On Linear Representations Of Finite Groups And Burnside's Theorem On Group Solvability

Pranav Shankar
emailpranavshankar@gmail.com

Euler Circle

July 14, 2024

Introduction

- Representation theory is the study of group representations, which are group actions on vector spaces.
- Representation theory makes use of both group theory and linear algebra.
- Representation theory is applied practically in quantum mechanics, crystallography, and coding theory. Even more, chemists use it to count molecules and engineers use it to count arrangements of switches in circuits.

What Is A Group?

A *group* is a set G, combined with a binary operation $*$ such that:

- For all $g, h \in G$, $gh \in G$. This condition on G is called *closure* under $*$.
- For all $g, h, j \in G$, $g(hj) = (gh)j$. This condition on $*$ is called *associativity* over G.
- There exists a unique element $1_G \in G$ such that $1_G * g = g * 1_G = g$. Such an element is called the *identity element* of G.
- For all non-identity elements $h \in G$, there exists an element $h^{-1} \in G$ such that $hh^{-1} = h^{-1}h = 1_G$, where 1_G is the identity element of G. Then h^{-1} is called the *inverse* of h in G.

Examples Of Groups

One example of an infinite group is the set of integers $\mathbb{Z}$ combined with addition. One example of a finite group is D_4, the set of symmetries of a square, combined with composition of transformations.

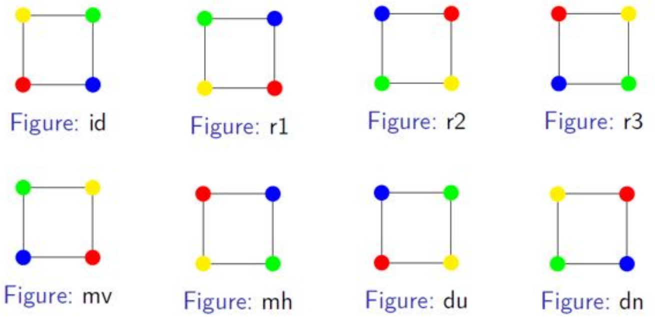

Figure: id

Figure: r1

Figure: r2

Figure: r3

Figure: mv

Figure: mh

Figure: du

Figure: dn

Figure: id and the rotations form a subgroup C_4 of D_4 (see next slide)

Subgroups

A *subgroup* H of a group G is a subset of G that is a group on its own under the same group operation. To prove a subset of a group is a subgroup, we need to prove that it satisfies the group axioms. however, there is a shortcut, known as the Subgroup Criterion.

Theorem

(Subgroup Criterion) Let G be a finite group and let S be a subset of G. Then S is a subgroup of G if and only if, for all $x, y \in S$, $xy^{-1} \in S$.

Proof.

Lets first prove the only if part. Let S be a subgroup of G. Then, for all $a, b \in S$, $ab \in S$ and $b^{-1} \in S$ due to group axioms. Inverting b gives $ab^{-1} \in S$. Now, let's prove the "if" part. Let S be a subset of G such that $cd^{-1} \in S$ for all $c, d \in S$. Associativity is clear. We can plug $c = d$ into $cd^{-1} \in S$ to get $1_G \in S$, and we can plug $c = 1$ to get $d^{-1} \in S$ for all $d \in S$. Inverting d^{-1} gives $cd \in S$. Thus S is a subgroup of G. ■

Basics of Group Theory

- A subset S of a group G *generates* G if all elements of G can be expressed as a product of elements of S. A group is *cyclic* if it is generated by only 1 element. (ex. C_4)
- The *left coset* gH of a subgroup H of a group G corresponding to an element $g \in G$ is the set of all values of gh for $h \in H$. (ex. $\{r1, r3\}$ is the left coset of C_2 in C_4, where C_2 consists of only id and r2)
- Elements a, b of a group G are *conjugate* if there is $g \in G$ such that $gag^{-1} = b$. Conjugacy divides G into disjoint *conjugacy classes* such that conjugate elements are in the same class. (ex. r1 and r3 form a conjugacy class of D_4)
- A subgroup S of a group G is *normal* if and only if it is a union of conjugacy classes of G (ex. C_4 is a normal subgroup of D_4)
- A group is *abelian* if any 2 elements commute, i.e. if the order of multiplication doesn't matter for any pair of elements. (ex. C_4 or any other cyclic group)

