Honours Algebra IV

MATH 457

Nicholas Hayek

Lectures by Prof. Henri Darmon

CONTENTS

I Representation Theory **1**

Characters **9**
Orthogonality of Irreducible Group Characters 12
Regular Representations of G 13

Abelian Groups **15**

Fourier Analysis **16**
Character tables of S_4 and A_5 17

Induced Representations **20**

Tensor Products **24**

Applications of Representations **24**

II Galois Theory **27**

Splitting Fields **34**

Normal, Separable, and Galois **36**

Galois Correspondence **39**

In Algebra III, we studiedd groups, rings (& fields), and modules (& vector spaces). In this class, we consider *composite* theories, i.e. interactions between these objects. We'll spend time on representation theory (groups $\leftrightarrow$ vector spaces) and Galois theory (fields $\leftrightarrow$ groups).

I Representation Theory

We can understand a group G by seeing how it acts on various objects (e.g. a set).

A *linear representation* of a finite group G is a vector space V over a field $\mathbb{F}$ equipped with a group action DEF 1.1

$$G \times V \to V$$

that respects the vector space, i.e. $m_g : V \to V$ with $m_g(v) = gv$ being a linear transformation. We make the following assumptions unless otherwise stated:

1. G is finite.
2. V is finite dimensional.
3. $\mathbb{F}$ is algebraically closed and of characteristic 0 (e.g. $\mathbb{F} = \mathbb{C}$).

Since V is a G-set, $\rho : G \to \mathrm{Aut}_{\mathbb{F}}(V)$ which sends $g \mapsto m_g$ is a homomorphism. Relatedly, if $\dim(V) < \infty$, then $\rho : G \mapsto \mathrm{Aut}_{\mathbb{F}}(V) = \mathrm{GL}_n(\mathbb{F})$.

The *group ring* $\mathbb{F}[G]$ is a (typically) non-commutative ring consisting of all finite linear combinations $\{\sum_{g\in G} \lambda_g g : \lambda_g \in \mathbb{F}\}$. It's endowed with the multiplication rule DEF 1.2

$$\left(\sum_{g\in G} \alpha_g g\right)\left(\sum_{h\in G} \beta_h h\right) = \sum_{g,h\in G\times G} \alpha_g \beta_h (gh)$$

where, in particular, $(\sum \lambda_g g)v = \sum \lambda_g (gv)$. Then, instead of viewing a representation V as a vector space over $\mathbb{F}$ with the additional group action $G \times V \to V$, we can simply view it as a module over the group ring $\mathbb{F}[G]$.

A representation V of G is *irreducible* if there is no G-stable, non-trivial subspace $W \subsetneq V$. This definition is somewhat analogous to transitive G-sets. Note, however, that V can never be a transitive G-set, since $g0 = 0\ \forall g$ is an orbit. DEF 1.3

By G-stable, we mean $gw \in W\ \forall w \in W, g \in G$

E.G. 1.1

Eg. 1 Let $G = \mathbb{Z}_2 = \{1, \tau\} : \tau^2 = 1$. If V is a representation of G, then V is determined by $\rho : G \to \mathrm{Aut}_{\mathbb{F}}(V)$, i.e. $\rho(\tau) \in \mathrm{Aut}_{\mathbb{F}}(V)$. What are the eigenvalues of $\rho(\tau)$? It's minimal polynomial must divide $x^2 - 1 = (x-1)(x+1)$.

Supposing $2 \neq 0$ in $\mathbb{F}$, we have

$$V = V_+ \oplus V_- \qquad V_+ = \{v \in V : \tau v = v\}, V_- = \{v \in V : \tau v = -v\}$$

V is then irreducible $\iff$ $(\dim(V_+), \dim(V_-)) = (1,0)$ or $(0,1)$, as otherwise we could take either V_+ or V_- as nontrivial G-stable subspaces.

Eg. 2 Let $G = \{g_1, ..., g_N\}$ be a finite abelian group. Let $\mathbb{F}$ be algebraically closed with characteristic 0 (e.g. $\mathbb{F} = \mathbb{C}$). If V is a representation of G, then $T_1, ..., T_N$ with $T_i = \rho(g_i) \in \mathrm{Aut}_{\mathbb{F}}(V)$ commute with eachother.

By complex, we mean (a vector space over) an algebraically closed field with characteristic 0.

1.1 Finite Abelian Representation

If G is a finite abelian group, and V is irreducible representation of G over a complex field, then $\dim(V) = 1$.

PROOF. $G = \{g_1, ..., g_N\}$. Then consider $\rho : G \to \mathrm{Aut}(V)$, and let $T_j : V \to V = \rho(g_i)$. Then, T_j and T_i pairwise commute (since G is abelian). $T_1, ..., T_N$ have a simultaneous eigenvector v by Prop 1.1. Hence, $\mathrm{span}(\{v\})$ is a G-stable subspace. Since V is irreducible, we conclude $V = \mathrm{span}(\{v\})$. □

PROP 1.1 If $T_1, ..., T_N$ is a collection of linear transformations on a complex vector space, then they have a simultaneous eigenvector, i.e. $\exists v : T_j v = \lambda_j v \ \forall j$.

PROOF. By induction. Consider T_1. Since $\mathbb{F}$ is complex, its minimal polynomial has a root λ, which is precisely an eigenvalue. Hence, an eigenvector exists.

$n \to n+1$. Let λ be an eigenvalue for T_{N+1}. Consider $V_\lambda := \mathrm{Eig}_{T_{N+1}}(\lambda)$, the eigenvectors for λ. We claim that T_j maps $V_\lambda \to V_\lambda$, i.e. V_λ is T_j-stable. For this, we have $T_{N+1} T_j v = T_j T_{N+1} v = \lambda T_j v$, so $T_j v \in V_\lambda$.

By induction hypothesis, there is a simultaneous eigenvector v in V_λ for $T_1, ..., T_N$. (Thinking of T_j as a linear transformation $V_\lambda \to V_\lambda$ via its restriction). □

E.G. 1.2

Eg. 1 Let $G = S_3$ and $\mathbb{F}$ be arbitrary with $2 \neq 0$. Then consider $\rho : G \to \mathrm{Aut}_{\mathbb{F}}(V)$, an irreducible representation. What is $T = \rho((23))$? $T^2 = I$, so T is diagonalizable with eigenvalues in $\{1, -1\}$.

Case 1: -1 is the only eigenvalue of T. Then (23) acts as $-I$. Since (23) and $(12), (13)$ are conjugate, $(12), (13)$ act as $-I$ as well (since $-I, I$ commute with everything). What about $\rho(123)$? This is $\rho((13)(12)) = \rho(13)\rho(12) = (-I)^2 = I$. Hence, all order 3 elements act as I. We conclude that $\rho(g) = \mathrm{sgn}(g)$ (i.e. 0 for even, 1 for odd permutations).

Case 2: 1 and -1 are eigenvalues of T. Consider the action of S_3 on 3 elements $\{e_1, e_2, e_3\}$, where $\sigma e_i = e_{\sigma(i)}$. This provides a natural representation homomorphism for $V = \mathrm{span}(e_1, e_2, e_3)$.

$\hookrightarrow$ *Case 2a:* $w = e_1 + e_2 + e_3$ is fixed under the action of S_3, so $W = \mathrm{span}(w) \subset$

V is a G-stable subspace. If $W = V$, then $\rho(\sigma) = \text{Id}$.

$\hookrightarrow$ *Case 2b:* We may split $V = W \oplus W^{\perp}$, i.e. W and $\{v : v \bullet w = 0\}$, i.e. $\{\alpha_1 e_1 + \alpha_2 e_2 + \alpha_3 e_3 : \alpha_1 + \alpha_2 + \alpha_3 = 0, \alpha_i \in \mathbb{F}\} = \text{span}(e_1 - e_2, e_2 - e_3)$. Then $W^{\perp}$ is G-stable, and provides a 2-dim representation

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

$$(123) \leftrightarrow \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \qquad (132) \leftrightarrow \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$$

There are essentially 3 distinct, irreducible representations of S_3:

1. $\text{sgn} : S_3 \to \{1, -2\}$
2. Id
3. A 2-dim representation

If V_1, V_2 are two representations of a group G, a *G-homomorphism* from V_1 to V_2 is a linear map $\varphi : V_1 \to V_2$ which is compatible with the action on G, i.e. $\varphi(gv) = g\varphi(v)\ \forall g \in G, v \in V_1$. DEF 1.4

If a G-homomorphism $\varphi : V_1 \to V_2$ is a vector space isomorphism, then we say two V_1 and V_2 are *isomorphic* as representations. DEF 1.5

E.G. 1.3

Eg. 1 Consider $G = D_8$, the symmetries of a square. We may label this group $G = \{1, r, r^2, r^3, V, H, D_1, D_2\}$. We want to think up some representation $\rho : D_8 \to \text{Aut}_{\mathbb{F}}(V)$, where $2 \neq 0$ by assumption.

Consider r^2. It commutes with everything. Then $T = \rho(r^2) \in \text{Aut}_{\mathbb{F}}(V)$ is an order 2 element, so $T^2 = I$. Since $2 \neq 0$, $V = V_+ \oplus V_-$, where $V_+ = \{v : Tv = v\}$ and $V_- = \{v : Tv = -v\}$.

We claim that V_+ and V_- are both preserved by any $g \in D_8$. Take $v \in V_+$. Then $Tgv = r^2 gv = gr^2 v = gTv = gv$. The result follows similarly for $v \in V_-$. Hence, if V is an irreducible representation, then either $V = V_+$ or $V = V_-$, i.e. $\rho(r^2) = I$ or $-I$.

Case 1: $\rho(r^2) = I$, so ρ is not injective, and $\ker(\rho) \supseteq \text{span}(1, r^2)$. Then $D_8/\ker(\rho) \hookrightarrow K_4$. We can write the following, then:

$$\begin{tikzcd} D_8 \arrow[rr, "\rho"] \arrow[dr, hook, "\pi"'] & & \text{Aut}_{\mathbb{F}}(V) \\ & K_4 \arrow[ur, "\varphi"'] & \end{tikzcd}$$

Since $2\mathbb{Z} \times 2\mathbb{Z} = K_4$ is abelian, we have 4 1-dim irreducible representations φ into $\mathrm{Aut}(V)$. (Why 4? Later we'll learn that the number of conjugacy classes coincide with the number of irreducible representations). Hence, we compose with π to yield these for D_8.

Case 2: $\rho(r^2) = -I$. We claim that $\rho(H)$ has both eigenvalues -1 and 1. If $\rho(H) = I$, then $\rho(V) = \rho(r^2 H) = -I$. But we also have $V = rHr^{-1}$, so $\rho(rHr^{-1}) = \rho(r)\rho(H)\rho(r^{-1}) = I \implies \lightning$. We draw a similar contradiction by taking $\rho(H) = -I$. Hence, H has both eigenvalues, so $\dim(V) \geq 2$.

Let $v_1, v_2 \in V$ be such that $Hv_1 = v_1$ and $v_2 = rv_1$. We claim that $\mathrm{span}(v_1, v_2)$ is preserved by D_8, and hence $\mathrm{span}(v_1, v_2) = V$.

Consider $r \in D_8$. We know $rv_1 = v_2$ and $rv_2 = r^2 v_1 = -v_1$, so $\{1, r, r^2, r^3\}$ preserve $\mathrm{span}(v_1, v_2)$.

Consider $H \in D_8$. $Hv_1 = v_1$ by construction. Also, $Hv_2 = Hrv_1 = r^{-1}Hv_1 = r^{-1}v_1 = r^3 v_1 = r^2 v_2 = -v_2$. Hence, H composed with $\{1, r, r^2, r^3\}$, i.e. the whole group D_8 preserve $\mathrm{span}(v_1, v_2)$, as desired.

$$H \leftrightarrow \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad r \leftrightarrow \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{(the rest follow by composition)}$$

Some questions to consider:

1. Can we describe *all* irreducible representations of G up to isomorphism?
2. How is a general representation of G made up of irreducible representations?

PROP 1.2 If V_1, V_2 are representations of G, then $V_1 \oplus V_2$ is also a representation of G, with $g(v_1, v_2) = (gv_1, gv_2)$. It has dimension $\dim(V_1) + \dim(V_2)$.

1.2 Maschke's Theorem

Any representation of a finite group G over a complex field can be expressed as a direct sum of irreducible representations.

PROOF. Let V be a representation of G. Let W be a proper sub-representation of G in V. Let W' be the G-stable complementary subspace such that $V = W \oplus W'$, as in Thm 1.3. Then $\dim(W), \dim(W') < n$. We proceed by induction, relying on this lessening of dimension. □

Remark 1: this is analogous to "every G-set is a disjoint union of transitive G-sets." However, this is a trivial result, but Maschke's is not.

Remark 2: generally, to prove counterexamples to Maschke's when its conditions are loosened, we find an irreducible sub-representation W of some fixed representation

V, and show that any other G-stable subspace necessarily contains W (hence, no decomposition exists).

Remark 3: the assumption $|G| < \infty$ is essential. As a counterexample, take $(\mathbb{Z}, +)$ and $\rho : G \to \mathrm{GL}_2(\mathbb{C}) = \rho(n) = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$, i.e. $ne_1 = e_1$ and $ne_2 = ne_1 + e_2$. Note that the line $\mathrm{span}(e_1)$ is a G-stable subspace, i.e. an irreducible sub-representation of V. Are there any other invariant lines? Take $ae_1 + be_2$. WLOG assume $b = 1$. Consider $W = G(ae_1 + e_2)$. Then $1 \cdot (ae_1 + e_2) = (1 + a)e_1 + e_2 \in W$, so $e_1 \in W$ $\lightning$.

Remark 4: $\mathbb{C}$ is necessary. Let $F = \mathbb{Z}/3\mathbb{Z}$, $G = S_3$. Then let V be the 3-dim representation given by the natural action of S_3 on $\{e_1, e_2, e_3\}$ over F. Then $\mathrm{span}(e_1 + e_2 + e_3)$ is a 1-dim irreducible sub-representation. Let W be any G-stable subspace of V. Then $\exists a, b, c$, not all equal, with $ae_1 + be_2 + ce_3 \in W$. Multiplying by (123), $ce_1 + ae_2 + be_3 \in W$, and once more by (132) yields $be_1 + ce_2 + ae_3 \in W$. Hence, $(a + b + c)(e_1 + e_2 + e_3) \in W$, so $\mathrm{span}(e_1 + e_2 + e_3) \subseteq W$. (Let $\gamma = a + b + c$. Since 3 is prime, $\exists k : k\gamma = 1$ in F).

1.3 Semi-Simplicity of Representations

Let V be a representation of a finite group G above a complex field. Let $W \subseteq V$ be a sub-representation. Then W has a G-stable complement W' such that $V = W \oplus W'$.

PROOF.

