Applied Algebra MAT 340

Lecturer: Mark McConnell Scribe: Kiran Vodrahalli

Contents

1 Group Definitions

First we introduce the primary object of study in these lecture notes.

Definition 1.1. Group.
A group is a set G equipped with a binary operation $\cdot$ such that the following properties hold:

1. Associativity: $(xy)z = x(yz)$ for all $x, y, z \in G$.
2. Identity: $\exists e \in G$ such that $xe = ex = x$ for all $x \in G$.
3. Inverse: For each $x \in G$, $\exists x^{-1} \in G$ such that $xx^{-1} = x^{-1}x = e$.

Definition 1.2. Abelian Group.
A group is said to be abelian if the group operation is commutative: That is, if $xy = yx$ for all $x, y \in G$.

Definition 1.3. Generation.
A group is said to be generated by elements $\{x_1, \cdots, x_n\}$, all in G, if by applying the group operation between members solely in this set one is able to completely construct all the elements in G.

Now we give some properties for all groups. Take G:

1. $\exists$ one identity element $e \in G$.
2. $xy = xz$ implies that $y = z$, and $yx = zx$ implies that $y = z$.
3. For each $x \in G$ there exists precisely one inverse x^{-1}.
4. Inverses have $(xy)^{-1} = y^{-1}x^{-1}$.

Now we give some more useful definitions:

Definition 1.4. Order.
The order of a group G is denoted $|G|$ and means the number of elements in the group. The order of an element $x \in G$ is denoted $|x|$. Let $|x| = k$, then $x^k = e$.

The subgroup is akin to the notion of subspace from linear algebra:

Definition 1.5. Subgroup.
A subgroup of group G is a subset $H \subseteq G$ such that the set H is also a group when equipped with the binary operation $\cdot$ of the group G. H is a subgroup if and only if for all $a, b \in H$ we have $ba^{-1} \in H$. This simultaneously tests closure, and the presence of identity and inverse in H. When all elements have finite order, we can simply check that H is closed under $\cdot$. We denote $H \leq G$ or $H \subseteq G$ to denote subgroup. $\{e\}$ is the trivial subgroup.

1.1 Some Special Subgroups

Here we list some interesting subgroups.

Definition 1.6. Finite Order Subgroup.
If we have an infinite group G and take the subset of elements with finite order, this subset forms a subgroup.

Definition 1.7. Abelian-Product Subgroup.
If G is abelian and $H, K \leq G$, then we have that $HK = \{hk : h \in H, k \in K\}$ is a subgroup of G as well. Note that this statement does not hold in general for G non-abelian.

Definition 1.8. Cyclic Subgroup.
Let $a \in G$. We denote $\langle a \rangle$ the set of elements $\{\cdots, a^{-3}, a^{-2}, a^{-1}, e, a, a^2, a^3, \cdots\}$. $\langle a \rangle$ is a subgroup of G. In general, if there are multiple elements between the brackets, then we mean all possible combinations of those elements.

Now we come to a very important subgroup.

Definition 1.9. Center Subgroup.
We let $Z(G)$ denote the center of subgroup G, defined to be

$$Z(G) = \{a \in G : ax = xa \text{ for all } x \in G\} \tag{1}$$

In other words, the center is the set of elements which commute with all elements of G. Note that considered alone, $Z(G)$ is abelian.

Now we define a subgroup analagous to the center, parametrized by group element g:

Definition 1.10. Centralizer Subgroup.
The centralizer subgroup $C(g)$ for an element $g \in G$ is defined by $\{a \in G : ag = ga\}$. The center is a subgroup of every centralizer: $Z(G) \subseteq C(g)$.

Here is another very important subgroup, which will be used later on:

Definition 1.11. Conjugate Subgroup.
Take a subgroup H and a fixed $x \in G$. Then the conjugate subgroup of H with respect to x is given by

$$xHx^{-1} = \left\{xhx^{-1} : h \in H\right\}$$

We also note that conjugating by an element preserves order: That is, $|xax^{-1}| = |a|$.

Definition 1.12. Normalizer.
Let H be a subgroup of G. Then, the normalizer

$$N(H) = \left\{x \in G : xHx^{-1} = H\right\}$$

In other words, it is the set of elements of G for which conjugation is closed within the subgroup. We will later see how the normalizer is related to the notion of normal subgroup (it is the largest normal subgroup which contains H).

