Honours Algebra IV

MATH 457

Nicholas Hayek

Lectures by Prof. Henri Darmon

CONTENTS

In Algebra III, we studied 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 ↔ vector spaces) and Galois theory (fields ↔ groups).

GALOIS MOTIVATION

Consider $ax^2 + bx + c = 0 : a, b, c \in \mathbb{F}$. A solution is given by the quadratic equation, which contains the root of the discriminant, i.e. $b^2 - 4ac$. There are similar formulas for the general cubic and quadratic, which contain cube and square roots. Is there a general solution for a n^{th} order equation? This question motivates Galois theory. No.

Galois was able to associate every polynomial $f(x) = a_n x^n + ... + a_0 : a_i \in \mathbb{F}$ to a group, which encodes whether $f(x)$ is solvable by radicals.

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 $m_g(v) = gv$ is 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 linear combinations $\{\sum_{g\in G} \lambda_g g : \lambda_g \in \mathbb{F}\}$. It's endowed with the multiplication 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, $(\sum \lambda_g)v = \sum \lambda_g(gv)$. Then, instead of viewing 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 $\mathbb{F}[G]$.

DEF 1.3

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

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 is never a transitive G-set, since $g\vec{0} = \vec{0} \; \forall g$.

E.G. 1.1

♠ *Examples* ♣

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.

If T_i commute with eachother, then they have a simultaneous eigenvector $v \in V$ (see Prop 1.1). Hence, the scalar multiples of v comprise a G-stable subspace, so the representation V is irreducible if $\dim(V) = 1$.

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). □

♠ *Examples* ♣ 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 is an eigenvalue of $T = \rho(23)$. Let e_1 be a non-zero vector fixed by T, i.e. $Te_1 = e_1$. Then let $e_2 = (123)e_1$ and $e_3 = (123)^2 e_1$. Then $\{e_1, e_2, e_3\}$ is an S_3-stable subspace, so $V = \mathrm{span}(e_1, e_2, e_3)$.

↪ *Case 2a:* $w = e_1 + e_2 + e_3 \neq 0$. Then S_3 fixes w. One checks that $\sigma(e_i + e_j + e_k) = e_{\sigma(i)} + e_{\sigma(j)} + e_{\sigma(k)}$. Hence, $\sigma w = w$.

↪ *Case 2b:* $e_1 + e_2 + e_3 = 0$. Then $V = \mathrm{span}(e_1, e_2, e_3)$ as before. $\dim(V) \leq 2$, and $e_1 \neq e_2 \neq e_3$. Then $(23)e_1 = e_1$ and $(23)(e_2 - e_3) = e_3 - e_2 = -(e_2 - e_3)$. Hence, we have two eigenvalues for $\rho(23)$, so $\dim(V) \geq 2 \implies \dim(V) = 2$.

Relative to the basis e_1, e_2 for V, the representation of S_3 is given by

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

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

Conclusion: there are essentially 3 distinct, irreducible representations of S_3:

1. $\mathrm{sgn} : S_3 \to \mathbb{C}^*$
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 φ is a vector space isomorphism, then $V_1 \cong V_2$ as representations. DEF 1.5

E.G. 1.3 ♠ *Examples* ♣

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 $\rho : D_8 \to \mathrm{Aut}_{\mathbb{F}}(V)$, where $2 \neq 0$ by assumption.

Consider r^2. It commutes with everything. Then $T = \rho(r^2) \in \mathrm{Aut}_{\mathbb{F}}(V)$ 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 $Tgv = r^2gv = gr^2v = gTv = gv$. 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 $\ker(\rho) \subseteq \{1, r^2\})$. We can write the following, then:

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

Since $2\mathbb{Z} \times 2\mathbb{Z} = K_4$ is abelian, we have 4 1-dim irreducible representations φ into $\mathrm{Aut}(V)$. 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 $\rho(V) = \rho(r^2H) = -I$. 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 $rv_2 = r^2v_1 = -v_1$, 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, $Hv_2 = Hrv_1 = r^{-1}Hv_1 = r^{-1}v_1 = r^3v_1 = r^2v_2 = -v_2$. 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?

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

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 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: 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 $e_1 \in W$ ↯.