Consider the standard projection $\pi_0 : V \to W$ with $\pi_0^2 = \pi_0$, $\mathrm{Im}(\pi_0) = W$. Let $\ker(\pi) = W_0'$. Then we can write $V = W \oplus W_0'$. However, we have no guarantee that W_0' is G-stable. We alter π by replacing it with

$$\pi = \frac{1}{\#G} \sum_{g \in G} \rho(g) \circ \pi_0 \circ \rho(g)^{-1}$$

Some properties of π:

1. $\pi \in \mathrm{End}_{\mathbb{C}}(V)$.
2. π is a projection onto W. See that

$$\pi^2 = \left(\frac{1}{\#G} \sum_{g \in G} g\pi_0 g^{-1} \right) \left(\frac{1}{\#G} \sum_{h \in G} h\pi_0 h^{-1} \right) = \frac{1}{\#G^2} \sum_{g,h \in G} g\pi_0 g^{-1} h\pi_0 h^{-1}$$

   where, by writing g (or h), we mean its linear representation in V. Note that $\pi_0 h^{-1}$ sends any $v \in V$ to a vector in W. Since W is G-invariant, $g^{-1}h\pi_0 h^{-1}$ also sends v to W. But now the next π_0 acts as the identity (since we're already in W). Hence, the above summand reduces to $h\pi_0 h^{-1}$, and we may write

$$\pi^2 = \frac{1}{\#G^2} \sum_{g,h \in G} h\pi_0 h^{-1} = \frac{1}{\#G} \sum_{h \in G} h\pi_0 h^{-1} = \pi$$

3. $\operatorname{Im}(\pi) = W$. $\operatorname{Im}(\pi) \subseteq W$. But let $w \in W$. Then $\pi(w) = w$ (check it).
4. $\pi(hv) = h\pi(v)\ \forall h \in G$. See that

$$\pi(hv) = \frac{1}{\#G} \sum_{g \in G} g\pi g^{-1} hv = \frac{1}{\#G} \sum_{g \in G} g\pi(h^{-1}g)^{-1} v$$

Now, let $\tilde{g} = h^{-1}g$. Then $g = h\tilde{g}$, and we write

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

We can now take $W' = \ker(\pi)$ and write $V = W \oplus W'$. We have that W' is G-stable, now, since $w \in W' \implies \pi(gw) = g\pi(w) = g0 = 0 \implies gw \in W'$. □

We'll now give a second proof of Thm 1.2. Consider

DEF 1.6 A *Hermitian inner product* of V is a Hermitian, bilinear mapping

$$V \times V \to \mathbb{C}$$

satisfying $\langle v_1 + v_2, w \rangle = \langle v_1, w \rangle + \langle v_2, w \rangle$ and $\langle \lambda v, w \rangle = \lambda \langle v, w \rangle$. On the second coordinate, we have $\langle v, w_1 + w_2 \rangle = \langle v, w_1 \rangle + \langle v, w_2 \rangle$ and $\langle v, \lambda w \rangle = \overline{\lambda} \langle v, w \rangle$. The skew linearity in the second argument allows us to conclude $\langle v, v \rangle \in \mathbb{R}^{\geq 0}$ and $\langle v, v \rangle = 0 \iff v = 0$.

One can think of $\langle v, v \rangle$ as the square of the "length" of v.

1.4 Special Hermitian Pairing

If V is a complex representation of a finite group G, then there is a Hermitian inner product on V such that

$$\langle gv, gw \rangle = \langle v, w \rangle \quad \forall g \in G \quad \text{and} \quad v, w \in V$$

PROOF. Let $\langle\ ,\ \rangle_0$ be an arbitrary Hermitian inner product on V. To do so, choose a basis $(e_1, ..., e_n)$ be a complex basis for V, and define

$$\left\langle e_i, e_j \right\rangle_0 = 0 \text{ if } i \neq j, 1 \text{ o.w.}$$

Then $\left\langle \sum_{i=1}^n \alpha e_i, \sum_{i=1}^n \beta e_i \right\rangle = \alpha_1 \overline{\beta_1} + ... + \alpha_n \overline{\beta_n} \in \mathbb{C}$. Similar to the proof for Thm

1.3, we will take an average. Consider another inner product

$$\langle v, w\rangle = \frac{1}{\#G}\sum_{g\in G}\langle gv, gw\rangle_0$$

This has some nice properties. In particular, $\langle\cdot,\cdot\rangle$ is Hermitian linear, positive definite, and G-equivalent.

We'll verify positiveness:

$$\langle v, v\rangle = \frac{1}{\#G}\sum_{g\in G}\underbrace{\langle gv, gv\rangle_0}_{\geq 0} \geq 0$$

Suppose $\langle v, v\rangle = 0$. Then $\sum_{g\in G}\langle gv, gv\rangle_0 = 0$, so $\langle gv, gv\rangle_0 = 0\ \forall g \in G$. In particular, for $g = 1$, $\langle v, v\rangle_0 = 0 \iff v = 0$.

And to verify G-equivariant, we have $\langle hv, hw\rangle = \langle v, w\rangle$. □

PROOF OF 1.2

We provide a new angle to proving Thm 1.2. If W is a sub-representation, let $W^\perp = \{v \in V : \langle v, w\rangle = 0\}$ over the Hermitian inner product outlined in Thm 1.4.

Then we may write $V = W \oplus W^\perp$. The G-stability of $W^\perp$ follows from equivariance of the inner product. Let $w \in W, v \in W^\perp \implies \langle gv, w\rangle = \left\langle v, g^{-1}w\right\rangle = 0 \implies gv \in W^\perp$.

This "semi-simple" structure of representations is a rare sight: abelian groups, and especially groups generally, are not necessarily made of irreducible components.

We narrow our previous 2 questions with 2 more:

1. Given G, produce the complete list of its irreducible representations (up to isomorphism).
2. Given a general, finite dimensional representation V of G, generate
$$V = V_1^{m_1} \oplus V_2^{m_2} \oplus \ldots \oplus V_t^{m_t} \qquad V_i \text{ irreducible}$$

If V and W are two G-representations, we may investigate $\mathrm{Hom}_G(V, W) = \{T : T \to W : T \text{ linear s.t. } T(gv) = gT(v)\}$. Note that $\mathrm{Hom}_G(V, W)$ is a $\mathbb{C}$-vector space.

1.5 Schur's Lemma

Let V, W be irreducible representations of G. Then

$$\mathrm{Hom}_G(V, W) = \begin{cases} 0 & V \ncong W \\ \mathbb{C} & V \cong W \end{cases}$$

where $\mathrm{Hom}_G(V, W)$ is the space of G-equivariant linear transformations.

PROOF. Suppose that $V \ncong W$, and let $T \in \mathrm{Hom}_G(V, W)$. $\ker(T) \subseteq V$ is a sub-representation of G, since $v \in \ker(T) \implies T(gv) = gT(v) = 0$. Hence, since V is irreducible, $\ker(T)$ may be trivial or V itself. If it were trivial, then $\mathrm{Im}(T) \cong V$. But $\mathrm{Im}(T) \subseteq W$, so by irreducibility of W we yield a contradiction. Hence, $\ker(T) = V$, so $T = 0$.

Suppose that $V \cong W$. Let $T \in \mathrm{Hom}_G(V, W) = \mathrm{End}_G(V)$. Since $\mathbb{C}$ is algebraically closed, T has an eigenvalue λ. Then $T - \lambda I \in \mathrm{End}_G(V)$. $\ker(T - \lambda I)$ is a non-trivial sub-representation of V, and hence $\ker(T - \lambda I) = V \implies T = \lambda I$. □

PROP 1.3 Let V decompose as

$$V = V_1^{m_1} \oplus \cdots \oplus V_t^{m_t}$$

As a corollary, we see that $m_j = \dim_{\mathbb{C}} \mathrm{Hom}_G(V_j, V)$.

PROOF. Unwrap $V_i^{m_i}$ into m_i copies of V_i, and label $1, ..., s$. Note that $\mathrm{Hom}_G(A, B \oplus C) = \mathrm{Hom}_G(A, B) \oplus \mathrm{Hom}_G(A, C)$.

$$\mathrm{Hom}_G(V_j, V) = \mathrm{Hom}_G(V_j, V_1 \oplus ... \oplus V_s) = \bigoplus_{i \in I} \mathrm{Hom}(V_j, V_i) : V_i \cong V_j \ \forall i \in I$$

$$= \underbrace{\mathbb{C} \oplus ... \oplus \mathbb{C}}_{|I| = m_j \text{ times}} \implies \dim \mathrm{Hom}_G(V_j, V) = m_j \quad \square$$

DEF 1.7 For an endomorphism $T : V \to V$, the *trace*, $\mathrm{tr}(T)$, is defined as $\mathrm{tr}([T]_\beta)$, where β is some basis. This is well-defined, since basis representations $[T]_\alpha, [T]_\beta$ are conjugate, and trace is a conjugate-invariant function.

PROP 1.4 Let $W \subseteq V$ be a subspace and π be a function $V \to W$ such that $\pi^2 = \pi$ and $\mathrm{Im}(\pi) = W$. Then $\mathrm{tr}(\pi) = \dim(W)$.

PROOF. Let $v_1, ..., v_d$ be a basis for W and $v_{d+1}, ..., d_n$ be a basis for $\ker(\pi)$. Then, since we can write $V = W \oplus \ker(\pi)$ (recall projection properties), $\beta = d_1, ..., d_n$ is a basis for V. In this basis, $\pi(v_i) = v_i$ for $1 \le i \le d$. Hence

$$[\pi]_\beta = \begin{pmatrix} \underbrace{\boxed{\begin{matrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{matrix}}}_{d} & \cdots \\ \vdots & \ddots \end{pmatrix}$$

As for the rest of the matrix, $\pi(v_i)$ for $i > d$ will be mapped to a linear combination of basis vectors $v_i : i \le d$, so, in particular, they will not have diagonal 1 entries. Since $d = \dim(W)$, we conclude $\mathrm{tr}(\pi) = \dim(W)$. □

Define $V^G = \{v \in V : gv = v \forall g \in G\}$ to be the members of V fixed by G. DEF 1.8

Remark that $V^G = \cap_{g \in G}$ (1-eigenspaces for $\rho(g)$)

1.6 Burnside

If V is a complex representation of a finite G, then

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

PROOF.

By Prop 1.4, for a projection $\pi : V \to W$ (i.e. $\mathrm{Im}(\pi) = W, \pi^2 = \pi$), we have $\mathrm{tr}(\pi) = \dim(W)$. Consider

$$\pi := \frac{1}{\#G} \sum_{g \in G} \rho(g) \in \mathrm{End}_{\mathbb{C}}(V)$$

Note that $\mathrm{Im}(\pi) \subseteq V^G$. Let $h \in G$ and $v \in V$. Then

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

Conversely, if $v \in V^G$, then $\pi(v) = v$. Hence, $V^G = \mathrm{Im}(\pi)$ exactly. This also shows that $\pi^2(v) = \pi(v)$. We conclude that π projects $V \to V^G$.

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

□

Thm 1.6 $\implies$ Burnside's Lemma. **PROP 1.5**

PROOF.

Consider later. □

CHARACTERS

If V is a finite dimensional, complex representation of G, then the *character* of V is the function $\chi_V : G \to \mathbb{C}$ with $\chi_V(g) = \mathrm{tr}(\rho(g))$. DEF 1.9

χ_V is constant on conjugacy classes, i.e. $\chi_V(hgh^{-1}) = \chi_V(g)$. **PROP 1.6**

PROOF.

$\mathrm{tr}(\rho(hgh^{-1})) = \mathrm{tr}(\rho(h)\rho(g)\rho(h)^{-1}) = \mathrm{tr}(\rho(g))$ □

E.G. 1.4

Eg. 1 Let $G = S_3$. We discovered 3 distinct representations of S_3: the trivial action; the sgn function $\rho(g) = \mathrm{sgn}(g)$; and the two-dimensional representation given by

$$\mathrm{Id} \leftrightarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad (12) \leftrightarrow \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad (13) \leftrightarrow \begin{pmatrix} -1 & 0 \\ -1 & 1 \end{pmatrix} \qquad (23) \leftrightarrow \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix}$$

$$(123) \leftrightarrow \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \qquad (132) \leftrightarrow \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$$

Denote these representations by "triv," "sgn," and 2, respectively. The conjugacy classes and associated traces are given by

	1	(12)	(123)
χ_{triv}	1	1	1
χ_{sgn}	1	−1	1
χ_2	2	0	−1

Eg. 2 Recall $G = D_8 = \{1, r, r^2, r^3, V, H, D_1, D_2\}$. We have 4 1-dim irreducible representations given by $D_8/\langle 1, r_2 \rangle = \mathbb{Z}_2 \times \mathbb{Z}_2$, including the trivial one. Denote these by $\chi_{\mathrm{triv}}, \ldots, \chi_4$. We also have the unique 2-dim irrep, $2D$, given by

$$\mathrm{Id} \leftrightarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad r \leftrightarrow \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad r^2 \leftrightarrow \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \quad r^3 \leftrightarrow \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

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

	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_{2D}	2	−2	0	0	0

From these two examples, it seems that the number of irreducible representations coincides with the number of conjugacy classes $h(G)$ of G (also called the *class number* of G). It *also* seems that the sum of squares of the rows, weighted by class size, is the cardinality of the group. Even more! The row look orthogonal. To that end, we conjecture:

$$\frac{1}{\#G} \sum_{g \in G} \chi_i(g) \chi_j(g) = \delta_{ij}$$

Eg. 3 The Monster Group, $\#G \approx 8 \cdot 10^{53}$, has a smallest non-trivial representation of dimension $d = 196,883$. ρ_V then is given as a collection of $8 \cdot 10^{53}$ $196,883 \times 196,883$ matrices. This is too much information to ever contain in a computer. However, G has only 194 conjugacy classes, and so χ_V, with 194 complex numbers, defines V.

PROP 1.7 $\chi_V(\text{triv}) = \dim(V)$

PROP 1.8 Given representations V and W, $\text{Hom}_G(V,W) = \text{Hom}(V,W)^G$, where we view $\text{Hom}(V,W)$ as a representation with the action $gT = g \circ T \circ g^{-1}$.

PROOF. Let $T \in \text{Hom}_G(V,W)$. Then $gT(v) = gTg^{-1} = gT(g^{-1}v) = T(gg^{-1}v) = T(v)$, so $T \in \text{Hom}(V,W)^G$.

Conversely, let $T \in \text{Hom}(V,W)^G$. Then $g^{-1}T(v) = g^{-1}T(g(v)) = T(v) \implies T(g(v)) = gT(v)$, so $T \in \text{Hom}_G(V,W)$. □

PROP 1.9 Given two G-representations V, W, then $V \oplus W$ is a representation with $g(v,w) = (gv, gw)$. Then

$$\chi_{V \oplus W} = \chi_V + \chi_W$$

PROP 1.10 Linear representations of finite groups are diagonalizable over $\mathbb{C}$.

PROOF. Fix $g \in G$. To be diagonalizable, $\rho(g)$'s minimal polynomial must split into distinct factors in $\mathbb{C}$. Since G is finite, $g^{|G|} = \mathbb{1}$, so $\rho(g)^{|G|} = \mathbb{1}$, so in particular $T = \rho(g)$ satisfies $x^{|G|} - 1$. We conclude $p_T | x^{|G|} - 1$. But, in $\mathbb{C}$, $x^{|G|} - 1$ splits into distinct factors, so p_T must as well. □

1.7 Character of Hom(V, W)

$$\chi_{\text{Hom}(V,W)} = \overline{\chi_V}\chi_W$$

PROOF. Let $g \in G$. Let $e_1, \dots, e_m$ be a basis of eigenvectors for $\rho_V(g)$, with $m = \dim(V)$, and $ge_i = \alpha_i e_i$. Similarly, let $f_1, \dots, f_n$ be a basis of eigenvectors for $\rho_W(g)$, with $gf_j = \beta_j f_j$. Then $\chi_V(g) = \sum_{i=1}^m \alpha_i$ and $\chi_W(g) = \sum_{j=1}^n \beta_j$.

Let $T_{ij} \in \text{Hom}(V,W)$, where $1 \le i \le m$ and $1 \le j \le n$, be the following

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

We claim that T_{ij} is a basis for $\mathrm{Hom}(V,W)$. We have

$$\begin{aligned}(gT_{ij})(e_k) &= gT(g^{-1}e_k) = gT(\lambda_k^{-1}e_k) = \lambda_k^{-1}gT_{ij}e_k \\ &= \lambda_k^{-1}\begin{cases}0 & j \neq i \\ \lambda_k^{-1}\beta_i f_j & j = i\end{cases} \implies gT_{ij} = \lambda_j^{-1}\beta_j T_{ij}\end{aligned}$$

Hence, $gT_{ij} = \alpha_i^{-1}\beta_j T_{ij}$. We have that $\rho_{\mathrm{Hom}(V,W)}(g)$ is a $mn \times mn$ matrix with entires $\{\alpha_i^{-1}\beta_j\}_{j\in[m],j\in[n]}$, so

$$\chi_{\mathrm{Hom}(V,W)}(g) = \sum_{\substack{1\le i\le m \\ 1\le j\le n}} \alpha_i^{-1}\beta_j = \left(\sum_{i=1}^m \alpha_i^{-1}\right)\left(\sum_{j=1}^n \beta_j\right) = \left(\sum_{i=1}^m \overline{\alpha_i}\right)\left(\sum_{j=1}^n \beta_j\right)$$

since α_i are roots of unity. But this is $\overline{\chi_V(g)}\chi_W(g)$ □

Orthogonality of Irreducible Group Characters

Let $V_1, \ldots, V_t$ be a complete list of distinct, irreducible representations of G. Call $\chi_1, \ldots, \chi_t : G \to \mathbb{C}$ the associated characters.