1.2 Conjugacy

We use the notion of conjugates to define the extremely important concept of **conjugacy class**: However, these are not subgroups.

Definition 1.13. Conjugacy Class.
For each $a \in G$, consider the set $\{xax^{-1} : x \in G\}$. This is the conjugacy class of a. The conjugacy classes of G partition G into nonintersecting subsets.

Definition 1.14. $x, y \in G$ are conjugate elements if $\exists a \in G$ s.t. $y = axa^{-1}$.

Definition 1.15. The conjugacy class of x is the set of all elements which are conjugate to it: $\{axa^{-1} | \forall a \in G\}$.

Theorem 1.16. *The relation (x is conjugate to y) is an equivalence relation where the conjugacy classes are the equivalence classes under this relation, and they partition G into disjoint subsets.*

Proof. By Midterm exam. □

Example 1.17. Let V be a vector space over $\mathbb{R}$ or any field F of dimension n. $(V, +, 0)$ is an additive group. Then $GL_n(\mathbb{R})$ consists of automorphisms of V. Let $A \in GL_n(\mathbb{R})$. If you fix a basis B of V and A is with respect to V, this gives a linear transformation $T : V \to V$. If you have another basis B', then the matrix of T w.r.t. B' is SAS^{-1} where S is the change of basis matrix.

Example 1.18. Conjugacy Classes of D_n
Recall every element of D_n is R^k or R^kE where E is some reflection. Since R and E generate the group, we can find all conjugacy classes by finding RxR^{-1} and ExE^{-1} for all $x \in D_n$. As an example: $(RE)x(RE)^{-1} = R(ExE^{-1})R^{-1}$. Here's a table of conjugacy classes of D_n.

$$\begin{bmatrix} x = 1 & R^k & R^kE \\ RxR^{-1} & R^k & R^{k+2}E \\ ExE^{-1} & R^{-k} & R^{-k}E \end{bmatrix}$$

Lemma 1.19. *If $x \in \mathbb{Z}(G)$, then the conjugacy class of x is $\{x\}$.*

Proof. $axa^{-1} = (xa)a^{-1} = x(aa^{-1}) = x$ since x is in the center. □

Note that the conjugacy class of R^kE preserves parity: either $(-k)$ or $(k+2)$ happens.

Definition 1.20. Given $a \in G$, the conjugation $\phi_a : x \to axa^{-1}$ is an automorphism of G. The set of all such automorphisms is a subgroup of Aut(G) called the inner automorphisms, or Inn(G).

Claim 1.21. *The map $G \to$Inn(G) (call $a \in G$, $\phi_a \in$Inn(G)) is a homomorphism.*

Proof. ϕ_a is a homomorphism because $\phi_a(xy) = axya^{-1} = axa^{-1}aya^{-1} = \phi_a(x) \cdot \phi_a(y)$. Then ϕ_a is bijective because it's invertible: Its inverse is $x \to a^{-1}xa$. Inn(G) is a subgroup because $\phi_{ab} \cdot x \to (ab)x(ab)^{-1} = a(bxb^{-1})a^{-1} = \phi_a(\phi_b(x))$. Thus $\phi_{ab} = \phi_a \cdot \phi_b$ which is composition (multiplication in Aut). □

Remark 1.22. Inn(G) can differ from G in that ϕ_a can $= \phi_b$ even if $a \neq b$.

Example 1.23. If $a \in Z(G)$, then $\phi_a = id$. $x \to axa^{-1} = xaa^{-1} = x$ if a is in the center of the group.

Corollary 1.24. *If G is abelian, Inn(G) is trivial.*

1.2.1 Conjugacy in S_n

Theorem 1.25. *In S_n, if $\alpha \in S_n$ and $\beta = (b_1 b_2 b_3 \cdots b_k)$ is a k-cycle, then $\alpha\beta\alpha^{-1} = (\alpha(\beta_1)\alpha(\beta_2)\cdots\alpha(\beta_k))$.*

Proof.

$$\alpha\beta\alpha^{-1}(\alpha(b_i)) = \alpha(\beta(\alpha^{-1}(\alpha(b_i)))) = \alpha(\beta(b_i)) = \alpha(b_{i+1})$$

If $y \in \{1, \cdots, n\}$ is not of the form $\alpha(b_i)$, then $\alpha^{-1}(y)$ is not one of the b_i, β fixes $\alpha^{-1}(y)$; α sends it to $\alpha\alpha^{-1}y = y$. □

Remark 1.26. If $\beta = (\beta_1\beta_2\cdots\beta_l)$ where β_j are cyclic, then $\alpha\beta\alpha^{-1} = \alpha\beta_1\alpha^{-1}\alpha\beta_2\alpha^{-1}\cdots\alpha\beta_l\alpha^{-1}$.