Remark 3: $\mathbb{C}$ is necessary. Let $\mathbb{F} = \mathbb{Z}/3\mathbb{Z}, G = S_3$. Then let $V = \mathbb{F}e_1 + \mathbb{F}e_2 + \mathbb{F}e_3$. $\mathbb{F}(e_1 + e_2 + e_3)$ is an irreducible 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, $(a + b + c)(e_1 + e_2 + e_3) \in W$.

We have, then, that $(a - b)(e_1 - e_2), (b - c)(e_2 - e_3), (a - c)(e_1 - e_3) \in W$. At least one of these must be non-zero, WLOG take $a - b \neq 0$. Then $e_1 - e_2, e_2 - e_3, e_3 - e_1 \in W$.

We find $e_1 + e_2 + e_3 \in W$, so $W \subseteq \mathbb{F}(e_1 + e_2 + e_3)$ ↯.

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 a projection $\pi_0 : V \to W$ with $\pi_0^2 = \pi_0$, $\text{Im}(\pi_0) = W$. 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. $\pi \in \text{End}_{\mathbb{C}}(V)$.
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. $\text{Im}(\pi) = W$. $\text{Im}(\pi) \subseteq W$. But let $w \in W$. Then $\pi(w) = w$ (check it).
4. $\pi(hv) = h\pi(v)\ \forall h \in G$. See that

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

   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

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

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

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 $\langle v, \lambda w\rangle = \overline{\lambda}\langle v, w\rangle$. This "skew linearity" in the second argument allows us to impose $\langle v, v\rangle \in \mathbb{R}^+$ 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, $\langle\ ,\ \rangle$ 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 ask the following 2 questions:

1. Given G, produce the complete list of 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 $T : V \to W$.

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 $\ker(T - \lambda I) = V \implies T = \lambda I$. □

Recall question (2) from above. As a corollary of Schur's Lemma, we see that $m_j = \dim_{\mathbb{C}} \operatorname{Hom}_G(V_j, V)$.

PROOF.

$$\operatorname{Hom}_G(V_j, V) = \operatorname{Hom}_G(V_j, V_1 \oplus \ldots \oplus V_s) = \bigoplus_{i \in I} \operatorname{Hom}(V_j, V_i) : V_i \cong V_j \; \forall i \in I$$
$$= \underbrace{\mathbb{C} \oplus \ldots \oplus \mathbb{C}}_{|I| = m_j \text{ times}} \implies \dim \operatorname{Hom}_G(V_j, V) = m_j \quad \square$$

DEF 1.7 For an endomorphism $T : V \to V$, the *trace*, $\operatorname{tr}(T)$, is defined as $\operatorname{tr}([T]_\beta)$, 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 1.3 Let $W \subseteq V$ be a subspace and π be a function $V \to W$ such that $\pi^2 = \pi$ and $\operatorname{Im}(\pi) = W$. Then $\operatorname{tr}(\pi) = \dim(W)$.

PROOF. Let $v_1, \ldots, v_d$ be a basis for W and $v_{d+1}, \ldots, d_n$ be a basis for $\ker(\pi)$. Then, since we can write $V = W \oplus \ker(\pi)$ (recall projection properties), $\beta = d_1, \ldots, d_n$ is a basis for V. In this basis, $\pi(v_i) = v_i$ for $1 \leq i \leq d$. 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 $v_i : i \leq d$, so, in particular, they will not have diagonal 1 entries. Since $d = \dim(W)$, we conclude $\operatorname{tr}(\pi) = \dim(W)$. $\square$

DEF 1.8 $V^G = \{v \in V : gv = v \forall g \in G\}$. If $V_1 = \mathbb{C}$ is the trivial action of G, then $\operatorname{Hom}_G(V_1, V) = V^G$.

PROP 1.4 $V^G = \cap_{g \in G}$ (1-eigenspaces for $\rho(g)$)

1.6 Burnside

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

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

PROOF.

By Prop 1.3, for a projection $\pi : V \to W$ (i.e. $\text{Im}(\pi) = W, \pi^2 = \pi$), we have $\text{tr}(\pi) = \dim(W)$. Consider

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

Note that $\text{Im}(\pi) \subseteq V^G$. 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, $V^G = \text{Im}(\pi)$ exactly. This also shows that $\pi^2(v) = \pi(v)$. We conclude that π projects $V \to V^G$.

