PMATH 445 Course Notes

Representations of Finite Groups

Jason Bell • Fall 2021 • University of Waterloo

Table of Contents

1 September 8, 2021

We begin the course by recalling Cayley's theorem, a famous result from group theory. It states that every finite group G embeds (there exists an injective homomorphism) into a symmetric group S_n. The proof is simple: let G act on itself by left multiplication, and show that this gives an embedding of G into S_n where $n = |G|$. This result is simple, but it allows us to understand finite groups as subgroups of symmetric groups, where one has many tools to use.

In representation theory, one seeks to understand groups in terms of maps into general linear groups $\mathrm{GL}_n(F)$, where F is a field. This is generally more desirable than an embedding into a symmetric group, as we obtain the full power of linear algebra at our disposal. We will consider all homomorphisms (not just injective ones) from groups to general linear groups, and such homomorphisms are called **representations** of our group. First, we show that every finite field embeds into $\mathrm{GL}_n(F)$ for some field F.

Proposition 1.1. Let F be a field. Every finite group embeds into $\mathrm{GL}_n(F)$ for some $n \geq 1$.

Proof. Let G be a finite group. By Cayley's theorem, we have an embedding $G \hookrightarrow S_n$ where $n = |G|$. Hence, it suffices to show that S_n embeds into $\mathrm{GL}_n(F)$. Define $\varphi : S_n \to \mathrm{GL}_n(F)$ by $\psi(\sigma) = P_\sigma$, where P_σ denotes the permutation matrix. Notice that for $\sigma_1, \sigma_2 \in S_n$, we have $\varphi(\sigma_1\sigma_2) = P_{\sigma_1\sigma_2} = P_{\sigma_1}P_{\sigma_2} = \varphi(\sigma_1\sigma_2)$, so φ is a group homomorphism. One can also check that if $\varphi(\sigma) = I$, the identity matrix, then σ must be the identity permutation, so φ is injective. □

It turns out that this result is not true for infinite groups in general.

Example 1.2. Let G be the group consisting of bijective maps from $\mathbb{Z}^+$ to itself such that f fixes all but finitely integers. We claim that there does not exist a field F and $n \geq 1$ such that G embeds into $\mathrm{GL}_n(F)$.

Proof. First, we note the following fact from linear algebra.

Fact. If A and B are commuting diagonalizable matrices, then they are simultaneously diagonalizable. That is, there is a common change of basis that makes both matrices diagonalizable. This result also extends to families of commuting diagonalizable matrices.

Now, we denote by (i, j) the bijective mapping from $\mathbb{Z}^+$ to itself which swaps i and j and fixes all other integers. Consider the permutations $(1, 2)$, $(3, 4)$, $(5, 6)$, and so on. Note that they pairwise commute. Suppose that there exists an injective homomorphism $\varphi : G \to \mathrm{GL}_n(F)$ for some $n \geq 1$ and a field F. Let $A_1 = \varphi(1, 2)$, $A_2 = \varphi(3, 4)$, and so on. Observe that we have

$$\varphi((i, i+1)^2) = \varphi(\mathrm{id}) = I,$$

which implies that $A_1^2 = A_2^2 = \cdots = I$. We now recall another fact from linear algebra.

Fact. If the minimal polynomial of a matrix has distinct roots over the (algebraically closed) field F, then the matrix is diagonalizable.

We see from above that the minimal polynomial of the A_i must divide $x^2 - 1$, since $A_i^2 - I = 0$. We can assume after a change of basis that each A_i is of the form

$$A_i = \begin{pmatrix} \varepsilon_{1,i} & & 0 \\ & \ddots & \\ 0 & & \varepsilon_{n,i} \end{pmatrix}$$

where $\varepsilon_{1,i}, \ldots, \varepsilon_{n,i} \in \{\pm 1\}$. Now we have a problem: there are only 2^n such matrices of the above form, and infinitely many positive integers. Thus, there exist positive integers $i < j$ such that $\varphi(A_i) = \varphi(A_j)$, so φ is not injective, and this yields our contradiction. □

We now turn to the notion of a group algebra.