Example 1.27. $(123)(186243)(123)^{-1} = (286341)$.

Theorem 1.28. *The conjugacy classes in S_n are exactly the sets of permutations of a given shape.*

Example 1.29. The conjugacy classes of S_3 by row are (..), (...).

2 Examples of Groups

Now we define several common groups and identify their properties.

2.1 Cyclic Groups

Recall the cyclic subgroup definition from the previous section. We simply call any $\langle a \rangle$ a **cyclic group**, where it is understood that the exponents of a range over $\mathbb{Z}$. Noteably, these subgroups are abelian. We will later see that a cyclic group of order n is isomorphic to $\mathbb{Z}_n$, the group on the set $\{0, \cdots, n-1\}$ with addition $\mod n$. We also note that this group is ismorphic to the unit group $U(m)$, where $n = \phi(m)$ where $\phi(m)$ is the Euler totient function, defined as follows:

Definition 2.1. Euler totient function.
The Euler totient $\phi(m)$ counts the number of relatively prime integers to m strictly less than m. For instance, $\phi(p) = p - 1$, where p is prime. Furthermore, the following factorization property holds: $\phi(m * n) = \phi(m) * \phi(n)$ if m, n are relatively prime (have $\gcd(m, n) = 1$).

We now list some properties of cyclic groups. Let $G = \langle a \rangle$ with $|G| = n$.

1. $a^i = a^j$ iff $i = j$ if G is infinite order; otherwise, $a^i = a^j$ iff $i \equiv j \mod n$.
2. The order of a is the order of the cyclic group: $|a| = |\langle a \rangle|$.
3. If $a^k = e$, then $k = n * m$ for some integer m. In other words, k is a multiple of the group order.

Now we come to a fact important enough to be designated a theorem.

Theorem 2.2. *We present three related facts about $G = \langle a \rangle$ in this theorem.*

1. $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$

2. $|a^k| = \frac{n}{\gcd(n,k)}$

3. Every subgroup of G is also cyclic, and there exists a unique subgroup of G of order m for each positive divisor m of n. These are given by $\langle a^{n/m} \rangle$.

4. The number of elements of order k in G is $\phi(k)$.

That is to say, all $k \leq n$ with the same gcd with respect to n are in the same cyclic subgroup, and the order of that subgroup is given by n divided by the gcd. Also, cyclic groups decompose into subgroups with order the positive factors of the original group. Take the subgroup with order k: This subgroup can be generated by $\phi(k)$ elements of G.

Note that

Corollary 2.3. *# Elements of Order k in a Finite Group.*
There are $m * \phi(k)$ elements of order k in a finite group, since if there is only one cyclic subgroup of order k, there are precisely $\phi(k)$ elements which can generate it. If there are m distinct cyclic subgroups of order k, they must be disjoint, and therefore there are $m * k\phi(k)$ elements of order k.

2.2 Permutation Groups

A permutation group is is a set of permutations of a set A which forms a group under the operation of function composition. A permutation is a bijection from $[n] \to [n]$. We denote the permutation in cyclic form, where reading from left to right gives the sequence of which number leads to which number. For instance, $1 \to 2 \to 1, 3 \to 4 \to 3$ by $(12)(34)$. As another example, we could write $(123)(56)$ to denote $1 \to 2 \to 3 \to 1$ and $5 \to 6 \to 5$.

Definition 2.4. Symmetric group S_n.
We denote the group of permutations on n elements by S_n, with the group operation of function composition, where the order of action on an element x is from right to left. For instance, $(12)(23)x$ means (23) acts on x first, and then (12) acts on the result. If $x = 2$, we would have $(12)(23)2 = (12)3 = 3$. If $x = 3$, we would have $(12)(23)3 = (12)2 = 1$.

The order $|S_n| = n!$ since there are $n!$ total possible permutations of n distinct elements.