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

□

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

PROOF. Consider later. □

CHARACTERS

DEF 1.9 If V is a finite dimensional, complex representation of G, then the *character* of V is the function $\chi_V : G \to \mathbb{C}$ such that

$$\chi_V(g) = \text{tr}(\rho(g))$$

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

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

E.G. 1.4 ♠ *Examples* ♣

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

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

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

Denote these representations by "triv," "sgn," and 2, respectively.

The conjugacy classes and associated traces are hence 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 $D_8/\langle 1, r_2\rangle = \mathbb{Z}_2 \times \mathbb{Z}_2$. Denote these by $\chi_{\text{triv}}, ..., \chi_4$. We also have the unique 2-dim irreducible representation given by

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

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

	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_5	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. 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.

$\chi_V(\mathbb{1}) = \dim(V)$ PROP 1.7

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 $gT = g \circ T \circ g^{-1}$

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

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

1.7 Character of $\text{Hom}(V,W)$

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

PROOF. Let $g \in G$. Then $\rho_V(g)$ acting on V is diagonalizable. Let $e_1, ..., e_m$ be a basis of eigenvectors for $\rho_V(g)$, with $m = \dim(V)$, and $ge_i = \alpha_i e_i$.

Similarly, let $f_1, ..., f_n$ 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 $1 \leq i \leq m$ and $1 \leq j \leq n$, be the following transofmrations

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

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

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

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

Orthogonality of Irreducible Group Characters

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

$\chi_j \in L^2(G)$. Given $f_1, f_2 \in L^2(G) \approx \mathbb{C}^{\#G}$, 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

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

PROOF.

$$\begin{aligned}\langle \chi_i, \chi_j \rangle &= \frac{1}{\#G}\sum_{g\in G}\overline{\chi_i(g)}\chi_j(g) \\ &= \frac{1}{\#G}\sum_{g\in G}\chi_{\mathrm{Hom}(V_i,V_j)}(g) && \text{by Thm 1.8} \\ &= \dim_{\mathbb{C}}(\mathrm{Hom}(V_i,V_j)^G) && \text{by Thm 1.6} \\ &= \dim_{\mathbb{C}}(\mathrm{Hom}_G(V_i,V_j)) = \dim_{\mathbb{C}}\begin{cases}\mathbb{C} & i = j \\ 0 & o.w.\end{cases} && \text{by Thm 1.5} \\ &= \begin{cases} 1 & i = j \\ 0 & o.w. \end{cases} \quad \square\end{aligned}$$

$\chi_1, \ldots, \chi_t$ is an orthonormal system of vectors in $L^2(G)$. PROP 1.10 i.e. an orthonormal basis

$\chi_1, \ldots, \chi_t$ are linearly independent. Hence $t \leq \dim(L^2(G)) = \#G$. PROP 1.11

$t \leq h(G)$, the number of conjugacy classes of G. PROP 1.12

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 $h(G)$. □

♠ *Examples* ♣ 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 $d_1 = \ldots = d_4 = 1$ 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. $V = V_1^{m_1} \oplus \cdots \oplus V_t^{m_t}$, where V_i are irreducible, by Thm 1.2. Then

$$\chi_V = m_1\chi_1 + \ldots + m_t\chi_t$$

Note that, by the orthogonality of characters, $\langle \chi_V, \chi_j \rangle = m_j$, and hence V is determined by χ_V. □

Regular Representations of G

In Prop 1.11, we argued that, for characters $\chi_1, \ldots, \chi_t$, $t \le h(G)$, the class number of G, by seeing that $\{\chi_1, \ldots, \chi_t\} \subseteq L^2_{\text{class}}(G)$.

DEF 1.10 Consider $\mathbb{C}[G] = \{\sum_{g\in G} \lambda_g g : \lambda_g \in \mathbb{C}\}$. Then $G \circlearrowleft \mathbb{C}[G]$ by left multiplication. We call $\mathbb{C}[G]$ the *regular representation*, and denote $V_{\text{reg}} = \mathbb{C}[G]$.

PROP 1.13

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

PROP 1.14 Every irreducible representation 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 1.15 We conclude $\#G = d_1^2 + \ldots + d_t^2$.

PROOF.

