# **MATH457** - Algebra 4

Representation Theory; Galois Theory

Based on lectures from Winter 2025 by Prof. Henri Darmon.
Notes by Louis Meunier

### Contents

% ! 01-06

# §1 Representation Theory

## §1.1 Introduction

↪**Definition 1.1** (Linear Representation): A *linear representation* of a group $G$ is a vector space $V$ over a field $\mathbb{F}$ equipped with a map $G \times V \to V$ that makes $V$ a $G$-set in such a way that for each $g \in G$, the map $v \mapsto gv$ is a linear homomorphism of $V$.

This induces a homomorphism

$$\rho : G \to \mathrm{Aut}_{\mathbb{F}}(V),$$

or, in particular, when $n = \dim_{\mathbb{F}} V < \infty$, a homomorphism

$$\rho : G \to \mathrm{GL}_n(\mathbb{F}).$$

Alternatively, a linear representation $V$ can be viewed as a module over the group ring $\mathbb{F}[G] = \left\{\sum_{g \in G} : \lambda_g g : \lambda_g \in \mathbb{F}\right\}$ (where we require all but finitely many scalars $\lambda_g$ to be zero).

↪**Definition 1.2** (Irreducible Representation): A linear representation $V$ of a group $G$ is called *irreducible* if there exists no proper, nontrivial *subspace* $W \subsetneq V$ such that $W$ is $G$-stable.

⊛ **Example 1.1**:

1. Consider $G = \mathbb{Z}/2 = \{1, \tau\}$. If $V$ a linear representation of $G$ and $\rho : G \to \mathrm{Aut}(V)$. Then, $V$ uniquely determined by $\rho(\tau)$. Let $p(x)$ be the minimal polynomial of $\rho(\tau)$. Then, $p(x) \mid x^2 - 1$. Suppose $\mathbb{F}$ is a field in which $2 \neq 0$. Then, $p(x) \mid (x-1)(x+1)$ and so $p(x)$ has either $1, -1$, or both as eigenvalues and thus we may write

$$V = V_+ \oplus V_-,$$

   where $V_{\pm} := \{v \mid \tau v = \pm v\}$. Hence, $V$ is irreducible only if one of $V_+, V_-$ all of $V$ and the other is trivial, or in other words $\tau$ acts only as multiplication by 1 or $-1$.

2. Let $G = \{g_1, ..., g_N\}$ be a finite abelian group, and suppose $\mathbb{F}$ an algebraically closed field of characeristic 0 (such as $\mathbb{C}$). Let $\rho : G \to \mathrm{Aut}\,(V)$ and denote $T_j := \rho\left(g_j\right)$ for $j = 1, ..., N$. Then, $\{T_1, ..., T_N\}$ is a set of mutually commuting linear transformations. Then, there exists a simultaneous eigenvector, say $v$, for $\{T_1, ..., T_N\}$, and so span $(v)$ a $G$-stable subspace of $V$. Thus, if $V$ irreducible, it must be that $\dim_{\mathbb{F}} V = 1$.

↪**Theorem 1.1**: If $G$ a finite abelian group and $V$ an irreducible finite dimensional representation over an algebraically closed field of characeristic 0, then $\dim V = 1$.

Proof. Let $\rho : G \to \mathrm{Aut}(V)$, label $G = \{g_1, ..., g_N\}$ and put $T_j := \rho\left(g_j\right)$ for $j = 1, ..., N$. Then, $\{T_1, ..., T_N\}$ a family of mutually commuting linear transformations on $V$. Then, there is a simultaneous eigenvector $v$ for $\{T_1, ..., T_N\}$ and thus $\mathrm{span}(v)$ is $T_1, ..., T_N$-stable and so $V = \mathrm{span}(v)$. ∎

↪**Lemma 1.1**: Let $V$ be a finite dimensional vector space over $\mathbb{C}$ and let $T_1, ..., T_N : V \to V$ be a family of mutually commuting linear automorphisms on $V$. Then, there is a simultaneous eigenvector for $T_1, ..., T_N$.

↪**Proposition 1.1**: Let $\mathbb{F}$ a field where $2 \neq 0$ and $V$ an irreducible representation of $S_3$. Then, there are three distinct (i.e., up to homomorphism) possibilities for $V$.

Proof. Let $\rho : G \to \mathrm{Aut}(V)$ and let $T = \rho((23))$. Then, notice that $p_T(x) \mid \left(x^2 - 1\right)$ so $T$ has eigenvalues in $\{-1, 1\}$.

If the only eigenvalue of $T$ is $-1$, we claim that $V$ one-dimensional.

If $T$ has 1 as an eigenvalue. ∎

↪**Proposition 1.2**: $D_8$ has a unique faithful irreducible representation, of dimension 2 over a field $F$ in which $0 \neq 2$.