DEF 1.10 $\chi_j \in L^2(G)$, the space of square integrable functions on G. Given $f_1, f_2 \in L^2(G)$, let $\langle f_1, f_2\rangle = \frac{1}{\#G}\sum_{g\in G}\overline{f_1(g)}f_2(g)$. This is indeed an inner product.

1.8 Orthogonality of Characters

Let χ_i, χ_j be irreducible characters of G. Then

$$\langle \chi_i, \chi_j\rangle = \begin{cases}0 & i \neq j \\ 1 & i = j\end{cases}$$

PROOF.

$$\begin{aligned}\langle \chi_i, \chi_j\rangle &= \frac{1}{\#G}\sum_{g\in G}\overline{\chi_i(g)}\chi_j(g) \\ &= \frac{1}{\#G}\sum_{g\in G}\chi_{\mathrm{Hom}(V_i,V_j)}(g) && \text{by Thm 1.7} \\ &= \dim_{\mathbb{C}}(\mathrm{Hom}(V_i,V_j)^G) && \text{by Thm 1.6} \\ &= \dim_{\mathbb{C}}(\mathrm{Hom}_G(V_i,V_j)) = \dim_{\mathbb{C}}\begin{cases}\mathbb{C} & i = j \\ 0 & o.w.\end{cases} && \text{by Thm 1.5} \\ &= \begin{cases}1 & i = j \\ 0 & o.w.\end{cases} \quad \square\end{aligned}$$

$\chi_1, ..., \chi_t$ is an orthonormal system of vectors in $L^2(G)$. **PROP 1.11**

PROOF. Follows immediately from Thm 1.8. □

$\chi_1, ..., \chi_t$ are linearly independent, and $t \le \#G$. **PROP 1.12**

PROOF. Orthonormal systems are linearly independent. $L^2(G) \cong \mathbb{C}^{\#G}$, so $t \le \dim(L^2(G)) = \dim(\mathbb{C}^{\#G}) = \#G$. □

$t \le h(G)$, the number of conjugacy classes of G. **PROP 1.13**

PROOF. $L^2_{\text{class}}(G) \subseteq L^2(G)$, where $L^2_{\text{class}}(G) = \{f : G \to \mathbb{C} : f(hgh^{-1}) = f(g)\}$. The dimension of this space is $h(G)$. □

E.G. 1.5

Eg. 1 $G = S_3$ (see Example 1.2), we had $t = 3$, with the dimensions of the first and second representations $d_1 = d_2 = 1$, and $d_3 = 2$. $h(G) = 3$ is hence a tight bound.

Eg. 2 $G = D_8$ (see Example 1.3), we had $t = 5$ with $d_1 = ... = d_4 = 1$ and $d_5 = 2$. Once again $t = h(G)$.

1.9 Character Characterizes Representations

If V and W are two complex representations of G, then V is isomorphic to W as a representation $\iff \chi_V = \chi_W$.

PROOF. If $V \cong W$, then let $\varphi : V \to W$ be a G-equivariant isomorphism. ${\rho_V}_g(v) = \varphi^{-1}{\rho_W}_g\varphi(v)$. But trace is conjugate-invariant, so $\chi_V(g) = \chi_W(g)$.

Conversely, assume $\chi_V = \chi_W$, and write $V = Z_1^{m_1} \oplus \cdots \oplus Z_t^{m_t}$, $W = Z_1^{n_1} \oplus \cdots \oplus Z_t^{n_t}$. Some $m_i, n_i = 0$, as needed. (In particular, let Z_i encompass all irreducible representations between V and W, shared or otherwise).

$$\chi_V = m_1\chi_1 + ... + m_t\chi_t \qquad \chi_W = n_1\chi_1 + ... + n_t\chi_t$$

Observe then that $\langle \chi_V, \chi_j \rangle = m_j$ and $\langle \chi_W, \chi_j \rangle = n_j$. But $\chi_V = \chi_W$, so $m_i = n_i$, and we are done. □

Regular Representations of G

In Prop 1.13, we argued that, for characters $\chi_1, ..., \chi_t$, $t \le h(G)$, the class number of G, by seeing that $\{\chi_1, ..., \chi_t\} \subseteq L^2_{\text{class}}(G)$. We will prove a converse to this.

DEF 1.11 Consider $\mathbb{C}[G] = \{\sum_{g\in G} \lambda_g g : \lambda_g \in \mathbb{C}\}$. Then $G \circlearrowright \mathbb{C}[G]$ by left multiplication. We call $\mathbb{C}[G]$ the *regular representation*, and denote $V_{\text{reg}} = \mathbb{C}[G]$.

PROP 1.14

$$\chi_{V_{\text{reg}}}(g) = \#\{h \in G : gh = h\} = \begin{cases} \#G & g = 1 \\ 0 & o.w. \end{cases}$$

PROOF. Consider $\rho(g)$. $\mathbb{C}[G]$ has a basis $\{g_1, ..., g_n\} = \#G$. Hence, $\text{tr}(\rho(g)) = \#\{h \in G : gh = h\}$. If $g = \mathbb{1}$, this is clearly all of G. Otherwise, we cannot have $gh = h$ (or else $g = \mathbb{1}$). $\square$

PROP 1.15 Every irreducible representation of G occurs in V_{reg} with multiplicity equal to its dimension, i.e. if $d_j = \dim_{\mathbb{C}}(V_j)$, then

$$V_{\text{reg}} = V_1^{d_1} \oplus \cdots \oplus V_t^{d_t}$$

PROOF. We write $V_{\text{reg}} = V_1^{m_1} \oplus \cdots \oplus V_t^{m_t}$, where m_i may be 0. Then

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

PROP 1.16 We conclude $\#G = d_1^2 + ... + d_t^2$.

PROOF.

$$\begin{aligned} \dim(V_{\text{reg}}) = \#G &= \dim(V_1^{\dim(V_1)} \oplus \cdots \oplus V_t^{\dim(V_t)}) \\ &= \dim(V_1)\dim(V_1) + ... + \dim(V_t)\dim(V_t) \qquad \square \end{aligned}$$

1.10 Class Number Coincides With Number of Irreducible Representations

Let t be the number of distinct irreducible representations of G. Let $h(G)$ be the class number of G. Then $t = h(G)$.

PROOF. $\mathbb{C}[G] \cong V_1^{d_1} \oplus \cdots \oplus V_t^{d_t}$. Note that $\mathbb{C}[G]$ is not just a G representation, but a ring under the following multiplication rule:

$$\sum_{g\in G} \alpha_g g \sum_{h\in G} \beta_h h = \sum_{g,h\in G} \alpha_g \beta_h gh$$

We then take $\rho = (\rho_1, ..., \rho_t) = G \to \text{Aut}(V_1) \times \cdots \times \text{Aut}(V_t)$. We can write ρ :

$\mathbb{C}[G] \to \mathrm{End}_{\mathbb{C}}(V_1) \oplus \cdots \oplus \mathrm{End}_C(V_t)$ by linearity, i.e.

$$\sum \lambda_g g \to \left(\sum \lambda_g \rho_1(g), ..., \sum \lambda_g \rho_t(g)\right)$$

Observe that $\dim(\mathbb{C}[G]) = \#G$ and $\dim(\mathrm{End}(V_1) \oplus \cdots \oplus \mathrm{End}(V_t)) = d_1^2 + ... + d_t^2$

We show that ρ is an injective ring homomorphism. Let $\theta = \sum_{g \in G} a_g g \in \ker(\rho)$. Then $\rho_j(\theta) = 0 \implies \theta$ acts as 0 on V_j. Hence θ acts as 0 on all irreducible representation $V_1, ..., V_t$ and hence as 0 on all representations (by Thm 1.2). Finally, then, θ is 0 on $\mathbb{C}[G]$, so in particular $\theta \cdot \sum_{g \in G} a_g g = 0 \implies \theta 1 = 0 \implies \theta = 0$. So ρ is injective.

$\dim(\mathbb{C}[G]) = \dim(\mathrm{End}(V_1) \oplus \cdots \oplus \mathrm{End}(V_t))$, so ρ is also surjective. Hence

$$\mathbb{C}[G] = M_{d_1}(\mathbb{C}) \oplus \cdots \oplus M_{d_t}(\mathbb{C})$$

We compute the centers Z of these rings

$$\dim Z(\mathbb{C}[G]) = \dim\{x = \sum \lambda_g g : x\theta = \theta x \ \forall \theta \in \mathbb{C}[G]\}$$

$$\dim Z(M_{d_1}(\mathbb{C}) \oplus \cdots \oplus M_{d_t}(\mathbb{C})) \cong \dim \mathbb{C} \oplus \cdots \oplus \mathbb{C} = t$$

We claim that $\theta = \sum \lambda_g g \in Z(\mathbb{C}[G]) \iff h\theta = \theta h \ \forall h \in G$, i.e. it is sufficient to show that an element commutes with the group to show commutativity with the group ring. But

$$\begin{aligned}
&\iff \sum \lambda_g hg = \sum \lambda_g gh \\
&\iff \lambda_g(hgh^{-1}) = \sum \lambda_g g \\
&\iff \sum \lambda_{h^{-1}gh} g = \sum \lambda_g g \ \forall h \in G \\
&\iff \lambda_{h^{-1}gh} = \lambda_g \ \forall h \in G, g \in G
\end{aligned}$$

hence, $g \to \lambda_g$ is a class function, so $\dim(Z(\mathbb{C}[G])) = h(G)$. But $\dim(Z(\mathbb{C}[G])) = t$, so we conclude $t = h(G)$. □

ABELIAN GROUPS

If G is abelian, we've seen that all irreducible representations $V_1, ..., V_t$ have dimension 1. From above, $t = h(G)$, but since G is abelian, $t = h(G) = \#G$. A direct proof would look like:

PROOF.

$$G \cong d_1\mathbb{Z} \times \cdots d_r\mathbb{Z} : d_1 | \cdots | d_r$$

by structure theorem. Hence, if ρ is an IRREP of G, then $\rho : G \to \mathrm{Aut}(\mathbb{C}) = \mathbb{C}^\times$. Let G be generated by $\{g_1, ..., g_r\}$, where $g_i^{d_i} = 1$. Then

$$G = \{g_1^{a_1} \cdots g_r^{a_r} : a_i \leq d_i\}$$

ρ is completely determined by the elements $\rho(g_1), ..., \rho(g_r)$. Consider

$$\mu_d = \{\xi \in \mathbb{C}^\times : \xi^d = 1\}$$

Consider now $\mathrm{Hom}(G, \mathbb{C}^\times) = \mu_{d_1} \times \cdots \times \mu_{d_r}$ by

$$\rho \mapsto (\rho(g_1), ..., \rho(g_r))$$

This is a natural isomorphism, where we note that $\mathrm{Hom}(G, \mathbb{C}^\times)$ and $\mu_{d_1} \times \cdots \times \mu_{d_r}$ have group structure. Let $\hat{G} = \{\text{irreducible representations of } G\}$. Then, also, $\hat{G} = \{\text{irreducible characters of } G\}$. As a group, $\hat{G} \cong G$, but we'll see this later (it's not natural). □

FOURIER ANALYSIS

We are primary concerned with

$$L^2(G) = \{\text{square integrable functions from } G \to \mathbb{C}\} \cong \mathbb{C}^{\#G}$$

where

$$\|f\|^2 = \frac{1}{\#G} \sum_{g \in G} |f(g)|^2 < \infty$$

for $g \in L^2(G)$. Note that $L^2(G)$ is a Hilbert space with

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

PROP 1.17 Let $\hat{G} = \{\chi_1, ..., \chi_N\}$ be the irreducible characters for G. Then $\hat{G}$ is an orthonormal basis for $L^2(G)$, and so, for $f \in L^2(G)$, we can write

$$f = \langle \chi_1, f \rangle \chi_1 + ... + \langle \chi_N, f \rangle \chi_N$$

DEF 1.12 Given $f \in L^2(G)$, the function $\hat{f} : \hat{G} \to \mathbb{C}$ defined by

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

is called the *Fourier transform* of f over G.

DEF 1.13 Correspondingly,

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

is called the *Fourier inversion formula*.

E.G. 1.6

Eg. 1 $G = \mathbb{R}/\mathbb{Z}$. Let $L^2(G)$ be the space of $\mathbb{C}$-values period functions on $\mathbb{R}$, i.e. $f(x+1) = f(x)$, which are square integrable on $[0,1]$. Then

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

Then $\hat{G} = \mathrm{Hom}(G, \mathbb{C}^\times)$. Any homomorphism from $\mathbb{R} \to \mathbb{C}^\times$ looks like $x \mapsto e^{\lambda x}$. But we also must satisfy

$$e^{\lambda n} = 1$$

Hence, $\lambda = k2\pi$ for $k \in \mathbb{Z}$. Hence,

$$\hat{G} = \{\chi_j : j \in \mathbb{Z} : \lambda_j(x) = e^{2\pi j x}\} \cong \mathbb{Z}$$

Recall, if G is abelian, then $\mathbb{C}[G]$, the group ring, is commutative. We also have $\mathbb{C}[G] \cong \bigoplus_{\chi \in \hat{G}} \mathbb{C}$ by the map

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

Character tables of S_4 and A_5

Consider S_4

Recall $\# S_4 = 24$ and there are $h = 5$ conjugacy classes. The classes of this group are as follows:

name	rep	size
$1A$	(1)	1
$2A$	$(12)(34)$	3
$2B$	(12)	6
$3A$	(123)	8
$4A$	(1234)	6

and we have the character table (to start):

char	$1A$	$2A$	$2B$	$3A$	$4A$
χ_1	1	1	1	1	1
$\chi_{\mathrm{sgn}} = \chi_2$	1	1	-1	1	-1

It suffices to look at abelian quotients of S_4 to find its 1-dim irreducible representations, hence the normal subgroups of S_4. One can mod out by A_4 to yield the sign homomorphism from $S_4 \to \mathbb{C}^\times$. There are no other abelian quotients, so this is the only 1-dim rep.

A rarity! S_{n-1} is a quotient of S_n only when $n = 4, 3$.

Note that K_4, the Klein 4 group, is naturally embedded in S_4, and also $S_4/K_4 = S_3$. Let φ be this homomorphism. Recall the character table of S_3 from Example 1.4:

	1	(12)	(123)
χ_{triv}	1	1	1
χ_{sgn}	1	−1	1
χ_2	2	0	−1

We compose φ with the 2-dim representation χ_2 above. $2A$ (i.e. (12)(34)) in S_4 is in the kernel of φ, so it will be mapped to the identity, i.e. have trace 2 as well. The image of $2B$ (i.e. transpositions) are exactly transpositions in S_3, and hence we have 0. Order 3 elements in S_4 get mapped to order 3 element in S_3, and hence we maintain -1 as the trace. Lastly, $4A$ becomes a transposition.

char	$1A$	$2A$	$2B$	$3A$	$4A$
χ_1	1	1	1	1	1
$\chi_{\text{sgn}} = \chi_2$	1	1	−1	1	−1
χ_3	2	2	0	−1	0

We're still missing 2 representations, since $h = 5$. We have the natural representation given by permuting 4 basis vectors. The trace of these representations is given by how many fixed points a permutation has, i.e. $(1A, 2A, 2B, 3A, 4A) = (4, 0, 2, 1, 0)$. This "natural" representation may be decomposed into the trivial representation and an irreudcible representation. Hence, we subtrace each trace by 1 to yield

char	$1A$	$2A$	$2B$	$3A$	$4A$
χ_1	1	1	1	1	1
$\chi_{\text{sgn}} = \chi_2$	1	1	−1	1	−1
χ_3	2	2	0	−1	0
χ_4	3	−1	1	0	−1

We still need to check that χ_4 is irreducible: for this, we compute $\langle \chi_4, \chi_4 \rangle$, and find that it is 1. To find the 5th representation, we can weasle our way out via number theory. To start, we know the inner product of the columns with themselves is equal to $\#S_4 = 24$, i.e.

$$1 + 1 + 2^2 + 3^2 + \chi_5(1)^2 = 24 \implies \chi_5(1) = 3$$

We could also try taking $\text{Hom}(V_i, V_j)$ for two of our existing representations, and hope it is irreducible. Since $\chi_{\text{Hom}(V_i,V_j)} = \overline{\chi_{V_i}}\chi_{V_j}$, it should be that $\chi_{V_i}(1)\chi_{V_j}(1) = 3$ The trivial representation won't do us any good, so our only valid path forward is $\text{Hom}(V_2, V_4)$. Filling in the character table would yield

char	$1A$	$2A$	$2B$	$3A$	$4A$
χ_1	1	1	1	1	1
$\chi_{\text{sgn}} = \chi_2$	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

One verifies that $\langle \chi_5, \chi_5 \rangle = 1$, so χ_5 is irreducible.