Basics of Group Theory 2

- The *order* of a group G is the number of its elements. The order of the cyclic subgroup of G containing an element $g \in G$ is called the *order* $|g|$ of g.
- The *trivial group*, denoted by C_1, is the unique group of order 1.
- The *centralizer* $C_G(S)$ of a subset S of a group G is the set of elements of G that commute with every element of S. If $S = G$, that set is called the *center* $C_G(G)$ of G. (ex. $C2$ is the center of $D4$). All centralizers are subgroups, and all centers are normal subgroups.
- The center of a (nontrivial) group of prime power order is never C_1.
- Lagrange's Theorem states that that, if H is a subgroup of G, then $|H|$ divides $|G|$.
- If H is a normal subgroup of G, the set of left cosets of H forms a subgroup G/H, called the *quotient group* of G, with order $\frac{|G|}{|H|}$ operation $*$ such that $gH * jH = gjH$ for all $g, j \in G$.

Basics of Group Theory 3

- A group G is *simple* if it has no normal subgroups other than C_1 and G.
- Let K be a conjugacy class of a group G, and let $g \in K$. Then $|K| = \frac{|G|}{|C_G(g)|}$.
- The above proposition gives us the following theorem: Let G be a group and $g_1, g_2, \dots g_k$ be representatives of all the non-central conjugacy classes of G. Then $|G| = C_G(G) + \sum_{j=1}^{k} |G/C_G(\{g_j\})|$.
- Take any group G and prime p such that $v_p(|G|) = a \geq 1$. The 1st Sylow Theorem states that there exists at least 1 subgroup of G of order p^a. All such subgroups are called *Sylow p-subgroups* of G.

Group Homomorphisms

- A *homomorphism* f is a function from a group G to a group H such that $f(g)f(h) = f(gh)$ for all $g, h \in G$.
- An *isomorphism* is a bijective homomorphism.
- The *nullspace* $Null(f)$ of a homomorphism f from G to H is the set of elements $g \in G$ such that $f(g) = 1_H$
- The *range* $Rng(f)$ of a homomorphism f from G to H is the set of elements $h \in G$ such that there's a $g \in G$ such that $f(g) = h$.

Group Solvability

- A group is *solvable* if if there exists, for some positive integer k, a sequence of subgroups $C_1 = G_1, G_2, \ldots G_k = G$ such that, for all j such that $1 \leq j \leq k-1$, G_j is a normal subgroup of G_{j+1} and G_{j+1}/G_j is abelian.
- For example, all abelian groups are solvable, as the sequence C_1, G satisfies all the conditions outlined above
- Let G be a group and N be a normal subgroup of G. Then, if both N and G/N are solvable, G is solvable.
- All groups of prime-power order, including C_1, are solvable.

Vector Spaces and Linear Transformations

- A *field* is a set combined with addition and multiplication (that is distributive over addition) that is an abelian group under addition with identity element 0, whose nonzero elements form an abelian group under multiplication.
- A *vector space* over a field F of 'scalars' is a set V of 'vectors' with vector addition and scalar multiplication such that
    - V is an abelian group under vector addition with identity element $\mathbf{0}$
    - Scalar multiplication is distributive over vector addition and field addition.
    - Scalar multiplication is compatible with field multiplication.
- A subset S of a vector space is *linearly dependent* if $\mathbf{0}$ can be written as a nonzero linear combination of vectors in S. Otherwise it's *linearly independent*

Vector Spaces and Linear Transformations 2

- A *basis* for a vector space V is a linearly independent subset S of V such that every element of V is a linear combination of elements of S. All bases for a vector space V have the same size, and that size is called the *dimension* of V.
- Let f be a function between from V to W where V and W are vector spaces over the same field F Then f is a *linear transformation* if and only if
  - f is compatible with vector addition: $f(\mathbf{a}+\mathbf{b}) = f(\mathbf{a}) + f(\mathbf{b})$ for all $\mathbf{a}, \mathbf{b} \in V$.
  - f is compatible with scalar multiplication: $cf(\mathbf{a}) = f(c\mathbf{a})$ for all $\mathbf{a} \in V$ and $c \in F$.

  If $W = V$, then f is called a *linear operator* on V.
- The nullspace and range of any linear transformation are both vector spaces.