DEFINITION 1.3. The **group algebra** of the group G over the field k is defined by

$$k[G] = \left\{ \sum_{g \in G} \alpha_g \cdot g : \alpha_g \in k,\ \alpha_g = 0 \text{ for all but finitely many } g \right\}.$$

We note that $k[G]$ is a ring with a natural addition, and multiplication given by

$$\left(\sum_{g \in G} \alpha_g \cdot g \right) \left(\sum_{h \in G} \beta_h \cdot h \right) = \sum_{y \in G} \left(\sum_{(g,h):gh=y} \alpha_j \cdot \beta_h \right) \cdot y.$$

Notice that the inner sum is finite because by definition, there are only finitely many non-zero α_g and β_h.

REMARK 1.4. We call $k[G]$ a group *algebra* because we have a "copy" of k in $k[G]$ given by $\lambda \mapsto \lambda \cdot 1_G$ for elements $\lambda \in k$, with $\lambda \cdot g = g \cdot \lambda$ for all $g \in G$. We see that $k[G]$ is a k-vector space of dimension $|G|$.

EXERCISE 1.5. Show that $\mathbb{C}[S_3] \cong \mathbb{C} \times \mathbb{C} \times M_2(\mathbb{C})$. Fun fact: using the naive approach to multiply matrices takes $O(n^3)$ operations, but applying this fact reduces the time complexity to $O(n^{2.373})$.

We now prove a version of Cayley's theorem for group algebras.

PROPOSITION 1.6. Let G be a finite group with $n = |G|$. Then G embeds into $\mathrm{GL}_n(k[G])$.

PROOF. Let G act on $k[G]$ by left multiplication. That is, for $g \in G$, define

$$L_g : k[G] \to k[G] : \sum_{h \in G} \alpha_h \cdot h \mapsto \sum_{h \in G} \alpha_h \cdot (g \cdot h).$$

Observe that for $g_1, g_2 \in G$, we have

$$L_{g_1} \circ L_{g_2}(x) = L_{g_1}(L_{g_2}(x)) = L_{g_1}(g_2 \cdot x) = g_1 \cdot (g_2 \cdot x) = (g_1 \cdot g_2) \cdot x = L_{g_1 g_2}(x).$$

For the second equality, we can think of G as sitting inside $k[G]$ by identifying $g \in G$ with $1 \cdot g \in k[G]$, so we simply have multiplication in the group algebra. Hence, we see that the map $L : G \to \mathrm{GL}_n(k[G]) : g \mapsto L_g$ is a group homomorphism. Finally, if L_g is the identity matrix, then $g \cdot x = x$ for all $x \in k[G]$. This implies that $g \cdot 1 = 1$ and so $g = 1$, so $\ker L = \{1\}$. Thus, L is injective and is the desired embedding. □

Later in the course, we will prove the following important theorem. In short, it states that if G is a finite group and k is an algebraically closed field of characteristic zero, then $k[G]$ is isomorphic to a finite direct of matrix rings over k. The isomorphism and these matrix rings will completely determine the representation of the group G.

THEOREM 1.7. Let G be a finite group and let k be an algebraically closed field of characteristic zero. Then we have

$$k[G] \cong \prod_{i=1}^{s} M_{n_i}(k),$$

where

(1) s is the number of conjugacy classes of G;

(2) $n_1^2 + n_2^2 + \cdots + n_s^2 = |G|$;

(3) $|\{i : n_i = 1\}| = |G/G'|$; and

(4) $n_i \mid |G|$ for all $1 \leq i \leq s$.

As a corollary of this theorem, one can prove Exercise 1.5 by noting that $\mathbb{C}[S_3]$ has three conjugacy classes: $\{(1)\}$, $\{(12), (13), (23)\}$, and $\{(123), (132)\}$.

To finish off the lecture, we give one more interesting linear algebra fact.

FACT. If $q = p^j$ where p is prime and $j \geq 1$, then

$$|\mathrm{GL}_n(\mathbb{F}_q)| = \prod_{i=0}^{n-1} (q^n - q^i).$$

It is not hard to see why. Let A be an invertible $n \times n$ matrix, and note that A must have linearly independent columns. For the first column, say v_1, we have $q^n - 1$ choices as we can pick any vector except the zero vector. For the second column, we can choose any vector except those in the span of v_1, which yields $q^n - q$ choices. One can repeat this argument to obtain the result.