Consider A_5.

It's cardinality is $\#A_5 = 60$ and it has no normal subgroups (hence, the method of finding abelian quotients won't work!). It's conjugacy classes are as follows:

name	rep	size
$1A$	(1)	1
$2A$	$(12)(34)$	15
$3A$	(123)	20
$5A$	(12345)	12
$5B$	(12354)	12

Once again, $h = 5$. Let's start building the character table

#	1	15	20	12	12
char	$1A$	$2A$	$3A$	$5A$	$5B$
χ_1	1	1	1	1	1

We can take the standard permutation representation and subtract off the trivial representation to yield a (hopefully) irreducible representation: $(1A, 2A, 3A, 5A, 5B)$ have $(5, 1, 2, 0, 0)$ fixed points, so:

#	1	15	20	12	12
char	$1A$	$2A$	$3A$	$5A$	$5B$
χ_1	1	1	1	1	1
χ_2	4	0	1	-1	-1

One checks that χ_1, χ_2 are orthogonal, and further that $\langle \chi_2, \chi_2 \rangle = 1$ (for irreducibly). Recall that S_5 acts transitively on $S_5/F_{20} = A_5/D_{10} =: X$, a set of 6 elements. Hence, we can consider how many fixed points of A_5 acting on X exist. Recall that an element $g \in A_5$ fixes a coset $hD_{10} \iff hgh^{-1} \in D_{10}$.

$5A$ On X, a five cycle acts as a five cycle (can you think of any other order 5 element permuting 6 letters?), which has 1 fixed point.

$5B$ Same as above.

$3A$ A 3 cycle does not exist in D_{10}, so no cosets are fixed.

$2A$ One finds two copies of $(12)(34)$ in D_{10}, and hence two fixed cosets.

#	1	15	20	12	12
char	$1A$	$2A$	$3A$	$5A$	$5B$
χ_1	1	1	1	1	1
χ_2	4	0	1	-1	-1
χ_3	5	1	-1	0	0

We have two more representations to weed out. We can figure their dimensions, since $1 + 16 + 25 + d_4^2 + d_5^2 = 60 \implies d_4^2 + d_5^2 = 18 \implies d_4 = d_5 = 3$. Hence, we will search for 3-dim representations.

It is interesting that A_5 acts on 3-dim space... we know that A_5 is the symmetry group of the icosahedron and dodecahedron. Consider $g = 2A$ under the action on one of these objects.

Consider $\mathrm{GL}_3(\mathbb{F}_2)$

Recall some key facts: $\#\mathrm{GL}_3(\mathbb{F}_2) = 168 = 2^3 \cdot 3 \cdot 7$, and it has a Sylow 2 subgroup isomorphic to D_8. We may first consider a trivial representation. Then, typically, we consider the permutation representation of $\mathrm{GL}_3(\mathbb{F}_2)$ on some transitive G-set. But $\mathbb{F}_2^3 \neq 0$ is such a set, and we generate χ_2 by subtracting off the trivial representation.

Then, for χ_3, we consider X, the set of Sylow 7 subgroups. $\#X|24$ and $\#X \equiv_7 1$, so $\#X = 8$. It is not 1, or else we would find a new conjugacy class. As a G set under conjugation, $X \cong G/H$, where H is the normalizer of a Sylow 7 subgroup P_7 (it must have cardinality 21). Then P_7 is, by definition, a normal subgroup of H, so we consider $H/P_7 \cong 3\mathbb{Z}$. Let $\pi : H \to 3/\mathbb{Z}$ be the quotient map. Then $\pi^{-1} = \ker(\pi) = P_7$, and every element which maps to 1 or 2 under this map is of order 3.

Since $3|\mathrm{ord}(g)|21$, and $g^3 \in P_7$

H has 6 elements of order 7, and 14 of order 3 (1 of order 1). Elements of order 2 or 4 in G may not fix any cosets G/H, since then $gaH = aH \implies a^{-1}ga \in H$, and $2, 4 \nmid 21$. Then, if $g \in 7A$, then g acts a cyclic permutation of length 7 on G/H, and therefore has a unique fixed point.

$$\mathbb{C}[V^*] = \{\sum w \in V^* \lambda_w[w] : \lambda_w \in \mathbb{C}\} \quad \text{where} \quad V^* = \mathbb{F}_2^3 - \{0\}$$

size class	1 $1A$	21 $2A$	56 $3A$	42 $4A$	24 $7A$	24 $7B$
$\chi_{\mathrm{triv}} = \chi_1$	1	1	1	1	1	1
χ_2	6	2	0	0	−1	−1
χ_3	7	−1	1	−1	0	0

INDUCED REPRESENTATIONS

Recall the permutation representation of G, i.e. how G permutes a transitive G-set $X \cong G/H$. We can view such a representation V as

$$V = \{f : G/H \to \mathbb{C}\}$$

where $gf(x) = f(g^{-1}(x))$. We may also write V as

$$V = \{f : G \to \mathbb{C} : f(xh) = f(x) \forall h \in H\}$$

DEF 1.14 Consider a subgroup $H < G$ and let $\chi : H \to \mathbb{C}^\times$ be a homomorphism, i.e. $\chi \in \mathrm{Hom}(H, \mathbb{C}^\times)$. Then the *induced representation* $\mathrm{Ind}_H^G(\chi)$ is given by

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

We observe some key facts about the representation V_χ. (Hopefully)

PROP 1.18 V_χ is preserved by the action of G, where we obey the rule $gf(x) = f(g^{-1}x)$.

PROOF. Let $f \in V_\chi, g \in G$. Then $gf(xh) = f(g^{-1}(xh)) = f(g^{-1}(x)h)$, and since $f \in V_\chi$, $\chi(h)f(g^{-1}(x)) = \chi(h)gf(x)$. Hence, $gf \in V_\chi$. □

PROP 1.19 $\dim(V_\chi) = \#G/H = [G : H]$.

PROOF. Let $a_1, ..., a_t$ be a set of coset representatives for $G = a_1H \sqcup \cdots \sqcup a_tH$. We claim the function

$$f \mapsto (f(a_1), ..., f(a_t)) \in \mathbb{C}^t$$

is an isomorphism from $V_\chi \to \mathbb{C}^t$. We find that this is injective by computing the kernel. If $f \in \ker$, then $f(a_1) = ... = f(a_t) = 0$. But since $f \in V_\chi$, $f(a_jh) = \chi(h)f(a_j) = 0$. Hence, $f(g) = 0\ \forall g \in G$. Conversely, for surjectivity, if we know how f acts on a_1, then we know how f acts on all $g \in G$, since we may write $g = a_ih$ for $h \in H$ and some a_i. □

Hence, if H is a quotient of G, then any representation of H yields a representation for G. Quotients are quite rare, though, and we observe further that for any subgroup $H < G$, any character of H yields a representation for G.

1.11 Basis of Induced Representation

Fix an induced representation V_ψ, on which we write instead $f : G \to \mathbb{C} : f(xh) = \psi^{-1}(h)f(x)$ for $f \in V_\psi$. For all $g \in G$, then

$$\chi_{V_\psi} = \sum_{\substack{aH \in G/H \\ a^{-1}ga \in H}} \psi(a^{-1}ga)$$

PROOF. We fix a basis for V_ψ. For $a \in G$, let δ_a be the unique function in V_ψ satisfying

$$\delta_a(a) = 1 \quad \delta_a(x) = 0\ x \notin aH$$

Since $\delta \in V_\psi$, we have $\delta_a(ah) = \psi^{-1}(h)$. Then $\delta_{a_1}, ..., \delta_{a_t}$ are linearly independent for coset representatives a_i, since all but $\delta_{a_i}(a_i)$ terms disappear.

Let an element $g \in G$ map a coset $ga_jH = a_{j'}H$. Then $ga_j = a_{j'}h_j$ for some $h_j \in H$. Observe, then, $g\delta_a = \delta_{ga}$ and $\delta_{ah} = \psi(h)\delta_a$.

$$g\delta_{a_j} = \delta_{ga_j} = \delta_{a_{j'}h_j} = \psi(h_j)\delta_{a_{j'}}$$

Then, finally,

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

□

1.12

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

PROOF.

$$\begin{aligned}\chi_{V_\psi}(g) &= \sum_{\substack{a \in G/H \\ gaH = aH}} \psi(a^{-1} g a) = \frac{1}{\#H} \sum_{\substack{a \in G \\ a^{-1} g a \in H}} \psi(a^{-1} g a) \\ &= \frac{\#Z(g)}{\#H} \sum_{a \in Z(g) \backslash G} \psi(a^{-1} g a) = \frac{\#G}{\#H} \frac{1}{\#C(g)} \sum_{a \in Z(g) \backslash G} \psi(\gamma)\end{aligned}$$

where, by Orbit Stabilizer, $\mathbb{Z}(g) \# C(g) = \#G$. We further get an isomorphism $Z(g) \setminus G \cong C(g)$. □

E.G. 1.7

Eg. 1 Let $G = \mathrm{GL}_3(\mathbb{F}_2)$ and H be the normalizer of P_7, a Sylow 7 subgroup of G. Consider $V_\psi = \mathrm{Ind}_H^G(\psi)$, where ψ is the 1-dim representation via $H \to \mathbb{Z}/3\mathbb{Z}$. By the theorem above, its character on 1 is

$$8 \times \frac{1}{1} \sum_{\mathbb{1}} \psi(\mathbb{1}) = 8$$

There are no order 2 elements in the Sylow subgroup of order 7, so its character is 0. The same holds for elements of order 4. For order 3 elements, we have

$$8 \times \frac{1}{56} \sum_{g \in \mathrm{ord}=3 \in H} \psi(g) = \frac{1}{7} \left(7 e^{\frac{2\pi i}{3}} + 7 e^{\frac{4\pi i}{3}} \right) = -1$$

To find the number of order 3 elements, we consider the quotient map $H \to \mathbb{Z}/3\mathbb{Z}$, and in particular the preimage of 1 and 2 (which are order 3 elements). Then, there are at least 7 elements of each, and so 14 in total.

For order 7 element, we consider both $7A \cap H$ and $7B \cap H$. One would imagine, since there are 6 such elements in total, that the classes are split 3 and 3. But this is true: if $g \in 7A$, then g^2 and g^4 belong to $7A$, but g^6, g^5, g^3

belong to $7B$. We yield 6 distinct elements, and hence conclude that they are distributed 3 and 3.

Hint about this fac: consider $x^3 + x^2 + 1 \leftrightarrow 7A$ and $x_3 + x + 1 \leftrightarrow 7B$

$$8 \times \frac{1}{24} \sum_{7A \cap H} \psi(g) = \frac{24}{24} = 1$$

The same will occur for $7B$, and we add a character row.

size	1	21	56	42	24	24
class	$1A$	$2A$	$3A$	$4A$	$7A$	$7B$
$\chi_{\text{triv}} = \chi_1$	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

One checks the inner product of χ_4 with itself to conclude that is is irreducibility. To find the dimensions of the remaining characters d_5, d_6, we have

$$1 + 6^2 + 7^2 + 8^2 + d_5^2 + d_6^2 = 168 \implies d_5^2 + d_6^2 = 18 \implies d_5 = d_6 = 3$$

TENSOR PRODUCTS

Previously, we've seen how to generate new representations from old ones, e.g. with direct sums $V_1 \oplus V_2$, where $g(v,w) = (gv, gw)$ and $\mathrm{Hom}_{\mathbb{C}}(V_1, V_2)$, where $gT = gTg^{-1}$. The characters of these new representations is $\chi_1 + \chi_2$ and $\overline{\chi_1}\chi_2$, respectively.

One could also take $\mathrm{Hom}(V_1, \mathbb{C}) := V^*$, the space of linear functionals (one envisages $\mathbb{C}$ as the trivial representation). Then $\chi_{V^*} = \overline{\chi_V}$.

DEF 1.15 $V_1 \otimes V_2 := \mathrm{Hom}_C(V_1^*, V_2)$ is the *tensor product* of V_1 and V_2.

PROP 1.20 $\dim(V_1 \otimes V_2) = \dim(V_1)\dim(V_2)$.

DEF 1.16 Given $v_1 \in V_1, v_2 \in V_2$, we define $v_1 \otimes v_2 \in V_1 \otimes V_2$ to take $\ell \in V_1^* \mapsto \ell(v_1)v_2$.

Let $e_1, ..., e_n$ be a basis for V_1 and $f_1, ..., f_m$ be a basis for V_2. Let $v_1 = a_1 e_1 + ... + a_n e_n$ and $v_2 = b_1 f_1 + ... + b_m f_m$. Then

$$v_1 \otimes v_2 = (a_1 e_1 + ... + a_n e_n) \otimes (b_1 f_1 + ... + b_m f_m) = \sum a_i b_j (e_i \otimes f_j)$$

PROP 1.21 G acts on $V_1 \otimes V_2$ by $g(v_1 \otimes v_2) = (gv_1) \otimes (gv_2)$. Then $\chi_{V_1 \otimes V_2} = \chi_{V_1}\chi_{V_2}$.

PROOF. Fix $g \in G$. Let $\{e_i\}$ and $\{f_i\}$ be bases of eigenvectors for g. Then let $ge_i = \lambda_i e_i$ and $gf_i = \mu_i f_i$. We have

$$g(e_i \otimes f_j) = (ge_i) \otimes (gf_j) = (\lambda_i e_i) \otimes (\mu_j f_j) = \lambda_i \mu_j (e_i \otimes f_j)$$

Then $\mathrm{tr}(\rho_{V_1 \otimes V_2}(g)) = \sum_{i \in [n], j \in [m]} \lambda_i \mu_j = (\sum_{i \in [n]} \lambda_i)(\sum_{j \in [m]} \mu_j) = \mathrm{tr}(\rho_{V_1}(g))\mathrm{tr}(\rho_{V_2}(g))$. One may also observe directly via $\chi_{\mathrm{Hom}(V_1, V_2)} = \overline{\chi_{V_1}}\chi_{V_2}$ □

APPLICATIONS OF REPRESENTATIONS

...

Let V is a representation of G and $T : V \to V$ be a G-equivariant endomorphism, i.e. $\in \mathrm{End}_G(V)$. If $V = V_1 \oplus \cdots \oplus V_t$ for irreducible, distinct representations of multiplicities all 1, then $T(V_j) \subseteq V_j$ and $T(v) = \lambda_j v \ \forall v \in V_j$. By composing inclusion maps and projection maps, we have

$$\begin{tikzcd}
& V \arrow[r, "T"] & V \arrow[dr, two heads, "\pi_i"] & \\
V_j \arrow[ur, hook, "\eta_j"] \arrow[rrr, dashed, "T_{ij}"'] & & & V_i
\end{tikzcd}$$

Where $\eta_j \in \mathrm{Hom}_G(V_j, V)$ and $\pi_i \in \mathrm{Hom}_G(V, V_i)$, as shown below. Take an arbitrary $v = v_1 + ... + v_t$. Then g distributes over the sum, and so

$$g\pi_i(v) = gv_i = \pi_i g(v)$$

We write $T_{ij} = \pi_i T \eta_j \in \mathrm{Hom}_G(V_j, V_i)$. By Schur's Lemma, then

$$T_{ij} = \begin{cases} 0 & i \neq j \\ \lambda_i & i = j \end{cases}$$

We observe this manually: let $v \in V_j = V_i$. Then

$$T(v) = \pi_1 T(v) + \ldots + \pi_t T(v) = T_{1j}(v) + \ldots + T_{tj}(v) = T_{jj}(v) = \lambda_j v$$

Using this, we have

$$T(v) = \begin{pmatrix} T_{11} & T_{12} & \cdots & T_{1t} \\ T_{21} & T_{21} & \cdots & T_{2t} \\ \vdots & \vdots & \ddots & \vdots \\ T_{t1} & Tt2 & \cdots & T_{tt} \end{pmatrix} \qquad T_{ij} \in \mathrm{Hom}_G(V_i, V_j)$$

In the extreme setting where $V_i = \mathbb{F}$ and V is $\mathbb{F}^t$, $T_{ij} \in \mathrm{Hom}_G(\mathbb{F}, \mathbb{F}) = \mathbb{F}$. Then $T : V \to V$ are represented by our familiar $t \times t$ matrices with entries in $\mathbb{F}$, as above.