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

1.10

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 $\rho = (\rho_1, \ldots, \rho_t) = G \to \mathrm{Aut}(V_1) \times \cdots \times \mathrm{Aut}(V_t)$. We can write $\rho : \mathbb{C}[G] \to \mathrm{End}_{\mathbb{C}}(V_1) \oplus \cdots \oplus \mathrm{End}_C(V_t)$ by linearity, i.e.

$$\sum \lambda_g g \to \Big(\sum \lambda_g \rho_1(g), \ldots, \sum \lambda_g \rho_t(g)\Big)$$

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

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 $V_1, \ldots, V_t$ 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 $\hat{G} = \{\text{irrep of } G\}$. 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

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

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 PROP 1.16

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

Given $f \in L^2(G)$, the function $\hat{f} : \hat{G} \to \mathbb{C}$ defined by DEF 1.11

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

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

Correspondingly, DEF 1.12

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

is called the *Fourier inversion formula*.

♠ *Examples* ♣ 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,

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

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
$\chi_{\text{sgn}} = \chi_2$	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.

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:

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

	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	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

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 1.13

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 1.17

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 1.18

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

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,

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

□

1.12

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

PROOF.

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

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

♠ *Examples* ♣

E.G. 1.7

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

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

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 class	1 $1A$	21 $2A$	56 $3A$	42 $4A$	24 $7A$	24 $7B$
$\chi_{\text{triv}} = \chi_1$	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 $\chi_{V^*} = \overline{\chi_V}$.

$V_1 \otimes V_2 := \mathrm{Hom}_C(V_1^*, V_2)$ is the *tensor product* of V_1 and V_2. DEF 1.14

$\dim(V_1 \otimes V_2) = \dim(V_1)\dim(V_2)$. PROP 1.19

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 $\ell \in V_1^* \mapsto \ell(v_1)v_2$. DEF 1.15

Let $e_1, ..., e_n$ be a basis for V_1 and $f_1, ..., f_m$ be a basis for V_2. Let $v_1 = a_1e_1 + ... + a_ne_n$ and $v_2 = b_1f_1 + ... + b_mf_m$. Then

$$v_1 \otimes v_2 = (a_1e_1 + ... + a_ne_n) \otimes (b_1f_1 + ... + b_mf_m) = \sum a_ib_j(e_i \otimes f_j)$$

G acts on $V_1 \otimes V_2$ by $g(v_1 \otimes v_2) = (gv_1) \otimes (gv_2)$. Then $\chi_{V_1 \otimes V_2} = \chi_{V_1}\chi_{V_2}$. PROP 1.20

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

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

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 $T(v) = \lambda_jv\ \forall v \in V_j$. 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

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

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 ♠ *Examples* ♣

Finite, C-valued functions on X

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.

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. DEF 1.16

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

DEF 2.1 If E and F are fields, then E is an *extension* of F if F is a subfield of E.

We always take fields to be commutative, unless specified.

If E is an extension of F, then E is also a vector space over F. Hence, we have

DEF 2.2 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 2.3 E over F is called a *finite* extension if $[E : F] < \infty$.

E.G. 2.1 ♠ *Examples* ♣

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 F be arbitrary, and $E = F[x]/\langle p(x)\rangle$, where p is irreducible, i.e. E are polynomials in F with degree $< p(x)$. In particular, E is an extension of F, and $[E : F] = \deg(p)$.

Eg 4: 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.

2.1 Multiplicity of the 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

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 quadratic extensions $\mathbb{Q} \subset F_1 \subset \cdots \subset F_n$ such that $[F_{i+1} : F_i] = 2$ and $\alpha \in F_n$.

The set of elements constructible by ruler and compass is an extension of $\mathbb{Q}$ of infinite degree.

2.2 Non-Constructible Roots

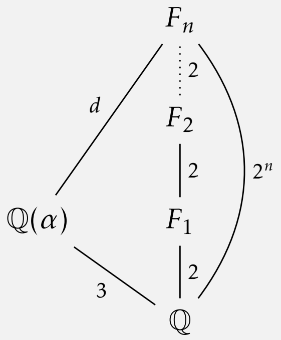
If $\alpha \in \mathbb{R}$ satisfies an irreducible, cubic polynomial over $\mathbb{Q}$, then α is not constructible by ruler and compass.