Vector Spaces and Linear Transformations 3

- Let L be a linear transformation. The *matrix representation* $[T]_B^C$ of L is the $m * n$ matrix A (whose entries are denoted by a_{jk} where $1 \leq j \leq m$ and $1 \leq k \leq n$.) such that $T(b_k) = \sum_{j=1}^{m} a_{jk}\mathbf{c}_j$ for all integers k such that $1 \leq k \leq n$.
- Let L be a linear operator on vector space V.For any vector-scalar pair $(\mathbf{v}, c)$, if $L(\mathbf{v}) = c\mathbf{v}$, $\mathbf{v}$ is called an *eigenvector* of L, and c is called an *eigenvalue* of L.
- Let L be a linear operator on a vector space V. Then L is called *diagonalizable* if and only if there exists a basis B (of eigenvectors of L) for V such that $[L]_B^B$ is a diagonal matrix.
- The *minimal polynomial* of a linear operator is the polynomial of least degree that gives 0 when the operator is plugged in. (Here the product of linear operators is their composition).

An Important Theorem About Linear Operators

Theorem

A linear transformation is injective if and only if it has a nullspace contaning only $\mathbf{0}$.

Proof.

For the "if" part, let L be an injective linear transformation. Let $\mathbf{x}$ and $\mathbf{y}$ be elements of $Null(L)$. Then $L(\mathbf{x}) = L(\mathbf{y}) = \mathbf{0}$. However, by injectivity, $L(\mathbf{x}) = L(\mathbf{y})$ implies $\mathbf{x} = \mathbf{y}$, so $Null(L)$ contains only 1 element. However, since L is linear, $L(\mathbf{0}) = \mathbf{0}$, so $Null(L)$ contains only $\mathbf{0}$.
For the "only if" part, let M be a linear transformation such that $Null(M)$ contains only $\mathbf{0}$. Let $M(\mathbf{x}) = M(\mathbf{y})$. Then $M(\mathbf{x} - \mathbf{y}) = M(\mathbf{x}) - M(\mathbf{y}) = \mathbf{0}$ by linearity. Thus $\mathbf{x} - \mathbf{y} = \mathbf{0}$, so $\mathbf{x} = \mathbf{y}$. Thus M is injective. ■

Representation Basics

- The *general linear group* $GL(V)$ of a vector space V is the set of linear operators on A, with the operation of function composition.
- A (linear) *representation* of a group G is a homomorphism from G to $GL(V)$ for some complex vector space V
- There exists a representation of G that sends all elements of G to the identity transformation I. That's the *trivial representation*.
- Let r and s be representations sending G to $GL(V)$ and $GL(W)$, respectively, where V, W are vector spaces. Then r, s are *isomorphic* if there's an invertible linear transformation f such that $f \cdot r_g = s_g \cdot f$ for all $g \in G$
- Let r be a representation from G to $GL(V)$ and let W be a vector subspace of V. Then if $r_g(w) \in W$ for all $g \in G$ and $w \in W$ (i.e. if W is invariant under r), then the restriction r^W of r to W is a *subrepresentation* of r.
- A nontrivial representation is *irreducible* if and only if it has no proper nontrivial subrepresentations

Representation Basics 2

- Let r and s be linear representations of a finite group from G to $GL(V)$ and $GL(W)$, respectively. Then, the *direct sum* of r and s, denoted by $r \oplus s$, is the unique representation such that $r \oplus s_g(\mathbf{x} + \mathbf{y}) = (r_g(\mathbf{x}), s_g(\mathbf{y}))$ for all $g \in G$ and $\mathbf{x}, \mathbf{y} \in V, W$, respectively.
- Maschke's Theorem states that, for any representation r from G to $GL(V)$ and subrepresentation s or r sending G to $GL(W)$ where W is a r-invariant subspace, there exists a subrepresentation t of r such that $r = s \oplus t$. From that we can discover that all nontrivial representations can be decomposed into a direct sum of irreducibles.

