\mathbb{R}$ hence $F = \mathbb{R}$ implies that $G = s$. Then $\#G = 2^t$. Then $\#G_0 = \#Gal(K/\mathbb{C}) = 2^{t-1}$. If G_0 is non-trivial, it contains a subgroup G_{00} of index 2 in G_0. This would contradict the fact that $\mathbb{C}$ has no quadratic extensions $\implies G_0 = 1 \implies K' = \mathbb{C} \implies K = \mathbb{C}$. □

Problem: How does one compute $Gal(f) = G$, $f(x) \in \mathbb{Q}[x]$? If $f(x)$ is irreducible, $deg(f) = n$, $G \subseteq S_n$, $f(x) = (x - r_1)(x - r_2)\ldots(x - r_n)$.
Resolvent of f, variables $x_1, \ldots, x_n$

$$\prod_{\delta \in S_n} (r_1 x_{S_1} + r_2 x_{S_2} + \ldots + r_n x_{S_N})$$

# Factor $R(x_1, \ldots, x_n)$ in $\mathbb{Q}[x_1, \ldots, x_n]$. $R(x_1, \ldots, x_n) = R_1 \cdot R_2 \cdots R_t$.

Theorem 3.69 ($G = Stab_{S_n}(R_1)$)**.** $G = Stab_{S_n}(R_1)$

Proof.

$$R(x_1, \ldots, x_n) = \prod_{\zeta \in G/S_n} \left(\prod_{\sigma \in S_n} (r_1 x_{\sigma_1} + r_2 x_{\sigma_2} + \ldots + r_n x_{\sigma_n}) \right)$$

Each factor inside is irreducible over $\mathbb{Q}$ and the stabilizer of R_1 is G. The question of calculating G given f is connected to problems of factoring polynomials over fields. Good algorithm exists. If we take polynomial $f(x) \in \mathbb{F}_p[x]$, then it is easy to factor $f(x)$ with

$$gcd(f(x), x^p - x) = \prod_{f(r)=0} (x - r), \quad x = 0, 1, \ldots, p - 1$$

$$x^p = x \cdot (x^{(p-1)/2})^2 \mod f(x)$$

Then we have that if $f \in \mathbb{Q}[x]$, we can associate it to $f \in \mathbb{Z}[x]$ and then further by $f \mod 2 \in \mathbb{Z}/2/ZZ[x]$ and $f \mod p \in \mathbb{Z}/p\mathbb{Z}[x]$.

□

Converse: Given G is there an extension of $\mathbb{Q}$ with $Gal(E/\mathbb{Q}) \simeq G$. This is an open question.