Proof. Write $G = D_8 = \left\{1, r, r^2, r^3, v, h, d_1, d_2\right\}$ as standard. Let $\rho$ be our irreducible, faithful representation and let $T = \rho\left(r^2\right)$. Then, $p_T(x) \mid x^2 - 1 = (x-1)(x+1)$ and so $V = V_+ \oplus V_-$, the respective eigenspaces for $\lambda = +1, -1$ respectively for $T$. Then, notice that since $r^2$ in the center of $G$, both $V_+$ and $V_-$ are preserved by the action of $G$, hence one must be trivial and the other the entirety of $V$. $V$ can't equal $V_+$, else $T = I$ on all of $V$ hence $\rho$ not faithful so $V = V_-$.

Next, it must be that $\rho(h)$ has both eigenvalues 1 and $-1$. Let $v_1 \in V$ be such that $hv_1 = v_1$ and $v_2 = rv_1$. We claim that $W := \mathrm{span}\,\{v_1, v_2\}$, namely $V = W$ 2-dimensional.

We simply check each element. $rv_1 = v_2$ and $rv_2 = r^2 v_1 = -v_1$ which are both in $W$ hence $r$ and thus $\langle r \rangle$ fixes $W$. Next, $hv_1 = v_1$ and $vv_2 = vrv_1 = rhv_1 = rv_1 = v_2$ (since $rhr^{-1} = v$) and so $hv_2 = -v_2$ and $vv_1 = -v_1$ and so $W$ $G$-stable. Finally, $d_1$ and $d_2$ are just products of these elements and so $W$ $G$-stable. ∎

↪**Theorem 1.2** (Maschke's): Any representation of a finite group $G$ over $\mathbb{C}$ can be written as a direct sum of irreducible representations, i.e.

$$V = V_1 \oplus \cdots \oplus V_t,$$

where $V_j$ irreducible.

**Remark 1.1**: $|G| < \infty$ essential. For instance, consider $G = (\mathbb{Z}, +)$ and 2-dimensional representation given by $n \mapsto \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$. Then, $n \cdot e_1 = e_1$ and $n \cdot e_2 = ne_1 + e_2$. We have that $\mathbb{C}e_1$ irreducible then. But if $v = ae_1 + e_2 \in W := V \setminus \mathbb{C}e_1$, then $Gv = (a+1)e_1 + e_2$ so $Gv - v = e_1 \in W$, contradiction.

**Remark 1.2**: $|\mathbb{C}|$ essential. Suppose $F = \mathbb{Z}/3\mathbb{Z}$ and $V = Fe_1 \oplus Fe_2 \oplus Fe_3$, and $G = S_3$ acts on $V$ by permuting the basis vectors $e_i$. Then notice that $F(e_1 + e_2 + e_3)$ an irreducible subspace in $V$. Let $W = F(w)$ with $w := ae_1 + be_2 + ce_3$ be any other $G$-stable subspace. Then, by applying $(123)$ repeatedly to $w$ and adding the result, we find that $(a+b+c)(e_1 + e_2 + e_3) \in W$. Similarly, by applying $(12), (23), (13)$ to $w$, we find $(a-b)(e_1 - e_2), (b-c)(e_2 - e_3), (a-c)(e_1 - e_3)$ all in $W$. It must be that at least one of $a-b, a-c, b-c$ nonzero, else we'd have $w \in F(e_1 + e_2 + e_3)$. Assume wlog $a - b \neq 0$. Then, we may apply $(a-b)^{-1}$ and find $e_1 - e_2 \in W$. By applying $(23), (13)$ to this vector and scaling, we find further $e_2 - e_3$ and $e_1 - e_3 \in W$. But then,

$$2(e_1 - e_2) + 2(e_1 - e_3) = e_1 + e_2 + e_3 \in W,$$

so $F(e_1 + e_2 + e_3)$ a subspace of $W$, a contradiction.

$\hookrightarrow$**Proposition 1.3**: Let $V$ be a representation of $|G| < \infty$ over $\mathbb{C}$ and let $W \subseteq V$ a sub-representation. Then, $W$ has a $G$-stable complement $W'$, such that $V = W \oplus W'$.

Proof. Denote by $\rho$ the homomorphism induced by the representation. Let $W_{0'}$ be any complementary subspace of $W$ and let

$$\pi : V \to W$$

be a projection onto $W$ along $W_{0'}$, i.e. $\pi^2 = \pi, \pi(V) = W$, and $\ker(\pi) = W_{0'}$. Let us "replace" $\pi$ by the "average"

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

Then the following hold:

(1) $\tilde{\pi}$ $G$-equivariant, that is $\tilde{\pi}(gv) = g\tilde{\pi}(v)$ for every $g \in G, v \in V$.

(2) $\tilde{\pi}$ a projection onto $W$.

Let $W' = \ker(\tilde{\pi})$. Then, $W'$ $G$-stable, and $V = W \oplus W'$. ■