Characters And The Character Inner Product

- Let L be a linear operator. The *trace* $Tr(L)$ of L is the sum of its eigenvalues. It is also the sum of the diagonal entries of any matrix representation of L.
- Let r be a linear representation from G to $GL(V)$. Then the *character* $X(r)$ of r is the function sending g to $Tr(r_g)$ for all $g \in G$.
- Let V be a complex vector space and f be a function sending pairs of vectors to scalars. Then f is an *inner product* if
  - It is conjugate-symmetric (i.e $f(\mathbf{x}, \mathbf{y}) = \overline{f(\mathbf{y}, \mathbf{x})}$
  - It is linear in the first argument (i.e. $af(\mathbf{x}, \mathbf{z}) + f(\mathbf{y}, \mathbf{z}) = f(a\mathbf{x} + \mathbf{y}, \mathbf{x})$)
  - It is positive definite (i.e. $f(\mathbf{x}, \mathbf{x}) \in \mathbb{R}_{>0}$ for all nonzero $\mathbf{x}$.)
- With respect to an inner product f, the *norm* of a vector $\mathbf{v}$ is $\sqrt{f(\mathbf{v}, \mathbf{v})}$.
- With respect to an inner product f, vectors $\mathbf{v}$ and $\mathbf{w}$ are *orthogonal* if $f(\mathbf{v}, \mathbf{w} = 0$. If $\mathbf{v}$ and $\mathbf{w}$ are also unit vectors (i.e. have norm 1), they are *orthonormal*.

Schur's Lemma

Theorem

(Schur's Lemma) Let r and s be irreducible representations from G to $GL(V)$ and $GL(W)$, respectively, and let f be a linear transformation from V to W that's compatible with the group operation of G. Then f is a scalar multiple of I, and $f = 0$ if r and s aren't isomorphic.

Proof.

Let $g \in G$ and let $\mathbf{n} \in Null(f)$. Then $f(g\mathbf{n}) = gf(\mathbf{n}) = \mathbf{0}$, so $g\mathbf{n} \in Null(f)$. Hence $Null(f)$ is a G-invariant of V. However, since r is irreducible, $Null(f) = 0$ or $Null(f) = V$. Hence f is either an isomorphism or 0.. Thus, if r and s aren't isomorphic, $f = 0$..
Since $\mathbb{C}$ is algebraically closed, the eigenvalues of f are all complex, so there exists a complex number z such that $f - zI$ is not invertible. Since s is irreducible, $f - zI = 0$, so $f = zI$. ■

Characters and Character Inner Product 2

- Let j and h be characters of linear representations of a group G. Let $\langle h, j\rangle = \frac{\sum_{g \in G} h(g)\overline{j(g)}}{|G|}$. Then $\langle h, j\rangle$ is an inner product.
- With respect to this inner product, characters of irreducible representations are orthonormal.
- The number of irreducible representations of a group G is equal to the number of conjugacy classes of G.
- The *regular representation* $reg(G)$ of a group G is the representation sending $g \in G$ to the function f such that $f(h) = gh$ for all $h \in G$. Then $X_{reg(G)}(1_G) = |G|$ and $X_{reg(G)}(j) = 0$ for all nonidentity $j \in G$.

An Important Theorem About Characters

Theorem

Let r be a linear representation sending a group G to $GL(V)$ for some complex vector space V. Then $X_r(g)$ is a sum of $X_r(1)$ roots of unity.

Proof.

We first prove the following lemma.

Lemma

The minimal polynomial of r_g has distinct roots, and these roots are $|g|$th roots of unity, for all $g \in G$.

Proof.

Note that $(r_g)^{|g|} = r_{g^{|g|}} = r_{1_G} = I..$ Thus the minimal polynomial of r_g is a factor of $x^{|g|} - 1$ whose degree is that of r_g, so its roots are $X_r(1)$ distinct $|g|$th roots of unity. ■

An Important Theorem About Characters 2

Proof.

Since r_g has a minimal polynomial with distinct roots, it's diagonalizable, and its eigenvalues are $|g|$th roots of unity. Thus $Tr(r_g) = X_r(g)$, is the sum of $X_r(1)$ $|g|$th roots of unity. ■

Burnside's Theorem: Lemmas

Lemma

Let r be an irreducible representation sending a finite group G to $GL(V)$ for some complex vector space V. Let K be a conjugacy class of G such that $\gcd(|K|, X_r(1)) = 1$. Then either $X_r(g) = 0$ or r_g is a scalar multiple of I, for all $g \in K$.

The above lemma is used to prove the following lemma below, which will be used to prove Burnside's Theorem (see next slide)

Lemma

Let G be a simple group with a conjugacy class whose size is a positive integer power of a prime p. Then G is cyclic of prime order.

Proof of Burnside's Theorem Lemma 2 Case 1

Proof.

Let r_1 be the trivial representation of G and let $r_2 \dots r_n$ be the irreducible representations of G. Consider the regular representation r_R of G and a nonidentity element g of G. Then $X_{r_R}(g) = 0 = \sum_{j=1}^{k} \deg(r_j) X_{r_j}(g) = \sum_{j=1}^{k} X_{r_j}(1) X_{r_j}(g)$. Since $X_{r_1}(g) X_{r_1}(1) = 1$, $\sum_{j=2}^{k} X_{r_j}(1) X_{r_j}(g) = -1$.