In fact, if $\alpha \in \mathbb{R}$ satisfies any odd-degree irreducible, then this holds

PROOF.

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

But $\mathbb{Q}[x]/p(x) = \mathbb{Q}(\alpha)$ for the cubic p of interest, where we consider the homomorphism $\mathbb{Q}[x] \to \mathbb{Q}(\alpha)$ by $f(x) \to f(\alpha)$. We can write, then $[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}[x]/p(x) : \mathbb{Q}] = 3$. 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. In other words, $3d = 2^n$, which is a contradiction.



In fact, then if $\alpha \in \mathbb{R}$ satisfies any irreducible, odd-degree polynomial over $\mathbb{Q}$, we get this result. □

E.G. 2.2

♠ *Examples* ♣

As a consequence of Thm 2.2, we cannot duplicate the unit cube, since $\sqrt[3]{2}$ is not constructible (is it the root of $x^3 - 2$). Similarly, we cannot trisect an angle, since $\cos(\frac{2\pi}{9})$ satisfies $4x^3 - 3x + \frac{1}{2} = 0$.

DEF 2.5 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 $F[x]$.

For example, $\sqrt{2}$ is algebraic over $\mathbb{Q}$ (see $x^2 - 2$), and i is algebraic over $\mathbb{Q}$ and $\mathbb{R}$ (see $x^2 + 1$). However, π is *not* algebraic over $\mathbb{Q}$, but it is algebraic over $\mathbb{Q}(\pi^3)$ (see $x^3 - \pi^3$). 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 2.1 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 2.6 The automorphism group of E/F is

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

PROP 2.2 $\sigma(1) = 1, \sigma(0) = 0, \sigma(a^{-1}) = \sigma(a)^{-1}$ for $\sigma \in \mathrm{Aut}(E/F)$.

PROP 2.3 If $[E : F] < \infty$, then $\mathrm{Aut}(E/F)$ acts on E with finite orbits.

PROOF. Consider an element $\alpha \in E$. Since α is algebraic for F, there is a polynomial $a_n\alpha^n + ... + a_1\alpha + a_0 = 0$, where $a_i \in F$. Let $\sigma \in \mathrm{Aut}(E/F)$. Then

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

by Prop 2.2. But, by linearity and vanishing conditions, this is also

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

We conclude: if α is a root of $f(x) \in F[x]$, then $\sigma(\alpha)$ is a root of $f(x)$. Hence, the orbit of α under the action of $\mathrm{Aut}(E/F)$ will be contained in the roots of $f(x)$, which is finite. □

We only used the fact, here, that $\alpha \in E$ is algebraic. Hence, if E/F is an algebraic extension (i.e. all $\alpha \in E$ are algebraic), then the result also holds.

PROP 2.4 If $[E : F] < \infty$, then $\#\mathrm{Aut}(E/F) < \infty$.

PROOF. Let $\alpha_1, ..., \alpha_n$ be generators for E over F. Let $G = \mathrm{Aut}(E/F)$. Then

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

If $\sigma \in \mathrm{Aut}(E/F)$, then σ is completely determined by $(\sigma(\alpha_1), ..., \sigma(\alpha_n))$, which is completely contained in

$$\mathrm{orb}_G(\alpha_1) \times \cdots \times \mathrm{orb}_G(\alpha_n) \quad \square$$

♠ *Examples* ♣ E.G. 2.3

Suppose that E is generated over F by a single element α. Then $E = F(\alpha)$. Let $p(x) \in F[x]$ be the minimal polynomial of α. We have $\mathrm{ev}_\alpha : F[x] \to F[\alpha]$ by $f(x) \mapsto \alpha$. Then $\ker(\mathrm{ev}_\alpha) = (p(x))$. Hence, $F[x]/(p(x)) \cong F[\alpha]$.

$F[x]/(p(x))$ is an integral domain, and hence a field, so $F[\alpha] = F(\alpha)$. Hence $[F(\alpha) : F] = \deg(p)$.

$\sigma \in \mathrm{Aut}(F(\alpha)/F)$ is determined by $\sigma\alpha \in \{\text{ roots of } p(x)\}$, which, as a set, is $\leq \deg(p(x)) = [F(\alpha) : F]$, so we have

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

This inequality is true in general.