E.G. 1.8

Finite, C-valued functions on X

Eg. 1 Let X be the faces of a cube. Let $V = L^2(X) \circlearrowleft G = S_4$. Then let

$$T : V \to V : T(\varphi)(x) = \frac{1}{4} \sum_{y \sim x} \varphi(y)$$

where $y \sim x \iff y$ and x are adjacent faces. We wish to decompose $L^2(X) = V$ into a sum of irreducible representations of S_4. Recall the characters of S_4 itself:

class size	$1A$ 1	$2A$ 6	$2B$ 3	$3A$ 8	$4A$ 6	
χ_1	1	1	1	1	1	triv
χ_2	1	−1	1	1	−1	sgn
χ_3	2	0	2	−1	0	
χ_4	3	1	−1	0	−1	natural
χ_5	3	−1	−1	0	1	$\chi_2 \otimes \chi_4$
χ_6	6	0	2	0	2	not irrep, calculate FP on X

We conclude from this table that $L^2(X) = V_1 \oplus V_3 \oplus V_5$. The trivial representation V_1 is comprised of all constant functions.

DEF 1.17

A function $\varphi : X \to \mathbb{C}$ is called *even* if $\varphi(X) = \varphi(x')$, where x' is the face opposite to x. The dimension of the vector space of even functions, say $L^2(X)_+$, is hence 3.

If $\varphi \in L^2(X)_+$, then $g\varphi(x) = \varphi(g^{-1}x)$, and $g\varphi(x') = \varphi(g^{-1}x')$, so $\varphi(g^{-1}x) = \varphi(g^{-1}x')$, so G preserves $L^2(X)_+$. We want to extract the trivial representation *out* of these functions, so define

$$L^2(X)_{+,0} := \{\varphi : X \to \mathbb{C} : \varphi \in L^2(X)_+ \text{ and } \sum_{x \in X} \varphi(x) = 0\}$$

with this we can write

$$\underbrace{\underbrace{V_1}_{\text{constant fns}} \oplus \underbrace{V_3}_{L^2(X)_{+,0}}}_{L^2(X)_+} \oplus V_5$$

Similarly, we consider the space of *odd* functions $L^2(X)_- = \{\varphi : X \to \mathbb{C} : \varphi(x') = -\varphi(x)\}$, and extract the trivial representation similarly to yield $L^2(X)_{-,0}$.

Recall that T, defined at the start, preserves V_1, V_3 and V_5. $T(\mathbb{1}) = \mathbb{1}$, thankfully. If $\varphi \in V_5$, then $T(\varphi) = 0$. If $\varphi \in V_3$, we consider

II Galois Theory

If E and F are fields, then E is an *extension* of F if F is a subfield of E. From now on, all fields are commutative. Note: if E is an extension of F, then E is *also* a vector space over F, by "forgetting" internal multiplication of elements in E. This motivates the following definition. DEF 2.1

The *degree* of E is $\dim_F(E)$, the dimension of E as an F-vector space. It is either a positive integer or infinity. We sometimes denote $[E : F] = \dim_F(E)$. DEF 2.2

E over F is called a *finite* extension if $[E : F] < \infty$. DEF 2.3

We write E/F to mean "the extension E over F," and, for $[E : F] = n$, draw

$$\begin{array}{c} E \\ \Big| \\ n \\ \Big| \\ F \end{array}$$

denoting inclusion by vertical position (higher containing lower).

E.G. 2.1

Eg. 1 Consider $E = \mathbb{C}$ and $F = \mathbb{R}$. Then $[\mathbb{C} : \mathbb{R}] = 2$, with a basis $\{1, i\}$.

Eg. 2 Consider $E = \mathbb{C}$ and $F = \mathbb{Q}$. Then $[\mathbb{C} : \mathbb{Q}] = \infty$.

Eg. 3 Let $E = F(x)$ be the fraction field of $F[x]$, i.e. all expressions

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

Then $[E : F] = \infty$, in much the same spirit as Eg 2.

Let F be a field, and $E = F[x]/\langle p(x) \rangle$, where $p \in F[x]$. Then E is an extension of F, with $[E : F] = \deg(p)$ by taking a basis $\{1, t, ..., t^{\deg(p)-1}\}$. **PROP 2.1**

2.1 Multiplicity of Degree

Let $K \subset F \subset E$ be finite extensions. Then

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

PROOF.

Let $n = [E : F]$ and $m = [F : K]$. Let $\alpha_1, ..., \alpha_n$ be a basis for E as an F-vector space, and similarly, $\beta_1, ..., \beta_m$ be a basis for F as a K-vector space. Let $a \in E$. Then

$$a = \lambda_1 \alpha_1 + ... + \lambda_n \alpha_n$$

uniquely for $\lambda_i \in F$. But each λ_i may be written uniquely as

$$\lambda_i = \lambda_{i1}\beta_1 + ... + \lambda_{im}\beta_m = \vec{\lambda_i}\vec{\beta}$$

where $\lambda_{ij} \in K$. Then, substituting this expression in for λ_i, we see that

$$a = \vec{\lambda_1}\vec{\beta}\alpha_1 + ... + \vec{\lambda_n}\vec{\beta}\alpha_n = \sum_{i=1}^{n}\sum_{j=1}^{m} \lambda_{ij}\alpha_i\beta_j$$

and hence $\{\alpha_i\beta_j\}_{\substack{1\le i\le n \\ 1\le j\le m}}$ is a K basis for E. □

DEF 2.4 Let F be a field and $\alpha \in E$, where E/F is an extension. Then F *adjoined with* α, denoted $F(\alpha)$ is the smallest subfield of E containing α and F.

One extends this idea for $F(\alpha_1, ..., \alpha_n)$, where $\{\alpha_1, ..., \alpha_n\} \subseteq E$.

We may think of $F(\alpha)$ outside of the context of a fixed extension E.

PROP 2.2 If α is algebraic over F (see Def 2.6), then $F(\alpha) = F[x]/p(x)|_{\alpha}$, the elements $f \in F[x]/p(x)$ evaluated at α, where p is the smallest irreducible polynomial in F which α satisfies. If α is *not* algebraic, then $F(\alpha) = F[\alpha]$, all polynomials in F at α.

DEF 2.5 A complex number is *constructible by ruler and compass* if it can be obtained from $\mathbb{Q}$ by successive applications of + or $\sqrt{\cdot}$. Alternatively, $\alpha \in \mathbb{R}$ is constructible if there exists extensions $\mathbb{Q} \subset F_1 \subset \cdots \subset F_n$ such that $F_{i+1} = F_i(\sqrt{\alpha_i})$, $\alpha_i \in F_i$, and $\alpha \in F_n$.

Sometimes called "quadratic extensions"

2.2 Non-Constructible Roots

If $\alpha \in \mathbb{R}$ satisfies an irreducible, cubic polynomial over $\mathbb{Q}$, then α is not constructible by ruler and compass.

PROOF. Suppose that α is constructible. Then $Q \subset F_1 \subset \cdots \subset F_n$, where $F_{i+1} = F_i(\sqrt{a_i})$: $a_i \in F_i$. Hence, $[F_{i+1} : F_i] = 2$, so $[F_n : \mathbb{Q}] = 2^n$. We have also $\alpha \in F_n$.

But consider $\mathbb{Q}[x]/p(x) = \mathbb{Q}(\alpha)$ for the cubic p of interest. $[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}[x]/p(x) : \mathbb{Q}] = 3$. But $\alpha \in \mathbb{F}_n$ and $\alpha \in \mathbb{Q}(\alpha)$, so F_n is a $\mathbb{Q}(\alpha)$ vector space of dimension d.

$3d = 2^n$ by Thm 2.1, which is a contradiction. Visually:

$$
\begin{tikzcd}
 & F_n \arrow[d, dotted, dash, "2"] \arrow[ddd, bend left, dash, "2^n"] \\
 & F_2 \arrow[d, dash, "2"] \\
\mathbb{Q}(\alpha) \arrow[uur, dash, "d"] & F_1 \arrow[d, dash, "2"] \\
 & \mathbb{Q} \arrow[ul, dash, "3"]
\end{tikzcd}
$$

□

As a corollorary, we see that, for any $\alpha \in R$ which satisfies an irreducible polynomial over $\mathbb{Q}$, this polynomial must have degree 2^t for some t in order to be constructible.

E.G. 2.2

Eg. 1 $\sqrt[3]{2}$ is not constructible, since it is a root of $x^3 - 2$, which is irreducible in $\mathbb{Q}$.

Eg. 2 $\cos\left(\frac{2\pi}{9}\right)$ is not constructible, since it is a root of $4x^3 + 3x + \frac{1}{2}$.

The constructability of the first two values in Example 2.2 are necessary to duplicate a cube and trisect an angle, respectively, with a ruler and compass.

DEF 2.6

Let E/F be a finite extension. An element $\alpha \in E$ is *algebraic* over F if α is the root of a polynomial in $F[x]$.

E.G. 2.3

Eg. 1 $\sqrt{2}$ is algebraic over $\mathbb{Q}$ (see $x^2 - 2$), and i is algebraic over $\mathbb{Q}$ and $\mathbb{R}$ (see $x^2 + 1$).

Eg. 2 π is *not* algebraic over $\mathbb{Q}$, but it is algebraic over $\mathbb{Q}(\pi^3)$ (see $x^3 - \pi^3$).

Eg. 3 The set of $\alpha \in \mathbb{R}$ which are algebraic over $\mathbb{Q}$ is countable!

Since we can essentially associate with each α a polynomial in $\mathbb{Q}$. But $\mathbb{Q}$ is countable, and hence $\mathbb{Q}[x]$ is.

PROP 2.3

If E/F is a finite extension, then every $\alpha \in E$ is algebraic over F.

PROOF.

$\{1, \alpha, \alpha^2, ..., \alpha^n\}$ cannot be linearly independent, since $[E : F] = n$. Hence, there exist coefficients which vanish a linear combination of these elements. □

DEF 2.7

The automorphism group of E/F is

$$\mathrm{Aut}(E/F) := \{\varphi : E \to E : \varphi(x+y) = \varphi(x) + \varphi(y) : \varphi(xy) = \varphi(x)\varphi(y) : \varphi|_F = \mathbb{1}\}$$

PROP 2.4

$\varphi(1) = 1, \varphi(0) = 0, \varphi(a^{-1}) = \varphi(a)^{-1}$ for $\varphi \in \mathrm{Aut}(E/F)$.

We observe that any $\varphi \in \mathrm{Aut}(E/F)$ is automatically injective. In fact, if $[E : F] < \infty$, it is automatically surjective as well (by viewing it as an F-linear transformation).

2.3 Aut(E/F) Has Finite Orbits on E

If E/F is a finite extension, then Aut(E/F) acts on E with finite orbits.

PROOF. By this, we mean, when taking $\varphi \in \text{Aut}(E/F)$, repeated action on some $\alpha \in E$ yields only finitely distinct elements.

Since α is algebraic for F, there is a polynomial $f(\alpha) = \lambda_n \alpha^n + \ldots + \lambda_1 \alpha + \lambda_0 = 0$, where $\lambda_i \in F$. Then

$$\varphi(\lambda_n \alpha^n + \ldots + \lambda_1 \alpha + \lambda_0) = 0$$

by Prop 2.4. But, by linearity and vanishing conditions on F, this is also

$$\varphi(\lambda_n \alpha^n) + \ldots + \varphi(\lambda_1 \alpha) + \varphi(\lambda_0) = \lambda_n \varphi(\alpha)^n + \ldots + \lambda_1 \varphi(\alpha) + \lambda_0$$

We conclude: if α is a root of $f(x) \in F[x]$, then $\varphi(\alpha)$ is a root of $f(x)$. Hence, the orbit of α under the action of Aut(E/F) will be contained in the roots of $f(x)$, which is finite (and bounded by $[E : F]$, by Prop 2.3).

To be precise: the orbit of *any* $\varphi \in \text{Aut}(E/F)$ is contained in the roots of f, so the orbit of *all* of Aut(E/F) is contained in the roots of f. □

Though we contextualized Thm 2.3 around finite extensions, we only used the fact that $\alpha \in E$ is algebraic. Hence, if E/F is an infinite, algebraic extension (i.e. all $\alpha \in E$ are algebraic), then the result also holds. We restate without proof:

PROP 2.5 If E/F is an algebraic extension, then Aut(E/F) acts on E with finite orbits.

PROP 2.6 If $[E : F] < \infty$, then $\#\text{Aut}(E/F) < \infty$.

PROOF. Let $\alpha_1, \ldots, \alpha_n$ be generators for E over F (i.e. every $\alpha \in E$ can be written as a polynomial in $\alpha_1, \ldots, \alpha_n$). Let $G = \text{Aut}(E/F)$. Then

$$E = F(\alpha_1, \ldots, \alpha_n)$$

$F(\alpha_1, \ldots, \alpha_n) \subseteq E$, since $\{\alpha_i\} \subseteq E$. Conversely, since $\{\alpha_i\}$ are generators, all elements in E are polynomials in $\{\alpha_i\}$, which are contained in $F(\alpha_1, \ldots, \alpha_n)$ by definition.

If $\varphi \in \text{Aut}(E/F)$, then φ is completely determined by $\{\varphi(\alpha_1), \ldots, \varphi(\alpha_n)\}$, which is contained in

$$\text{orb}_G(\alpha_1) \times \cdots \times \text{orb}_G(\alpha_n)$$

Since $\text{orb}_G(\alpha_i)$ is finite by Thm 2.3, this is finite, and so is Aut(E/F). □

E.G. 2.4

Eg. 1 Suppose that E is generated over F by a single element α, i.e. $E = F(\alpha)$. Let $p(x) \in F[x]$ be the minimal polynomial of α. Then $E = F/\langle p \rangle$ as well.

$\varphi \in \text{Aut}(F(\alpha)/F)$ is determined by $\varphi(\alpha) \in \{\text{roots of } p(x)\}$, which, as a set, is

$\leq \deg(p(x)) = [F(\alpha) : F]$, so we have

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

We remark that this inequality is true in general.

PROP 2.7 If E/F is any finite extension, then $\#\mathrm{Aut}(E/F) \leq [E : F]$.

PROOF. We'll proceed by induction on the number of generators for E over F. (A similar proof is employed for Prop 2.15.) Let $E = F(\alpha_1, ..., \alpha_n)$. Notice that $\mathrm{Aut}(E/F) = \mathrm{Hom}_F(E, E)$. Let M be any extension of F, and consider $\mathrm{Hom}_F(E, M)$. We'll instead prove $\#\mathrm{Hom}_F(E, M) \leq [E : F]$.

The $n = 1$ case is essentially covered above in Example 2.4. Let $E = F(\alpha) = F/\langle p\rangle$, where $p(x) \in F[x]$ is the minimal polynomial of α. Let $d = [E : F] = \deg(p)$. Consider $\varphi \in \mathrm{Hom}_F(E, M)$. Then the map $\varphi \mapsto \varphi(\alpha)$ is an inclusion $\mathrm{Hom}_F(E, M) \hookrightarrow \{\text{roots of } p\}$, by observing

$$\varphi(a_0 + a_1\alpha + ... + a_{d-1}\alpha^{d-1}) = a_0 + a_1\varphi(\alpha) + ... + a_{d-1}\varphi(\alpha)^{d-1}$$

In particular, these are the roots of p in M, the collection of which is bound in size by $\deg(p) = [E : F]$.

Now we show $n \to n + 1$. Set $E = F(\alpha_1, ..., \alpha_{n+1})$. Let $F' = F(\alpha_1, ..., \alpha_n)$. If $F' = E$, then we're done. One may write $E = F'(\alpha_{n+1})$. Let $[F' : F] = d_1$ and $[E : F'] = d_2$.