Now, we take 2 cases. In the first case, for all k such that $1 \leq k \leq n$, either $X_{r_k}(1)$ is divisible by p or $X_{r_k}(g) = 0$. Then $\sum_{j=2}^{k} X_{r_j}(1) X_{r_j}(g)$ Since either $X_{r_k}(1)$ is divisible by p or $X_{r_k}(g) = 0$ for all k such that $1 \leq k \leq n$, $\frac{\sum_{j=2}^{k} X_{r_j}(1) X_{r_j}(g)}{p} = \frac{-1}{p}$ is a sum of integer multiples of values of $X_{r_k}(g)$. These values are sums of roots of unity, and thus algebraic integers, making $\frac{-1}{p}$ an algebraic integer, contradiction. ■

Proof of Burnside's Theorem Lemma 2 Case 2

Proof.

In the second case, there exists a value of m such that $1 \leq m \leq n$ such that $X_{r_m}(1)$ is not divisible by p and $X_{r_m}(g)$ is nonzero. Then $\gcd(|K|, X_r(1)) = 1$, so by the previous lemma, $r_m(k)$ is a nonzero scalar multiple of I for all $k \in K$, so r_g is therefore central in $Rng(r)$. Letting $h \in G$ we can thus write $r_h r_g r_{h^{-1}} = r_g$, so $r_{hgh^{-1}} = r_g$. Since G is a nontrivial simple group, $Null(r) = C_1$, so r is injective. Therefore, $r_{hgh^{-1}} = r_g$ implies $hgh^{-1} = g$ for all $h \in G$, so $g \in C_G(G)$. Since $g \neq 1_G$ and $C_G(G)$ is a normal subgroup of G , $C_G(G) = G$, so G is abelian. Hence every subgroup of G is normal, but G also has no nontrivial normal subgroups except for G itself. Thus G has no nontrivial proper subgroups, so it's a cyclic group of prime order. ■

Proof of Burnside's Theorem: Case 1

Theorem

(Burnside's Theorem) Let G be a group whose order has at most 2 prime factors. Then G is solvable.

Proof.

Let x and y be fixed prime numbers, and assume that there exists an unsolvable group H of order $x^a y^b$ where a and b are nonnegative integers, such that every group whose order is a proper divisor of $x^a y^b$ is solvable. Then, since all abelian groups are solvable, H is not abelian. We take 2 cases

CASE 1: H is not simple. Then it has a proper, nontrivial, normal subgroup J whose order is a proper divisor of $x^a y^b$, and the order of the quotient group, $|H/J| = \frac{|H|}{|J|}$ is also a proper divisor of $x^a y^b$. Since these groups have order that are proper divisors of $x^a y^b$, they are both solvable. Then by Proposition 4.13, H is solvable, contradiction. ■

Proof of Burnside's Theorem, Case 2

Proof.

CASE 2: H is simple. Let X be a Sylow x-subgroup of G. Since X is of prime-power order, its center has a nonidentity element c. Then X is a subgroup of $C_G(c)$ so $|C_G(c)|$ is divislble by x^a Then, the order of the conjugacy class of c in G $\frac{|G|}{C_G(c)}$, which is a power of q, which makes H cyclic of prime-order by Lemma 2 and thus solvable.

Thus, no H satisfying our assumption exists, and Burnside's Theorem follows. ■

Conclusion

- Other than its practical applications, Burnside's Theorem has a lot of applications in pure math.
- Burnside's Theorem was used to prove that every acyclic finite simple group has even order (known as the Feit-Thompson Theorem) and, eventually, this groundbreaking theorem that, in effect, creates a "periodic table" of all the finite simple groups.

Theorem

(Enormous Theorem) Every finite simple group is either cyclic, alternating, in one of 16 *"Lie-type" infinite families, or one of* 26 *"sporadic" groups (or* 27 *if the Tits group is included).*

References

- Ian Magnell (REU paper pdf) (2022)
  Linear Representations of Finite Groups
- Julie Linman (Master's paper pdf)(2010)
  Burnside's Theorem
- Vincent Bouchard (Lecture notes website)(Unknown year)
  MA PH 464 - Group Theory In Physics: Lecture notes