ALGEBRA IV NOTES

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 $\leftrightarrow$ vector spaces) and Galois theory (fields $\leftrightarrow$ 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, $(\sum \lambda_g)v = \sum \lambda_g (gv)$.

A representation V of G is *irreducible* if there is no G-stable, non-trivial sub- DEF 1.3

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

space $W \subsetneq V$. 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 $(0,1)$.

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.

It's a fact that, if T_i commute with eachother, then they have a simultaneous eigenvector $v \in V$. 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). $\square$

♠ *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 $\boxed{\rho(g) = \mathrm{sgn}(g)}$ (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 $V = \mathrm{span}(e_1, e_2, e_3)$.

$\hookrightarrow$ *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, $\sigma w = w$.

$\hookrightarrow$ *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

DEF 1.5 If a G-homomorphism φ is a vector space isomorphism, then $V_1 \cong V_2$ as representations.

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:

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

Since $2\mathbb{Z} \times 2\mathbb{Z} = K_4$ is abelian, we have 4 1-dim irreducible representations φ into $\mathrm{Aut}(V)$. 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 Prop 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 $e_1 - e_2, e_2 - e_3, e_3 - e_1 \in W$.

Observe now that $(e_1 - e_2) + (e_2 - e_3) - (e_3 - e_1) = 2e_1 -$ BLAH. it works out. Show that $e_1 + e_2 + e_3 \in W \implies W \subseteq \mathbb{F}(e_1 + e_2 + e_3)$.

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 $w \in W' \implies \pi(gw) = g\pi(w) = g0 = 0 \implies gw \in W'$. $\square$

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 Hermitian Pairing on Representation

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

$$\langle gv, gw\rangle = \langle v, w\rangle \ \forall g \in G, v, w \in V$$

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 Prop 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 $\langle hv, hw\rangle = \langle v, w\rangle$. $\square$

Let $G = S_3$. We saw there is a unique 2-dim representation of S_3, where we construct $e_1, e_2, e_3 \in V$ with $e_1 + e_2 + e_3 = 0$ such that σ simply permutes the vectors. However, they are not necessarily the same "length."

PROOF OF 1.2

Now, to 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. $v \in W^{\perp} \implies \langle gv, w \rangle = \left\langle v, g^{-1}w \right\rangle = 0 \implies gv \in W^{\perp}$.

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

$$\mathrm{Hom}_G(V, W) = \begin{cases} 0 & V \not\cong W \\ \mathbb{C} & V \cong W \end{cases}$$

PROOF.

Suppose that $V \not\cong W$, 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 irreducible 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 $\ker(T - \lambda I) = V \implies T = \lambda I$. $\square$

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

PROOF.

$$\mathrm{Hom}_G(V_j, V) = \mathrm{Hom}_G(V_j, V_1 \oplus \ldots \oplus V_{t'}) = \bigoplus_{i \in I} \mathrm{Hom}(V_j, V_i) : V_i \cong V_j \; \forall i \in I$$
$$= \underbrace{\mathbb{C} \oplus \ldots \oplus \mathbb{C}}_{|I| = m_j \text{ times}} \implies \dim \mathrm{Hom}_G(V_j, V) = m_j \quad \square$$

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

PROP 1.3 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 $v_1, \ldots, v_d$ 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 $\mathrm{tr}(\pi) = \dim(W)$. $\square$

DEF 1.8 Let $V_1 = \mathbb{C}$ have the trivial action of G. Then $\mathrm{Hom}_G(V_1, V) = V^G = \{v \in V : gv = v \forall g \in G\}$.

1.6 "Burnside"

If V is any representation of G, then

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

PROP 1.4 Thm 1.6 $\implies$ Burnside's Lemma.

PROOF.

Given a G-set X, we can consider $V = \mathbb{C}^{\times}$, the set of scalar functions on X. Then $V^G = \{f : X \to \mathbb{C} : gf = f\}$. Then $f \in V^G \implies gf(x) = fg^{-1}(x)$. Hence, $f(x) = f(g^{-1}x)$. $\dim(V^G) = \#$ of orbits of G on X. Similarly, $\mathrm{tr}(g \circlearrowleft V) = \#\mathrm{FP}_X(g)$. $\square$