Consider the restriction map

$$\mathrm{Hom}_F(E, M) \twoheadrightarrow \mathrm{Hom}_F(F', M)$$

We know, by induction, that $\#\mathrm{Hom}_F(F', M) \leq [F' : F] = d_1$. Now we ask: given $\varphi_0 \in \mathrm{Hom}_F(F', M)$, how many $\varphi \in \mathrm{Hom}_F(E, M)$ exist such that $\varphi|_{F'} = \varphi_0$? In other words, we wish to describe the preimage of the map above. Define

$$g(x) = \lambda_{d_2}x^{d_2} + ... + \lambda_1 x + \lambda_0 : \lambda_i \in F'$$

to be the minimal polynomial of α_{n+1} in $F'[x]$. Fix $\varphi_0 \in \mathrm{Hom}_F(F', M)$ and let $\varphi \in \mathrm{Hom}_F(E, M)$ be such that $\varphi|_{F'} = \varphi_0$. Then

$$\begin{aligned} 0 = \varphi(g(\alpha_{n+1})) &= \varphi(\lambda_{d_2})\varphi(\alpha_{n+1})^{d_2} + ... + \varphi(\lambda_1)\varphi(\alpha_{n+1}) + \varphi(\lambda_0) \\ &= \varphi_0(\lambda_{d_2})\varphi(\alpha_{n+1})^{d_2} + ... + \varphi_0(\lambda_1)\varphi(\alpha_{n+1}) + \varphi_0(\lambda_0) \end{aligned}$$

We conclude that $\varphi(\alpha_{n+1})$ is a root of $\tilde{g}$, which replaces g's coefficients λ_i by $\varphi_0(\lambda_i)$. $\#\{\text{roots of } \tilde{g}\} \leq \deg(\tilde{g}) = \deg(g) = d_2$, so there can be at most d_2 choices for $\varphi(\alpha_{n+1})$. However, φ's behavior outside of F' is completely determined by $\varphi(\alpha_{n+1})$. We conclude that $\#\mathrm{Hom}_F(E, M) \leq d_2 \cdot \#\mathrm{Hom}_F(F', M) \leq d_2 d_1 = [E : F]$.

□

DEF 2.8 E/F is called *Galois* if $\#\mathrm{Aut}(E/F) = [E : F]$. We write $\mathrm{Gal}(E/F) := \mathrm{Aut}(E/F)$.

E.G. 2.5

Eg. 1 Let $E = \mathbb{C}$ and $F = \mathbb{R}$, with $[E : F] = 2$. Consider complex conjugation $\tau : \mathbb{C} \to \mathbb{C}$ by $x + iy \mapsto x - iy$. This is a field automorphism, so $\{1, \tau\} \subseteq \mathrm{Aut}(\mathbb{C}/\mathbb{R})$, and indeed $\mathrm{Aut}(\mathbb{C}/\mathbb{R}) = \{1, \tau\}$, since $\#\mathrm{Aut}(\mathbb{C}/\mathbb{R}) \leq [\mathbb{C} : \mathbb{R}] \leq 2$. Hence, $\mathbb{C}$ is Galois over $\mathbb{R}$.

Eg. 2 Let $F = \mathbb{Q}$ and $E = \mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}[x]/(x^3-2) \subset \mathbb{R}$. Then $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) \leftrightarrow \{$roots of $x^3 - 2$ over $\mathbb{Q}(\sqrt[3]{2})\}$. But the only such root *is* $\sqrt[3]{2}$, so $\#\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = 1$. Hence, $\mathbb{Q}(\sqrt[3]{2})$ is not Galois over $\mathbb{Q}$. What can we do to *make* this Galois?

Eg. 3 Let $F = \mathbb{Q}$ as above and $E = \mathbb{Q}(\sqrt[3]{2}, \xi)$, where $\xi^3 = 1$ is a cube root of unity, and thus satisfies $x^2 + x + 1$. We claim that E is Galois. We can write

Recall that all n-th roots ξ satisfy the polynomial $\xi^{n-1} + \ldots + \xi + 1 = 0$

$$\begin{tikzcd}
 & \mathbb{Q}(\sqrt[3]{2}, \xi) \arrow[dl, dash, "3"'] \arrow[dd, dash, "6"] \arrow[dr, dash, "2"] & \\
\mathbb{Q}(\xi) \arrow[dr, dash, "2"'] & & \mathbb{Q}(\sqrt[3]{2}) \arrow[dl, dash, "3"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

by observing $\mathbb{Q}(\sqrt[3]{2}, \xi) = \mathbb{Q}(\sqrt[3]{2})(\xi)$ and noting that $x^2 + x + 1$ is still irreducible in $\mathbb{Q}(\sqrt[3]{2})$. (Then $[\mathbb{Q}(\sqrt[3]{2}, \xi) : \mathbb{Q}(\sqrt[3]{2})] = 2$, and the rest follows).

$\implies [E : F] = 6$. Now let $\varphi \in \mathrm{Aut}(E/\mathbb{Q})$. $\varphi(\xi)$ will be a root of $x^2 + x + 1$, i.e. ξ or $\overline{\xi}$. Similarly, $\varphi(\sqrt[3]{2})$ will satisfy $x^3 - 2$, so it may be $\sqrt[3]{2}$, $\xi\sqrt[3]{2}$, or $\overline{\xi}\sqrt[3]{2}$.

φ is completely determined by where it sends ξ and $\sqrt[3]{2}$, as outlined above. Its action on the roots r_1, r_2, r_3 of $x^3 - 2$ follow. Fix $r_1 = \sqrt[3]{2}$, $r_2 = \xi\sqrt[3]{2}$, and $r_3 = \overline{\xi}\sqrt[3]{2}$. We will construct a table of automorphisms:

	$\xi \to \xi$	$\xi \to \overline{\xi}$
$\sqrt[3]{2} \to \sqrt[3]{2}$	Id	$(r_2\ r_3)$
$\sqrt[3]{2} \to \xi\sqrt[3]{2}$	$(r_1\ r_2\ r_3)$	$(r_1\ r_2)$
$\sqrt[3]{2} \to \overline{\xi}\sqrt[3]{2}$	$(r_1\ r_3\ r_2)$	$(r_1\ r_3)$

Hence, $\mathrm{Gal}(E/F) \cong S_3$, and has size 6, as desired.

DEF 2.9 Let E/F be a finite extension. Consider $G \subseteq \mathrm{Aut}(E/F)$. Then

$$E^G = \{\alpha \in E : g\alpha = \alpha\ \forall g \in G\}$$

is called the *fixed field* of G under E.

PROP 2.8 E^G is a subfield of E, which contains F.

2.4 Galois Fixed Fields are the Base Field

If E/F is a Galois extension, with $G = \mathrm{Gal}(E/F)$, then $E^G = F$.

PROOF.

For reference, consider the diagram

$$\begin{array}{c} E \\ | \\ E^G \\ | \\ F \end{array}$$

We know $\#G \leq [E : E^G]$, since $G \subset \mathrm{Aut}(E/E^G)$. (Let $\varphi \in G = \mathrm{Gal}(E/F), \alpha \in E^G$. We claim $\varphi|_{E^G} = \mathbb{1}$. $\varphi(\alpha) = \alpha$ by definition, since $\varphi \in G$.) We also know $[E : F] = \#G$, since E/F is Galois. But $[E : E^G]$ divides $[E : F]$ by multiplicity, so we conclude $[E : E^G] = [E : F] \implies [E^G : F] = 1$. Hence, $E^G = F$ exactly. $\square$

2.5 E/F Galois $\implies$ Normal

Let E/F be a Galois extension. 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 $E[x]$. We call this property normality (see Def 2.12).

PROOF.

Let $r \in E$ be a root of $f(x)$. Let $\{r_1, ..., r_n\}$ be the orbit of $r \in E$ under $\mathrm{Gal}(E/F)$ (as in Thm 2.3). Consider now

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

Expanded out, we get

$$g(x) = x^n + \sigma_1 x^{n-1} + \sigma_2 x^{n-1} + ... + (-1)^n \sigma_n$$

where σ_i are the "elementary symmetric functions" in $r_1, ..., r_n$, i.e. equivalent up to permutations on the indices of r_i. For instance, $\sigma_1 = r_1 + ... + r_n$ and $\sigma_n = r_1 \cdots r_n$. We find that $\sigma_i \in E^G$, since $G = \mathrm{Gal}(E/F)$ permutes the roots $r_1, ..., r_n$, and σ_i are symmetric. But $E^G = F$, so $\sigma_i \in F$. Hence, $g(x) \in F[x]$.

Since f is irreducible, it is the minimal polynomial which vanishes r over F. But $g \in F[x]$ vanishes r, so $f(x) | g(x) = (x - r_1) \cdots (x - r_n)$. We conclude that $f(x) = \prod_{j \in I}(x - r_j)$ for some index restriction $I \subseteq [n]$, so it splits. $\square$

SPLITTING FIELDS

DEF 2.10 Let F be a field and $f(x)$ be any polynomial in $F[x]$. A *splitting field* of $f(x)$ is an extension E/F satisfying

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

PROP 2.9 A splitting field always exists.

PROOF. By induction on $\deg(f) = n$. If $n = 1$, then $E = F$ itself.

Let $\deg(f) = n + 1$. Let $p(x)$ be an irreducible factor of $f(x)$ in $F[x]$. (If f is irreducible itself, then set $p = f$, and our argument does not change).

Consider $L = F[x]/\langle p\rangle$. Then L is a field containing F and a root of $p(x)$ (and hence of $f(x)$). Let r be such a root of $p(x)$ in L. Then $(x - r)$ divides $p(x)$, and hence $f(x)$, in $L[x]$, i.e. we can write $f(x) = (x - r)g(x)$, with $\deg(g) = n$.

Let E be the splitting field of $g(x)$ over L. We claim that this is the splitting field of f over F. First note that, over E, g splits completely. But $f(x) = (x - r)g(x)$ in a subfield of $L \subset E$, so f splits completely too. E will be generated by the roots of g, which are contained in the roots of f. □

We remark that it is computationally hard to compute the degree of a splitting field of $f(x)$. In particular, if $f(x)$ is irreducible of degree n, and E is the splitting field of $f(x)$, then
$$n \leq [E : F] \leq n!$$
In the best case, we have an irreducible with only one root to affix, in which we mod out by a degree n polynomial, yielding a degree n extension. In the worse case, we must affix *all* roots "manually," generating extensions-of-extensions-of-... of decrementing degree, which yields a total extension of degree $n \cdot (n-1) \cdot ... \cdot 1 = n!$ by multiplicity.

2.6 All Splitting Fields Are Equivalent

If $f(x) \in F[x]$ and E, E' are two splitting fields of $f(x)$ over F, then $E \cong E'$ as extensions of F.

PROOF. By induction on the degree $\deg(f) = n$. If $n = 1$, then $E = E' = F$.

Let $p(x)$, as before, be an irreducible factor of $f(x)$, and let r be a root of $p(x)$ in a splitting field E of p. Similarly, let r' be a root of $p(x)$ in E', another splitting field of p. We know that $F(r)$ and $F(r')$ are isomorphic over F, since they are both equal to $F[x]/p(x)$. Let φ be the isomorphism $F(r) \underset{\varphi}{\cong} F(r')$.

Denote $L = F(r) = F(r')$. Then E and E' are also splitting fields of $g(x)$, where $(x-r)g(x) = f(x)$, over L. By induction, then, they are E and E' are isomorphic as extensions. □

PROP 2.10 If E/F is Galois, then E is the splitting field of a polynomial $f(x)$ in $F[x]$.

PROOF. Since $[E : F] < \infty$, let $\alpha_1, \ldots, \alpha_n$ be a finite set of generators for E/F. Let $f_1, \ldots, f_n$ be the minimal irreducible polynomials in $F[x]$ having $\alpha_1, \ldots, \alpha_n$ as roots, respectively (e.g. f_1 is minimally irreducible such that α_1 is a root).

Consider $f(x) = f_1(x) \cdots f_n(x)$. By normality of $E[x]$ (see Thm 2.5), all the f_j's factor completely in $E[x]$. Hence, f factors completely. The roots of $f(x)$ generate E by construction, so we conclude that E is a splitting field of $f(x)$. □

PROP 2.11 All finite fields have cardinality p^n for some prime p and $n > 0$.

PROOF. Let F be a finite field. Recall that $\text{char}(F) = p$, the minimal p such that $\overbrace{1 + \ldots + 1}^{p \text{ times}} = 0$, is always prime. We can naturally extract $\mathbb{F}_p \subset F$ by taking the subfield generated by 1. Let $n := \dim_{\mathbb{F}_p}(F)$. We have $\#F = p^n$. □

2.7 Unique Field of Prime Power Cardinality

Given a prime p and an integer $n > 0$, there is a field F of cardinality p^n. Furthermore, this field is unique.

This theorem implies a one-to-one correspondence between finite fields and prime powers.

PROOF. One possible approach is to find a polynomial $f(x)$ in $\mathbb{F}_p[x]$ which is irreducible of degree n. Then

$$F = \mathbb{F}_p[x]/(f(x))$$

is the desired field. This is a valid approach. However, instead, we'll construct a polynomial of degree p^n whose roots form a field, and are distinct.

Let F be the splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$. Note that $x^{p^n} - x$ has distinct roots in any extension of $\mathbb{F}_p$. Hence, $\#F \geq p^n$. We now need to show that $\#F = p^n$ exactly. To do so, recall that the set of roots of $x^{p^n} - x$ is closed under addition and multiplication, and is hence a field, so $\#F \leq p^n$.

The uniqueness of F up to isomorphism follows from Thm 2.6. □

Note that F, as constructed above, is an extension of $\mathbb{F}^p$. It happens to be Galois.

2.8 Extensions of $\mathbb{F}_p$ are Galois

If $F/\mathbb{F}_p$ is a finite extension for prime p, then $\#\mathrm{Aut}(F/\mathbb{F}_p) = [F : \mathbb{F}_p]$. Moreover, $\mathrm{Aut}(F/\mathbb{F}_p) = \mathbb{Z}/p\mathbb{Z}$.

DEF 2.11 The map $\varphi : F \to F$ by $a \mapsto a^p$ is called the *Frobenius automorphism*.

PROOF. Consider the Frobenius homomorphism $\varphi : F \to F$. Because φ is a homomorphism, it is injective. But $\dim_{\mathbb{F}_p}(F) < \infty$, so φ is a bijection, and hence an automorphism.

$\varphi^k(a) = a^{p^k}$. Let $k = \mathrm{ord}(\varphi)$. This is the least k such that $\varphi^k(a) = a\ \forall a \in F$. If there exists such a k, then $x^{p^k} - x$ has at least p^n roots, and so $k \geq n$. But also $\varphi^n = I$, so exactly $k = n$, and $\mathrm{ord}(\varphi) = n$ in $\mathrm{Aut}(F/\mathbb{F}_p)$. Hence, $\mathbb{Z}/p\mathbb{Z} \subset \mathrm{Aut}(F/\mathbb{F}_p)$.

But $\#\mathrm{Aut}(F/\mathbb{F}_p) \leq [F : \mathbb{F}_p] = n$, so in fact $\mathbb{Z}/p\mathbb{Z} = \mathrm{Aut}(F/\mathbb{F}_p)$, with a canonical generator φ of order n:

$$\mathrm{Gal}(F/\mathbb{F}_p) = \{\varphi, ..., \varphi^{n-1}, \varphi^n\} \quad \square$$

NORMAL, SEPARABLE, AND GALOIS

DEF 2.12 E/F is called *normal* if every irreducible polynomial $f \in F[x]$ with a root in E splits completely in E.

PROP 2.12 Any Galois extension E/F is normal.

PROOF. See proof of Thm 2.5. $\square$

DEF 2.13 An extension E over F is *separable* if every irreducible polynomial $f \in F[x]$ with a root in E has no multiple roots.

DEF 2.14 A polynomial $f \in F[x]$ is called *separable* if it is irreducible and has no repeated roots in its splitting field. Equivalently, f is irreducible and $\gcd(f, f') = 1$.

PROP 2.13 If $\mathrm{char}(F) = 0$, then every extension E/F is separable.

PROOF. If $\gcd(f, f') = 1$, where f' is the formal derivative, then E/F is separable. (This is necessary and sufficient—if a root appears with multiplicity > 1, it will show up in the gcd). We show this is the case when $\mathrm{char}(F) = 0$.

