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 subspace DEF 1.3

$W \subsetneq V$. This 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 $G = \{g_1, \ldots, g_N\}$ 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 $T_1, \ldots, T_N$ 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 $\dim(V) = 1$.

1.1 Finite Abelian Representation

If G is a finite abelian group, and V is an irreducible representation of G, then $\dim(V) = 1$. Our conclusion is that the associated homomorphism $\rho : G \to \mathbb{C}^\times$.

PROOF.

$G = \{g_1, \ldots, g_N\}$. 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 (follows from ρ being a homomorphism). $T_1, \ldots, T_N$ 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 $T_1, \ldots, T_N$ is a collection of linear transformations on a complex vector space, then they have a simulaneaous eigenvector, i.e. $\exists v : T_j v = \lambda_j v\ \forall j$.

PROOF.

By induction. Consider T_1. It's minimal and characteristic polynomials split, with at least an eigenvalue λ, and so it has an eigenvector.

$n \to n+1$. 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

$T_1, \ldots, T_N$. (Thinking of T_j as linear transformations $V_\lambda \to V_\lambda$). $\square$

♠ *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. 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 $\rho(g) = \mathrm{sgn}(g)$.

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 $e_3 = (123)e_2$. 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, e.g. $(12)(e_1 + e_2 + e_3) = e_2 + e_1 + e_3$. Then $V = \mathrm{span}(w)$.

$\hookrightarrow$ *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

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