Permutations have distinct form when expressed in terms of **disjoint cycles**. That is, a number from $[n]$ appears in one and only one cycle in the cycle composition. Furthermore, disjoint cycles commute. Let $()_k$ denote a cycle of order k. Suppose that the following element is a composition of disjoint cycles:

$$x = ()_{k_1}()_{k_2} \cdots ()_{k_m}$$

Then, the order of x is $|x| = \text{lcm}(k_1, \cdots, k_m)$.

Permutations also have distinct form when expressed in several permutations of the form (..). The number of (..) a permutation decomposes to tells whether or not a permutation is even or odd (even if the number is even, odd otherwise).

The subset of permutations which are odd does not form a subgroup. However, the subset of permutations which are even does:

Definition 2.5. Alternating Group A_n.
The subgroup of S_n consisting of only even permutations is given by A_n. We have $|A_n| = \frac{n!}{2}$.

2.3 Dihedral Groups

The dihedral groups are the groups of symmetries of regular polygons in the plane. They are perhaps one of the simplest classes of nonabelian groups, as they can essentially be thought of as two cyclic groups paired together, each with a different orientation, "face up" or "face down".

Definition 2.6. Dihedral group D_n.
We have $|D_n| = 2n$, and it is generated by R, F, where R is a rotation of $2\pi/n$ radians and F is a flip across an aribtrarily chosen axis of symmetry in the regular polygon with n sides. We have the following rules:

1. $R^n = e, F^2 = e$.

2. $FR^kF = R^{-k}$.

2.4 GL_n, SL_n, PSL_n

GL_n is the general linear group on $n \times n$ matrices. We sometimes write $GL_n(\mathbb{F})$ where $\mathbb{F}$ is typically $\mathbb{R}$, $\mathbb{C}$, or finite field $\mathbb{Z}_n$ to denote the field the matrix is over. The only requirement on the matrices is that they have full rank/are invertible/have non-zero determinant. SL_n is the subgroup with determinant 1. PSL_n is the subgroup of SL_n quotiented by the center.

Theorem 2.7. $|GL_n(\mathbb{Z}_q)| = \prod_{i=0}^{n-1}(q^n - q^i)$.

Proof. The order of $GL_n(\mathbb{Z}_q)$ is $(q^n - 1) * (q^n - q) * (q^n - q^2) * \cdots * (q^n - q^{n-1}) = \prod_{i=0}^{n-1}(q^n - q^i)$. We can see this by noting that there are $q^n - 1$ nonzero possible first rows. The second row must not be a linear combination of the first row. There are only q multiples of the first row, thus there are $q^n - q$ possibilities for the second row. Then, there are q^2 linear combinations of the first two rows which must be avoided for the third row, and thus there are $q^n - q^2$ possibilities. Thus, for the i^{th} row, there are $q^n - q^i$ possibilites and we have our result. □

The order of $SL_n(\mathbb{Z}_q)$ is $\frac{\prod_{i=0}^{n-1}(q^n - q^i)}{q-1}$, which will follow from the First Isomorphism Theorem (we will see this later on) after realizing that the determinant is a homomorphism from $GL_n(\mathbb{Z}_q) \to \mathbb{Z}_q$, and that the restriction to $SL_n(\mathbb{Z}_q)$ is the kernel of this homomorphism.

3 Isomorphisms

3.1 Isomorphism Properties

Definition 3.1. Homomorphisms.
A homomorphism of groups is a map $f : G \to \overline{G}$ s.t. $f(xy) = f(x) \cdot f(y)$.

We can think of non-surjective homomorphisms from $G \to \overline{G}$ as maps which realize a group G in a subgroup of $\overline{G}$, and non-injective surjective homomorphisms as maps which "project" a larger group G to a smaller group $\overline{G}$.

Definition 3.2. Isomorphisms.
A homomorphism of groups that is bijective is an isomorphism. We write $G \cong \overline{G}$.

An isomorphism is a one-to-one map which preserves algebraic structure, and the phrase "identical up to isomorphism" means that for all algebraic intents and purposes, two groups are equivalent.

Theorem 3.3. *Cayley's Theorem.*
Every group is isomorphic to a group of permutations.

We can think of this theorem as saying that a group element applied to every element of the set is equivalent to a permutation of the set of group elements since each group multiplication produces another group element. Formally, we define the permutation functions $\pi_g(x) = gx$. This theorem is deeply related to the results about group actions we discuss later.