We write

$$f(x) = a_n x^n + ... + a_1 x + a_0 : a_i \in F \implies f'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} ... + 2a_2 x + a_1$$

We know that $\gcd(f, f') | f$. But f is irreducible, so $\gcd(f, f') = f$ or 1. If

$\gcd(f, f') = f$, then $n = n-1$ in F (as $\deg(f) = n, \deg(f') = n-1$). But $\text{char}(F) = 0$, so this can't occur. $\square$

PROP 2.14 A finite Galois extension E/F is separable.

PROOF. We repeat the proof in Thm 2.5. By necessity, the orbit of a root contains distinct elements. Assume we "terminate" the orbit, i.e. observe $\mapsto \alpha \mapsto \beta \mapsto \beta \mapsto$. Let φ be the automorphism we take the orbit through. $\varphi(\alpha) = \beta$ and $\varphi(\beta) = \beta \implies \varphi(\alpha^{-1}\beta) = 1 \implies \alpha^{-1}\beta = 1 \implies \alpha = \beta$. $\square$

PROP 2.15 If E/F is finite, normal, and separable, then E/F is Galois.

PROOF. We provide a similar proof to that of Prop 2.7. In particular, we show $\#\text{Hom}_F(K, E) = [K : F]$ for $F \subset K \subset E$ by induction over $n = [K : F]$. Then, $\#\text{Aut}(E/F) = [E : F]$ as desired. If $n = 1$, then $K = F$, so $\#\text{Hom}_F(F, E) = \{\mathbb{1}\}$, since, for $\varphi \in \text{Hom}_F(F, E), \varphi(\alpha) = \alpha\varphi(\mathbb{1}) = \alpha$.

We show for $n > 1$. Let K be some intermediate extension of F with generators $\alpha_1, ..., \alpha_t$, i.e. $K = F(\alpha_1, ..., \alpha_t)$ with $[K : F] = n$. We can write $K = F(\alpha_1, ..., \alpha_{t-1})(\alpha_t) =: K_{t-1}(\alpha_t)$. By the induction hypothesis, $\#\text{Hom}_F(K_{t-1}, E) = [K_{t-1} : F]$.

We now wish to show that there exist $[K : K_{t-1}]$ ways to extend the domain of $\varphi_0 \in \text{Hom}_F(K_{t-1}, E)$ to a homomorphism $\varphi \in \text{Hom}_F(K, E)$. Then, $\#\text{Hom}_F(K, E) = [K : K_{t-1}][K_{t-1} : F] = [K : F]$.

Let $\alpha_t \in K$ have minimal polynomial $p(x) \in K_{t-1}[x]$, so that $K = K_{t-1}[x]/\langle p(x)\rangle$. Fix $\varphi_0 \in \text{Hom}_F(K_{t-1}, E)$ with $\varphi|_{K_{t-1}} = \varphi_0$. The remainder of φ's mapping is determined by $\varphi(\alpha_t)$.

$\varphi(\alpha_t)$ will be a root of p, since α_t is a root of p. Let $[K : K_{t-1}] = d$. Then

$$\begin{aligned} 0 = \varphi(p(\alpha_t)) &= \varphi(\lambda_n \alpha_t^d + ... + \lambda_1 \alpha_t + \lambda_0) \\ &= \varphi_0(\lambda_n)\varphi(\alpha_t)^d + ... + \varphi_0(\lambda_1)\varphi(\alpha_t) + \varphi_0(\lambda_0) \end{aligned}$$

where we note that $\varphi(\lambda_i) = \varphi_0(\lambda_i)$, since $\varphi|_{K_{t-1}} = \varphi_0$. We conclude that $\varphi(\alpha_t)$ is a root of $\tilde{p}$, the polynomial p with its coefficients composed with φ_0. In any case, it is of degree d, so we can find at most d roots, and hence d mappings for $\varphi(\alpha_t)$.

We need to demonstrate that there are *exactly* d ways to extend φ_0, i.e. exactly d distinct roots of $\tilde{p}$ in E. p is minimal in K_{t-1}, so it divides g, the minimal polynomial of α_t in F. Composing p and g's coefficients with φ_0 yields $\tilde{p}|\tilde{g}$. But g has coefficients in F, so φ_0 doesn't alter the polynomial, i.e. $g = \tilde{g}$.

Why? $g \in F[x] \subset K_{t-1}[x]$ is satisfied by α_t. But p is minimal in $K_{t-1}[x]$ with this property.

By normality and separability, g splits into distinct linear factors in $E[x]$, and therefore $\tilde{p}$ does as well. We conclude that $\tilde{p}$ attains all its roots in $E[x]$, so $\varphi(\alpha_t)$ has exactly d valid mappings. $\square$

PROP 2.16 If E/F is a finite extension, then the following are equivalent:

1. $\#\mathrm{Aut}(E/F) = [E : F]$
2. E is normal and separable
3. E is the splitting field of a separable polynomial over F.

PROOF. ($1 \implies 2$) is done in Prop 2.14 and Thm 2.5. ($2 \implies 1$) was completed above. ($1 \implies 3$) and ($3 \implies 2$) are completed in Prop 2.10 (we did not have the notion of separability at the time—notice that $f = f_1 \cdots f_n$ has distinct roots by construction). □

PROP 2.17 If E/F is Galois, and K is a subfield of E containing F, then E is Galois over K.

PROOF. Since E/F is normal and separable, if $\alpha \in E$, there exists a polynomial $f \in F[x]$ which is irreducible, splits distinctly in E, and is satisfied by α (take the minimal polynomial).

Let g be the minimal irreducible polynomial of α over K. Then $g|f$. But in $E[x]$, f factors into distinct linear factors, and, therefore, so does g. We conclude that E/K is normal and separable.

Caveat: K need not be Galois over F. Let $G = \mathrm{Gal}(E/F)$, $X = \mathrm{Hom}_F(K, E)$. Then $\#X = [K : F]$ by the induction argument employed in Prop 2.15.

$\mathrm{Hom}_F(K, K) \subsetneq \mathrm{Hom}_F(K, E) = X$ is reasonable, where then $\#\mathrm{Aut}(K/F) < [K : F]$.

The idea above can also prove that E/K is Galois. We write, by orbit stabilizer,

$$\#X = \frac{\#G}{\mathrm{stab}(\varphi)} \implies \mathrm{stab}(\varphi) = \frac{\#G}{\#X} = \frac{[E : F]}{[K : F]} = [E : K]$$

where we take the action $g\varphi = g \circ \varphi$ for $\varphi \in X$. Then $\mathrm{stab}(\varphi) = \mathrm{Aut}(E/K)$ exactly. For this, let $g\varphi = \varphi$ and $\alpha \in K$. Then $g\varphi(\alpha) = \varphi(\alpha)$, but $\varphi(\alpha) = \alpha$, so $g\alpha = \alpha \implies g \in \mathrm{Aut}(E/K)$. The converse holds similarly. □

E.G. 2.6 **Eg. 1** Recall that, if $E/\mathbb{F}_p$ is a finite extension, then $E/\mathbb{F}_p$ is Galois with Galois group $\mathbb{Z}/p\mathbb{Z}$ (see Thm 2.8).

Consider then $K = \mathbb{F}_{p^t}$, with $\mathbb{F}_p \subset K \subset E$, then E is Galois over K. $\mathrm{Gal}(E/K) = \langle \varphi^t \rangle$, with $\varphi^t : x \to x^{p^t}$.(The "relative Frobenius" over K).

GALOIS CORRESPONDENCE

Let $F \subset E$ be a finite Galois extension. The map $K \mapsto \mathrm{Gal}(E/K)$ is an injection from **PROP 2.18**

$$\{\text{subfields } K : F \subset K \subset E\} \hookrightarrow \{\text{subgroups of } \mathrm{Gal}(E/F)\}$$

PROOF. We'll construct a left inverse for $K \mapsto \mathrm{Gal}(E/K)$. Let $H = \mathrm{Gal}(E/K) \subset \mathrm{Gal}(E/F)$. Consider E^H (recalling Def 2.9). This is K exactly by Thm 2.4. $\square$

If E/F is finite and Galois, then there are finitely many fields K such that $F \subset K \subset E$. **PROP 2.19**

If E/F is finite and separable, then there are finitely many subfields $F \subset K \subset E$. **PROP 2.20**

PROOF. Let E/F be separable and finite. Then E is generated by $\alpha_1, ..., \alpha_t$, where α_j is the root of a separable polynomial $g_j(X) \in F[x]$. Hence, $\widetilde{E}$, the splitting field of $g_1 \cdot ... \cdot g_t$, contains the generators of E, and hence $E \subset \widetilde{E}$. Since $g_1, ... g_t$ is separable, $\widetilde{E}/F$ is Galois. By the previous corollary, there are finitely many $K : F \subset K \subset \widetilde{E}$, and so finitely many $K : F \subset K \subset E$. $\square$

Eg. 1 We remark that E/F being separable is *essential*. As a counterexample, take $F = \mathbb{F}_p(u, v)$, the field of rational functions on two variables u, v, over $\mathbb{F}_p$. We then adjoin to F the p^{th} roots of u and v, and write $E = F(u^{1/p}, v^{1/p})$. Then $K_\alpha = F(u^{1/p} + \alpha v^{1/p})$ as $\alpha \in F$ are all distinct subfields $F \subset K \subset E$. E.G. 2.7

As proof, first note that $[E : F] = p^2$, since $u^{\frac{1}{p}}$ and $v^{\frac{1}{p}}$ are the roots of irreducible polynomials $x^p - u$ and $x^p - v$, respectively. Writing $E = F(u^{1/p})(v^{1/p})$, and noting that $x^p - v$ is still irreducible in $F(u^{1/p})$, delivers this fact.

Fix $\alpha \in F$. Then $K_\alpha = F(u^{1/p} + \alpha v^{1/p}) \subset E$, since we can write $u^{1/p} + \alpha v^{1/p}$ in E, and $F \subset E$. We also claim that K_α, K_β are distinct fields. If this were not the case, then $u^{1/p} + \alpha v^{1/p} - (u^{1/p} + \beta v^{1/p}) = (\alpha - \beta)v^{1/p}$. But then $(\alpha - \beta)^{-1}(\alpha - \beta)v^{1/p} = v^{1/p} \in K_\alpha = K_\beta$. But then $u^{1/p} + \beta v^{1/p} - \beta v^{1/p} = u^{1/p} \in K_\alpha = K_\beta$. Then $K_\alpha = K_\beta = E$. But E is of degree $p^2 \lightning$.

2.9 Primitive Element Theorem

Let E/F be finite and separable. Then $\exists \alpha \in E$ such that $E = F(\alpha) = F/\langle p(x) \rangle$, where p is the minimal irreducible polynomial of α in $F[x]$.

Let $H \subset \mathrm{Gal}(E/F)$. Then $[E : E^H] = \#H$. **PROP 2.21**

PROOF.

Proof under construction □

2.10 Galois Correspondence

Let F/E be finite and Galois. The maps

$$\{\text{subfields } F \subset K \subset E\} \leftrightarrows \{\text{subgroups } H \subset \mathrm{Gal}(E/F)\}$$

given by $K \mapsto \mathrm{Gal}(E/K)$ and $H \mapsto E^H$ are mutual, inclusion-reversing inverses.

PROOF.

We know that $H \mapsto E^H$ inverts $K \mapsto \mathrm{Gal}(E/K)$. To show the converse, consider E^H. We claim that $\mathrm{Gal}(E/E^H) = H$. But $H \subseteq \mathrm{Gal}(E/E^H)$, since $\varphi(\alpha) = \alpha$ for $\varphi \in H$, $\alpha \in E^H$, by construction. Prop 2.21 establishes $\#H = \mathrm{Gal}(E/E^H)$, and we are done.

If $K \subset L$ as subfields, then $\mathrm{Gal}(E/L) < \mathrm{Gal}(E/K)$ as subgroups (anything that fixes L will also fix K), so this map is inclusion reversing. □

E.G. 2.8

Eg. 1 Let $F = \mathbb{Q}$ and E be the splitting field of $x^4 - 2$. Let $E_0 = \mathbb{Q}(\sqrt[4]{2})$. In this field, then

$$x^4 - 2 = (x - \sqrt[4]{2})(x + \sqrt[4]{2})(x^2 + \sqrt{2})$$

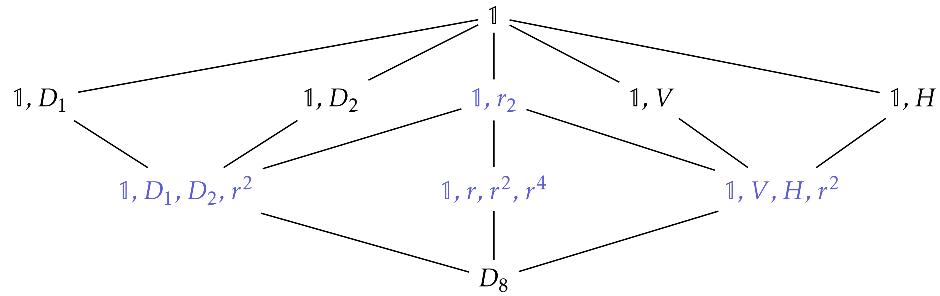
But $E_0 \subseteq \mathbb{R}$ (not $\mathbb{C}$), so we cannot factor the last term further. We conclude that $E = E_0[x]/(x^2 + \sqrt{2})$. This will have a root $i(\sqrt[4]{2})$, so we may adjoin $E = E_0(i(\sqrt[4]{2})) = E_0(i)$, and conclude $E = \mathbb{Q}(\sqrt[4]{2}, i)$.

$$\begin{tikzcd}
E = \mathbb{Q}(\sqrt[4]{2}, i) \arrow[d, dash, "2"] \arrow[dd, dash, bend right, "8"'] \\
E_0 = \mathbb{Q}(\sqrt[4]{2}) \arrow[d, dash, "4"] \\
\mathbb{Q}
\end{tikzcd}$$

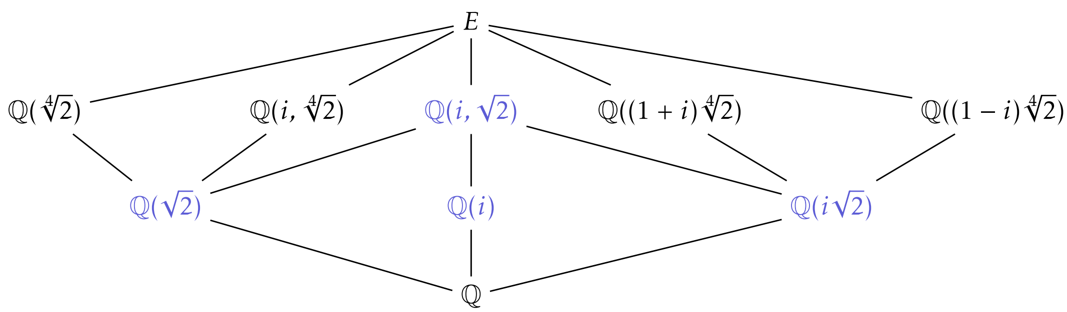
Let $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$. It is determined by where it sends $\sigma(r)$ and $\sigma(i)$, where $r = \sqrt[4]{2}$:

$$\sigma(r) \in \{r, -r, ir, -ir\} \qquad \sigma(i) \in \{i, -i\}$$

One computes the action of σ on the roots to find that $\mathrm{Gal}(E, \mathbb{Q}) \cong D_8$. We list the subgroup structure of D_8 (nontrivial normal subgroups in blue):



Using the Galois correspondence, with $H \mapsto E^H$, we generate the associated fixed fields (non-trivial Galois extensions in blue):



Note that each intermediary extension is of degree 2.

Let $\varphi \in \mathrm{Gal}(E/F)$, with $F \subset K \subset E$. Then $\varphi K = \{\varphi x : x \in K\}$, called the *complement*, is also a subfield $F \subset \varphi K \subset E$. DEF 2.15

Let $\varphi \in \mathrm{Gal}(E/F)$. If $H \leftrightarrow K$ under the Galois correspondence, then $\varphi H \varphi^{-1} \leftrightarrow \varphi K$. **PROP** 2.22

PROOF. $\mathrm{Gal}(E/\varphi K) = \{\alpha \in \mathrm{Gal}(E/F) : \alpha(\varphi x) = \varphi x \ \forall x \in K\}$. But then $\varphi^{-1}\alpha\varphi(x) = x$, so $\varphi^{-1}\alpha\varphi \in \mathrm{Gal}(E/K) = H$, and hence $\alpha \in \varphi H \varphi^{-1}$. □

2.11 Galois Intermediate Fields

Given $F \subset K \subset E$, the following are equivalent:

1. $\varphi K = K \ \forall \varphi \in \mathrm{Gal}(E/F)$
2. K is Galois over F
3. $\mathrm{Gal}(E/K)$ is a normal subgroup of $\mathrm{Gal}(E/F)$, with $\mathrm{Gal}(E/F)/\mathrm{Gal}(E/K) = \mathrm{Gal}(K/F)$ (as a quotient).