Any homomorphism $\varphi : E \to E$ is automatically injective. In fact, since $[E : F] < \infty$, it is automatically surjective as well. PROP 2.5

If E/F is any finite extension of fields, then $\#\mathrm{Aut}(E/F) \leq [E : F]$. PROP 2.6

PROOF. We'll proceed by induction on the number of generators for E over F. Let $E = F(\alpha_1, ..., \alpha_n)$.

Notice $\mathrm{Aut}(E/F) = \mathrm{Hom}_F(E, E)$. 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 $n = 1$ is similar to the example above. $E = F(\alpha) = F[\alpha]$, where $p_\alpha(x) \in F[x]$ is the minimal polynomial of α. Then $d = [E : F] = \deg(p_\alpha(x))$.

Consider $\varphi \in \mathrm{Hom}_F(E, M)$. Then the map $\varphi \to \varphi(\alpha)$ is an inclusion $\mathrm{Hom}_F(E, M)$ into the roots of $p_\alpha(x)$ in M, by observing

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

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 $[E : F'] = d_2$.

Let $g(x) \in F'[x]$ be the minimal polynomial of α_{n+1}. Then $d_2 = \deg(g(x))$. Compute the restriction map

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

We know, by induction, $\#\mathrm{Hom}_F(F', M) \leq [F' : F] = d_1$. We ask: given $\varphi_0 \in \mathrm{Hom}_F(F', M)$, how many $\varphi : E \to M$'s exist such that $\varphi|_{F'} = \varphi_0$? Consider

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

α_{n+1} satisfies g. Then $\varphi(\alpha_{n+1})$ is a root of the polynomial $\varphi_0(g(x)) \in M[x]$, so there at most d_2 choices of roots. Hence, $\#\mathrm{Hom}_F(E, M) \leq d_1 \cdot d_2 = [E : F]$. □

DEF 2.7 An extension E/F is called *Galois* is $\#\mathrm{Aut}(E/F) = [E : F]$. We the write $\mathrm{Gal}(E/F) := \mathrm{Aut}(E/F)$.

E.G. 2.4 ♠ *Examples* ♣

Eg 1: Let $F = \mathbb{C}$ and $F = \mathbb{R}$, $[E : F] = 2$. We have $c : \mathbb{C} \to \mathbb{C}$ by $x + iy \mapsto x - iy$. This is a field automorphism, so $\mathrm{Aut}(\mathbb{C}/\mathbb{R}) \subseteq \{1, c\}$, and indeed $= \{1, c\}$, since $\#\mathrm{Aut}(\mathbb{C}/\mathbb{R}) \leq [\mathbb{C} : \mathbb{R}] \leq 2$.

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 $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$. But the only such root *is* $\sqrt[3]{2}$, so $\#\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = 1 < 3$, so $\mathbb{Q}(\sqrt[3]{2})$ 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 the cube root of unity, and satisfies $x^2 + x + 1$. We claim that E is Galois.

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

Hence, $[E : \mathbb{Q}] = 6$. Now let $\varphi \in \mathrm{Aut}(E/\mathbb{Q})$. Then $\varphi(\xi)$ 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 $\overline{\xi}\sqrt[3]{2}$.

Now, let $r_1 = \sqrt[3]{2}$, $r_2 = \xi\sqrt[3]{2}$, and $r_3 = \overline{\xi}\sqrt[3]{2}$. These are the three roots of $x^3 - 2$. We will construct a table of automorphisms depending on where φ sends ξ and $\sqrt[3]{2}$.

	$\xi \to \xi$	$\xi \to \overline{\xi}$
$\sqrt[3]{2} \to \sqrt[3]{2}$	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 2.8 Let E/F be a finite Galois extension. Consider $G = \mathrm{Gal}(E/F)$. Then

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

PROP 2.7 E^G is a subfield of E, which contains F.

2.3 $E^G = F$

PROOF.

$$\begin{tikzcd}
E \arrow[d, dash] \\
E^G \arrow[d, dash] \\
F
\end{tikzcd}$$

We know $\#G \leq [E : E^G]$, since $G \subset \mathrm{Aut}(E/E^G)$, and also $[E : F] = \#G$, since E/F is Galois. But $[E : E^G] | [E : F]$ by multiplicity, so we conclude $[E : E^G] = [E : F] \implies [E^G : F] = 1$. Hence, $E^G = F$ exactly. □

2.4 If E/F is Galois, it is Normal

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

PROOF.