Now we list some properties of isomorphisms. Let $\phi : G \to \overline{G}$ be an isomorphism. Then

1. $\phi(e_G) = e_{\overline{G}}$.
2. $\phi(a^n) = \phi(a)^n$, and thus orders are preserved.
3. $\phi^{-1} : \overline{G} \to G$ is an isomorphism.
4. All group properties (abelian-ness, cylic-ness, etc.) and substructures (subgroups, center, numbers of elements of a given order) are preserved across an isomorphism.

3.2 Automorphisms

Definition 3.4. Automorphisms $\mathrm{Aut}(G)$.
An automorphism of G is an isomorphism $\phi : G \to G$. The set of all automorphisms of G is called $\mathrm{Aut}(G)$.

Definition 3.5. Inner automorphism $\mathrm{Inn}(G)$.
Let G be a group with $a \in G$. Then the automorphism $\phi_a(x) = axa^{-1}$ is called an inner automorphism of G induced by a. The set of all inner automorphisms of G is called $\mathrm{Inn}(G)$.

Theorem 3.6. *The sets $Aut(G)$ and $Inn(G)$ are groups under function composition.*

Proof. If $\phi, \psi : G \to G$ are automorphisms, then $\phi \cdot \psi$ is a homomorphism because

$$\phi \cdot \psi(xy) = \phi(\psi(xy)) = \phi(\psi(x) \cdot \psi(y)) = \phi(\psi(x)) \cdot \phi(\psi(y))$$

Then we have that $\phi \cdot \psi$ is a bijection since ϕ, ψ are both bijections. We get inverses since if it's a bijection there exists an inverse function. Then $id : G \to G$ is an automorphism, $id(xy) = xy = id(x) \cdot id(y)$. □

Example 3.7. $\mathrm{Aut}((\mathbb{Z}_6, +, 0))$ is a cyclic group of order 2. $\mathbb{Z}_6$ has two elements of order 6, namely 1 and 5. Any isomorphism must carry an element of order 6 to another of order 6.

Claim 3.8. *$Aut(\mathbb{Z}_6) = \{id, f\}$ where $f(1) = 5$. We have $0 \to 0$. If a homomorphism sends $1 \to 1$, it must send $x \to x$ for all $x \in \mathbb{Z}_6$, so it is the identity. You can also try to send 1 to 5: $f(2) = f(1+1) = f(1) + f(1) = 5 + 5 = 10 \mod 6 \equiv 4 \mod 6$. Then $f(3) = f(2+1) = 4 + 5 = 9 \mod 6 \equiv 3 \mod 6$. Then $f(4) = f(2+2) = f(2) + f(2) = 20 \mod 6 = 2$, and $f(5) = f(4) + f(1) = 2 + 5 \mod 6 = 1$.*

Theorem 3.9. *$U(n) \cong \mathrm{Aut}(Z_n)$.*

1. *Every homomorphism $f : \mathbb{Z}_n \to \mathbb{Z}_n$ has the form $f : x \to ax$ for some $a \in \mathbb{Z}_n$.*

2. *Every automorphism $\phi : \mathbb{Z}_n \to \mathbb{Z}_n$ has the form $\phi : x \to ax$ for some $a \in \mathcal{U}(n)$.*

3. *The homomorphism $\Phi : U(n) \to \mathrm{Aut}(\mathbb{Z}_n)$ given by $\Phi(a) = (x \to ax)$ is an isomorphism, and thus $U(n) \cong \mathrm{Aut}(\mathbb{Z}_n)$.*

Proof.

1. Set a equal to whatever $f(1)$ is. Then by induction, $f(x) = f(1 + \cdots + 1)$ x times, so this equals $f(1) + \cdots + f(1) = ax$. So $f : x \to ax$. Then, $x \to ax$ is a homomorphism because $f(x + y) = a(x + y) = ax + ay = f(x) + f(y)$.

2. First if $\phi : x \to ax$ is an automorphism, it's surjective: $\exists x_0$ such that $ax_0 = 1$ which implies a is a unit with inverse x_0. Second, if $a \in U(n)$, let $b = a^{-1} \mod n$. We have $\phi_a : x \to ax$, $\phi_b : x \to bx$. Then $\phi_a \cdot \phi_b = id$, since $x \to a(bx) = (ab)x = 1x = x$, which implies ϕ_a invertible and thus bijective.