PROOF. $1 \implies 3$. Let $H = \mathrm{Gal}(E/K)$. Then if $\varphi K = K\ \forall \varphi \in \mathrm{Gal}(E/F)$, then $\varphi H \varphi^{-1} = H\ \forall \varphi \in \mathrm{Gal}(E/F)$ by Prop 2.22, i.e. $H < \mathrm{Gal}(E/F)$ is normal.

$1, 3 \implies 2$. Consider the restriction $\eta : \mathrm{Gal}(E/F) \to \mathrm{Aut}(K/F)$ (this is valid, since $\varphi K = K$ for $\varphi \in \mathrm{Gal}(E/F)$). This is a homomorphism. Then $\ker(\eta) = \mathrm{Gal}(E/K)$, so the isomorphism theorem tells us that $\mathrm{Gal}(E/F)/\mathrm{Gal}(E/K) \hookrightarrow \mathrm{Aut}(K/F)$.

But then $\frac{[E:F]}{[E:K]} \leq \#\mathrm{Aut}(K/F)$, while also, by multiplicity, $\frac{[E:F]}{[E:K]} = [K : F]$. We conclude that $[K : F] \leq \mathrm{Aut}(K/F)$, and so $\mathrm{Aut}(K/F) \leq [K : F]$ implies the result.

$3 \implies 1$. Let $H = \mathrm{Gal}(E/K)$. Then $H \leftrightarrow K$ in the Galois correspondence. By Prop 2.22, $\varphi H \varphi^{-1} \leftrightarrow \varphi K$. But $\varphi^{-1} H \varphi = H$ for $\varphi \in \mathrm{Gal}(E/F)$ by normality, so $H \leftrightarrow \varphi K$. Since the correspondence is one-to-one, $K = \varphi K$. □

DEF 2.16 An extension E/F is called a *radical extension* if $\exists n \geq 1$ and $\alpha \in F$ such that $E = F(\sqrt[n]{\alpha}) = F[x]/\langle x^n - \alpha\rangle$ (if $x^n - \alpha$ is irreducible) or $E = F(\sqrt[n]{\alpha}) = F[x]/\langle p(x)\rangle$, where $p | x^n - \alpha$ is an irreducible factor (if $x^n - \alpha$ is reducible).

DEF 2.17 A *tower of radical extensions* E/F is a sequence

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

where E_i/E_{i+1} is a radical extension, i.e. $E_i = E_{i+1}\ \sqrt[n_i]{\alpha_i} : n_i \geq 1, \alpha_i \in E_{i-1}$.

This definition is motivated by the following two questions: is every finite extension of $\mathbb{Q}$ contained in a tower of radical extensions?; and, given a polynomial $f(x) \in \mathbb{Q}[x]$, can its roots be expressed in terms of radicals?

Recall Def 2.5: an element $\alpha \in \mathbb{C}$ is constructible if it is contained in a tower of quadratic tower of extensions. We showed in Thm 2.2 that $\alpha \in \mathbb{R}$ is *not* constructible if $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. More generally, α is constructible only if $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^t$ for some t.

Our goal is to find a structural invariant of $\mathbb{Q}(\alpha)/\mathbb{Q}$ when α *is* constructible by radicals (not necessarily quadratic).

Let $E = F(\sqrt[n]{\alpha})$ for $\alpha \in F, n \geq 1$. This need not be Galois (see $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$). We know $\mathbb{Q}(\sqrt[n]{\alpha})$ is contained in the splitting field of $x^n - \alpha$, i.e. $\mathbb{Q}(\sqrt[n]{\alpha}, \xi)$, where ξ is a primitive n-th root of unity. Hence, if $\xi \in \mathbb{Q}(\sqrt[n]{\alpha})$, then we would have a simple structure for $\mathrm{Gal}(\mathbb{Q}(\sqrt[n]{\alpha})/\mathbb{Q})$.

It's automorphism group is trivial: we need to map roots of $x^3 - 2$ to roots of $x^3 - 2$, but there is only one in $\mathbb{Q}(\sqrt[3]{2})$, namely $\sqrt[3]{2}$

2.12 Galois Radical Extensions

Suppose that F contains distinct n-th roots of unity. Let $\mu_n(F) = \{x \in F^\times : x^n = 1\} \cong \mathbb{Z}/n\mathbb{Z}$. Then $F(\sqrt[n]{\alpha})$ is Galois with an abelian Galois group. Moreover, this group is (canonically) a subgroup of $\mu_n(F)$.

PROOF.

Let F be as above, and let $E = F(\sqrt[n]{\alpha})$. Consider the mapping

$$\eta : \mathrm{Aut}(E/F) \to \mu_n(F) \quad \varphi \mapsto \xi^j$$

where $\varphi(\sqrt[n]{\alpha}) = \xi^j \sqrt[n]{\alpha}$ for some j. One checks that η is indeed a homomorphism. It is also injective: $\eta(\varphi) = 1 \implies \varphi(\sqrt[n]{\alpha}) = \sqrt[n]{\alpha}$, so φ is the identity on E. Hence, $\mathrm{Aut}(E/F) \hookrightarrow \mu_n(F)$. Observe also that, since $\xi \in F$, $E = F(\sqrt[n]{\alpha}) = F(\sqrt[n]{\alpha}, \xi)$ is the splitting field of $x^n - \alpha$. □

Let char(F) = 0 from now on.

DEF 2.18

A finite group is *solvable* if there is a sequence

$$\{\mathbb{1}\} = G_0 \subset G_1 \subset \cdots \subset G_n = G$$

where $G_{i-1} < G_i$ is normal as a subgroup, and G_i/G_{i-1} is abelian.

DEF 2.19

We say that an extension E/F is *solvable* or *abelian* if its Galois group is solvable or abelian, respectively.

E.G. 2.9

Eg. 1 Every abelian group G is solvable, with a trivial sequence $\{1\} \subset G$.

Eg. 2 S_3 and S_4 are solvable, by the sequences

$$\{1\} \subset A_3 \subset S_3 \quad \text{and} \quad \{1\} \subset K_4 \subset A_4 \subset S_4$$

For S_3, observe that A_3 is normal in S_3, and $S_3/A_3 = \mathbb{Z}2$. The same holds for S_4 and A_4. We also have $A_4/K_4 = \mathbb{Z}3$.

Eg. 3 S_5 is *not* solvable, since it only has itself and $\{1\}$ as normal subgroups. But $S_5/\{1\} = S_5$ is not abelian.

PROP 2.23

If G is solvable, then any quotient $\overline{G}$ is solvable.

PROOF.

Let η be the quotient map on G. Then we may apply this map to all subgroups $G_i \subset G$, i.e. $\eta(G_i) = \overline{G_i}$, which make up its solvable sequence. η then induces a surjective homomorphism $\tilde{\eta} : G_i/G_{i-1} \to \overline{G_i}/\overline{G_{i-1}}$ by $\eta(\alpha G_{i-1}) = \eta(\alpha)\overline{G_{i-1}}$. We conclude that $\overline{G_i}/\overline{G_{i-1}}$ is abelian. η preserves normality, so we're done. □

PROP 2.24

If E/F is a tower of radical extensions, it is contained in a Galois extension $\tilde{E}/F$, where $\mathrm{Gal}(\tilde{E}/F)$ is solvable.

PROOF.

Proof under construction. □

2.13 Main Theorem of Galois Theory

If $f(x) \subseteq F[x]$ is solvable by radicals, then $\mathrm{Gal}(f)$ is a solvable group.

PROOF. We say that f is solvable by radicals if all its solutions are constructible with radicals (over the base field). Then, its splitting field E (generated by these roots) is contained in a tower of radical extensions, which itself is contained in a Galois extension $\tilde{E}$, for which $\mathrm{Gal}(\tilde{E}/F)$ is solvable. Therefore, $\mathrm{Gal}(E/F)$ is a quotient of $\mathrm{Gal}(\tilde{E}/F)$. (Refer to the proof of Thm 2.11). But solvability is preserved by taking quotients, so we are done. □

PROP 2.25 Every solvable extension of F is constructible by radicals.

PROOF. It is enough to show this for abelian extensions, i.e. E/F such that $\mathrm{Gal}(E/F)$ is abelian. Recall that if *any* E is solvable, then its Galois group G is such that

$$\{1\} = G_0 < \cdots < G_n = G$$

with G_i/G_{i-1} abelian and $G_{i-1} < G_i$ normal. The Galois correspondence yields

$$F = E_0 \subset \cdots \subset E_n = E$$

where $\mathrm{Gal}(E_i/E_{i-1})$ is abelian. Hence, if we consider the result on each sub-extension, also have the result for E. Also assume that F contains the n-th roots of unity, where $n = [E : F]$. (One *can* prove the result without this assumption).

We can view E as an F-linear representation of $G = \mathrm{Gal}(E/F)$. But G is abelian, so all its irreducible representations are 1-dim. (In the context of our previous results, F is "complex," since $\mathrm{char}(F) = 0$). Let $\hat{G} = \mathrm{Hom}(G, F^\times)$ (all representations of G), with

$$E = \bigoplus_{\chi \in \hat{G}} E[\chi]$$

where $E[\chi] = \{v \in E : \sigma v = \chi(\sigma)v \ \forall \sigma \in G\}$. We claim $\dim_F(E[\chi]) \leq 1$. Suppose $v \in E[\chi]$, with $v \neq 0$. Consider $\frac{w}{v}$ for some $w \in E[\chi]$. We would like this to be in F. (Then, one could write $w = \lambda v$ with $\lambda \in F$ for any $w \in E[\chi]$, i.e. $E[\chi] = \lambda F$. We conclude that $\dim_F(E[\chi]) \leq 1$).

$$\sigma\left(\frac{w}{v}\right) = \frac{\sigma w}{\sigma v} = \frac{\chi(\sigma)w}{\chi(\sigma)v} = \frac{w}{v} \ \forall \sigma \in G$$

so, by prior theory, $\frac{w}{v} \in E^G = F$, so $\dim_F(E[\chi]) \leq 1$ indeed. But $\dim_F(E) = [E : F] = \#G$ and $\dim_F\left(\oplus_\chi E[\chi]\right) \leq \#\hat{G} = \#G$. Hence, exactly, $\dim_F(E[\chi]) = 1$. Then, E is isomorphic to $F[G]$ as a G-representation (recall: the regular representation, Def 1.10).

For each $\chi \in \hat{G}$, let $y_\chi \in E[\chi]$ be a basis for it. Then $E = F(y_\chi : \chi \in \hat{G})$. Consider now y_χ^n:

$$\sigma(y_\chi^n) = [\sigma(y_\chi)]^n = [\chi(\sigma) y_\chi]^n = \chi(\sigma)^n y_\chi^n = y_\chi^n$$

we conclude that $y_\chi^n \in F$. Relabeling, $y_\chi^n = a_\chi \implies a_\chi^{\frac{1}{n}} = y_\chi$, and we rewrite

$$E = F(a_\chi^{\frac{1}{n}} : \chi \in \hat{G}) \qquad \square$$

Exercise: if G is a finite group, and $H < G$ is a solvable normal subgroup, with G/H also solvable, then G itself is solvable.

PROP 2.26 If $f(x)$ is a quintic polynomial, and $\mathrm{Gal}(f) = S_5$, then $f(x)$ is not solvable by radicals.

PROOF. If this were the case, then S_5 would be solvable. But we've seen in Example 2.9 that this is not possible. $\square$

In order for this proposition to be useful, we should demonstrate some quintic polynomial which has the full Galois group S_5:

PROP 2.27 Let G be a transitive subgroup of S_5 containing a transposition. Then $G = S_5$.

PROOF. Since G acts transitively on 5 element, $5 | \#G$. Hence, WLOG, $\sigma = (12345) \in G$. It also contains a transposition, say $\tau = (12) \in G$.

Conjugating by $\sigma^i : i < 5$, we get all the other transpositions. But S_5 is generated by all transpositions, and we are done. $\square$

Then, let f be a polynomial of degree 5 over $\mathbb{Q}$ which is irreducible over $\mathbb{Q}$. Suppose further that f has exactly 3 real roots and 2 complex roots. Then $\mathrm{Gal}(f)$ is a field whose Galois group is isomorphic to S_5.

PROOF. Let E be the splitting field of f. Then $\mathrm{Gal}(E/\mathbb{Q}) \subset S_5$ acts transitively on the 5 roots of f. Complex conjugation is an automorphism, and it must interchange the two complex roots. Hence, $\mathrm{Gal}(E/\mathbb{Q})$ contains a transposition. By Prop 2.26, $\mathrm{Gal}(E/\mathbb{Q}) \cong S_5$. $\square$

PROP 2.28 If $n \geq 4$, then S_{n-1} is the maximal subgroup of S_n.

PROOF. *Proof under construction.* $\square$

PROP 2.29 If α satisfies a polynomial f of degree $n \geq 4$, and $\mathrm{Gal}(f) \cong S_n$, then α is not constructible.

PROOF. We have, by the Galois correspondence,

$$\begin{tikzcd}
\mathrm{Gal}(E/\mathbb{Q}(\alpha)) = S_{n-1} \arrow[r, dotted, dash] & \mathbb{Q}(\alpha) \arrow[d, dash, "8"] \\
\mathrm{Gal}(E/\mathbb{Q}) = \mathrm{Gal}(f) = S_n \arrow[r, dotted, dash] & \mathbb{Q}
\end{tikzcd}$$

But, if α were constructible, we'd need intermediate fields between $\mathbb{Q}(\alpha)$ and $\mathbb{Q}$. By the Galois correspondence, then, we'd find a subgroup $S_{n-1} \subset H \subset S_n$, violating Prop 2.28. $\square$

2.14 Fundamental Theorem of Algebra

$\mathbb{C}$ is algebraically closed.

PROOF. We'll use the following two (analytic) facts: every polynomial of odd degree in $\mathbb{R}[x]$ has a root in $\mathbb{R}$. Equivalently, every odd-degree extension of $\mathbb{R}$ is trivial. Secondly, every quadratic equation in $\mathbb{C}[x]$ has a root in $\mathbb{C}$.

This follows from the IVT.

Let K be a finite extension of $\mathbb{C}$. Then K is an even degree extension of $\mathbb{R}$. Let K' be the Galois closure of K over $\mathbb{R}$, and consider $G = \mathrm{Gal}(K'/\mathbb{R})$. We have $\#G = 2^t m$, where m is odd, since this extension must be odd. By the Sylow theorems, there exists a subgroup $S \subset G$ of size 2^t.

$$\begin{tikzcd}
 & & K' \arrow[dd, dash, "2^t"] \arrow[ddrr, dash, "2^{t-1}"] \arrow[drr, dash] \arrow[dddr, dash, bend right] & & & \\
 & & & & K \arrow[d, dash] & \\
 & S \arrow[r, dotted, leftrightarrow] & F \arrow[dr, dash, "m"] & & \mathbb{C} \arrow[dl, dash, "2"] \arrow[r, dotted, leftrightarrow] & G_0 = \mathrm{Gal}(K'/\mathbb{C}) \\
\mathrm{Gal}(K'/\mathbb{R}) = G \arrow[rrr, dotted, leftrightarrow] & & & \mathbb{R} & &
\end{tikzcd}$$

The field $F = K'^S$ has $[K' : F] = 2^t$, so F is odd degree m over $\mathbb{R}$. Hence $F = \mathbb{R}$, so $G = S$. We conclude $\#G = 2^t$, and $\#G_0 := \#\mathrm{Gal}(K'/\mathbb{C}) = 2^{t-1}$. If $G_0 \neq \{1\}$, then it contains a subgroup G_{00} of index 2 in G_0. Then $[K' : K'^{G_{00}}] = 2^{t-1}$, so this is a quadratic extension of $\mathbb{C}$. But we know no such extensions exist.

$\implies G_0 = \{1\} \implies K' = \mathbb{C}$, and we are done. $\square$