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

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

Exanded out, we get

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

where σ_i are the "elementary symmetric functions" in $r_1, ..., r_n$, e.g. $\sigma_1 = r_1 + ... + r_n$ and $\sigma_n = r_1 \cdots r_n$. We find that $\sigma_j \in E^G$, since $G = \mathrm{Gal}(E/R)$ permutes the roots $r_1, ..., r_n$, and σ_i are symmetric. But $E^G = F$, so $\sigma_i \in F$. Hence, $g(x) \in F[x]$.

$f(x)$ is the minimal polynomial which vanishes r over F, since it is irreducible, so $f(x) | g(x) = (x - r_1) \cdots (x - r_n)$, as desired. □

SPLITTING FIELDS

DEF 2.9

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 $E[x]$:

$$f(x) = (x - r_1) \cdots (x - r_n) : r_n \in E$$

2. E is generated, as a field, by the roots $r_1, ..., r_n$.

PROP 2.8 The 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 $f(x)$. Consider $L = F[x]/(p(x))$. 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, and in particular recall that $r = x + (p(x))$. Then $x - r$ divides $f(x)$ in $L[x]$, i.e. we can write $f(x) = (x - r)g(x)$, with $\deg(g) = n$.

See March 17th, 45:00min

Let E be the splitting field of $g(x)$ over L. □

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

$$n \leq [E : F] \leq n!$$

2.5 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. We'll show again 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 the splitting field E. Similarly, let r' be a root of $p(x)$ in E'. We know that $F(r)$ and $F(r')$ are isomorphic over F, since hey are both $F[x]/p(x)$. Let φ be the isomorphism $F(r) \to F(r')$.

Denote $L = F(r) = F(r')$. Then notice that E, E' are splitting fields of $g(x) : (x - r)g(x) = f(x)$ over L, so E and E' are isomorphic as extensions of L, and hence F. □

PROP 2.9 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 $\alpha_1, ..., \alpha_n$ be a finite set of generators for E/F. Let $f_1, ..., f_n$ be the minimal irreducible polynomials in $F[x]$ having these roots.

Consider $f(x) = f_1(x) \cdots f_n(x)$. By normality of $E[x]$ (see Thm 2.4), all the $f_j's$ factor completely in $E[x]$, and hence in F. The roots of $f(x)$ generate E, so E is a splitting field of $f(x)$. □

Recall that any finite field F contains $\mathbb{F}_p$ for some prime p, notably $p = \text{char}(F)$. Then, let $n := \dim_{\mathbb{F}_p}(F)$. We have $\#F = p^n$.

2.6 Unique Field of Prime Power Cardinality

Given a prime p and an integer $n \geq 1$, there is a field F of cardinality p^n. Furthermore, this field is unique.

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.

If F is a field of cardinality p^n, then $F^\times$ is an abelian, cyclic group of cardinality $p^n - 1$. Hence, for all elements $x \in F^\times$, $x^{p^n-1} \equiv 1$, and hence $x^{p^n-1} - 1 \equiv 0 \implies x^{p^n} - 1 \equiv 0$.

F is then the collection of roots of the polynomial $x^{p^n} - x$. Let F be the splitting field of $x^{p^n} - x$.

Claim: This is the a field of cardinality p^n. Note that $x^{p^n} - x$ has distinct roots in any extension of $\mathbb{F}_p$.

$$f(x) = x^{p^n} - x \implies f'(x) = -1$$

by considering the identity above. Hence, $\gcd(f, f') = 1$, and $\#F \geq p^n$. 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 2.5. □

Note that F, as constructed above, is an extension of $\mathbb{F}^p$. Is it Galois?

DEF 2.10

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

Because φ is a homomorphism, it injects $F \hookrightarrow F$; but, as $\dim_{\mathbb{F}_p}(F) < \infty$, φ is a bijection, and hence an automorphism. We can write $\varphi \in \mathrm{Aut}(F/\mathbb{F}_p)$. What is the order of φ? $\varphi^k(a) = a^{p^k}$. What 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:

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