3. Part (b) proved that Φ is bijective. It's a homomorphism because $\Phi(ab) = (x \to (ab)x) = x \to a(bx) = \phi_a \cdot \phi_b = \Phi(a) \cdot \Phi(b)$ where $\cdot$ is function composition. This is like functional programming.

□

4 Cosets

Definition 4.1. A left coset of H in G is a set of the form $aH = \{ah : h \in H\}$ for $a \in G$.

Definition 4.2. A right coset of H in G is a set of the form $Ha = \{ha : h \in H\}$ for $a \in G$.

Call a a coset representative.

Example 4.3. Find the left and right cosets for $G = S_3$, $H = \langle(12)\rangle$; $|G| = 6, |H| = 2$. For the left cosets, we have $eH = \{e, (12)\}$. Then $(123)H = \{(123), (13)\}$. $(132)H = \{(132), (23)\}$. For the right cosets, we have $He = \{e, (12)\}, H(123) = \{(123), (23)\}, H(132) = \{(132), (13)\}$. There are three of each kind of coset, and there are always 2 elements per coset.

If G is non-abelian, then the left and right cosets are different in general.

Example 4.4. Let $G = (\mathbb{R}^2, +, 0)$. Let $H =$ some line through the origin. Then the cosets are the lines parallel to H (we have $(a + H)$ is a line shifted away that is still parallel to H).

Example 4.5. Let $G = D_n$ where $|G| = 2n$. Let R be the unit rotation and E be some fixed reflection. Let H be the subgroup generated by R, $\langle R\rangle$. We proved earlier that $G = H \cup EH$ and also $G = H \cup HE$. These are disjoint unions since H is all the rotations, and EH and HE is all the reflections.

Remark 4.6. Coset representatives are not unique. For $G = S_3$, we showed that $(123)H = \{(123), (13)\} = (13)H$.

Subgroups and equivalence relations were made for each other.

Theorem 4.7. *Define a relation $\sim$ on group G by saying $a \sim b$ iff $\exists h \in H$ such that $a = bh$. Then $\sim$ is an equivalence relation and its equivalence clases are the left cosets. (If you define $a \sim b$ if $a = hb$, then the classes are right cosets).*

Proof. We check reflexivity, symmetry, and transitivity. We see $a \sim a$ because $a = ae$, and $e \in H$. Now assume $a \sim b$, then $a = bh$. Then taking inverses, we see $ah^{-1} = b$ and $h^{-1} \in H$ by subgroup property. Thus $b \sim a$. Then if $a \sim b, b \sim c$, we have that $a = bh_1, b = ch_2$. Then note that $a = ch_1h_2$, and $h_1h_2 \in H$ under closure of subgroups. Therefore $a \sim c$ and we are done. The proof for right cosets being an equivalence relation is analagous. Since $\sim$ is an equivalence relation we have $S_a = \{ah : h \in H\} = aH$ by definition. These give a disjoint partition $\{S_a\}_{a \in H}$ of G. □

Theorem 4.8. *Any two left cosets aH and bH have the same cardinality. This also implies $|aH| = |H|$ since $e \in H$.*

Proof. Define $f : G \to G$ by $x \to (ba^{-1})x$. Then observe that the restriction of f to aH maps $ah \to bh$ ($x = ah$, then $f(x) = (ba^{-1})ah = bh \in bH$. Define $g : G \to G$ by $x \to ab^{-1}x$. Then the restriction of g to bH maps to aH, and thus this is an inverse function since $g \circ f(x) = ab^{-1}ba^{-1}x = x$ and similarly $f \circ g$ is also identity, implying bijectivity. Thus aH and bH have the same cardinality. □

Remark 4.9. The bijection $G \to G$ by $x \to x^{-1}$ maps the set of left cosets bijectively onto the set of right cosets. Consider $(aH)^{-1} = \{(ah)^{-1} : h \in H\} = \{h^{-1}a^{-1} : h \in H\} = \{h_0a^{-1} : h_0 \in H\}$ since H is closed under inverses. Now this is a right coset, Ha^{-1}! Thus any theorem about left cosets is also a theorem about right cosets, you just invert the whole group.

4.1 Lagrange's Theorem

Theorem 4.10. *Lagrange's Theorem.*
If G is a finite group and H is a subgroup, then $|H|$ is a divisor of $|G|$. The number of left cosets for H is $\frac{|G|}{|H|}$.

Proof. G is partioned by left cosets of H and each coset is finite and has the same number of elements as any other coset (that was the last theorem we proved). Each coset has $|H|$ elements. Therefore $|G| = k|H|$ and the result follows, where k is the number of cosets. □

Definition 4.11. The index of H in G, denoted $[G : H]$ is the number of left cosets of H.

Corollary 4.12. *If $|G|$ is finite, then $[G : H] = \frac{|G|}{|H|}$.*

4.2 Applications of Lagrange's Theorem

Corollary 4.13. *If G is finite and $a \in G$, then the order $|a|$ is a divisor of $|G|$.*

Proof. Well note that $|a| = |\langle a \rangle|$. Then letting $H = \langle a \rangle$ the cyclic subgroup, by applying Lagrange's theorem we get the result. □

Now let us consider some interesting questions: Find all groups of order 6 up to isomorphism. Are $\mathbb{Z}_6$ and $\mathbb{S}_3$ the only ones? Well we know that $U(7) \cong \mathbb{Z}_6$, and we know that $D_3 \cong S_3$. We know that these two groups are not the same, since one is abelian and one is non-abelian. Morever, there is no element of order 6 in S_3. Well, it turns out these are the only two groups of order 6 up to isomorphism, which we will get to next time. Now how about all groups of order $2p$, where p is an odd prime? How about p^2? We will do these next time.

There's one question we can answer right now though.

Corollary 4.14. *All groups of prime order p are cyclic. There is only one group of order p for each p up to isomorphism.*

Proof. Let $|G| = p$. Choose $a \in G$, $a \neq e$. Then $|a|$ divides p hence is 1 or p by Lagrange's theorem. By we said $|a| \neq 1$, therefore $|a| = p$! Thus G is cyclic and generated by a. □

Corollary 4.15. *If G is finite,*

$$a^{|G|} = e$$

for all $a \in G$.

Proof. Pick $a \in G$, then $|a| = n||G|$ by Lagrange's theorem. Then $a^{|G|} = a^{nk} \to (a^n)^k = e^k = e$. □

Definition 4.16. The exponent of G is the smallest positive integer $n = \exp(G)$ s.t. for all $a \in G$, $a^n = e$.

Example 4.17. In D_4, $\exp(D_4) = 4$ since $R^4 = e$, $(R^3)^4 = 3$, $e^4 = e$, and $E^2 = e$.

Theorem 4.18. *Fermat's Little Theorem.*
If p is prime and $a \in \mathbb{Z}$, then $a^k \equiv a \mod (p)$.

Proof. We have that $|U(p)| = p - 1$. Then choose $a \in \mathbb{Z}$. If $p|a$, then $a \equiv 0 \mod (p)$ and $0^k \equiv 0 \mod (p)$. If $p \not| a$, then they are relatively prime and $a \in U(p)$. Then we know that $a^{|U(p)|} \equiv 1 \mod (p)$, and thus $a^{p-1} \equiv 1 \mod p$ and we get the result by multiplying both sides by a. □

The converse of Lagrange's theorem is false in general: If $n||G|$, there may not be a subgroup H with $|H| = n$.

Theorem 4.19. *A_4 which has order 12 has no subgroup of order 6.*

We will note as a fact that this is the smallest example of a subgroup of order 12.

Proof. Assume the contrary, that there is some $H \leq A_4$ with $|H| = 6$. A_4 has elements of order 3, and in particular, 8 of them: $(123), (234), (134), (124)$ and each of their inverses, $(321), (432), (431), (421)$. Let a be an element of order 3. Then we claim that $a \in H$. If it were not, then $A_4 = H \cup aH$ and we have a partition of 2 sets of order 6. Which piece is a^2 in then? If $a^2 \in H$, then $(a^2)^2 = a^4 = a \in H$ which is a contradiction since it will be in aH. If $a^2 \in aH$, then $a \in H$, again contradiction. Thus $a \in H$. Since a was arbitrary among the order 3 elements, there are at least 8 elements in H, which contradicts $|H| = 6$, and thus we are done. □

Another useful theorem following from Lagrange is given here:

Theorem 4.20. *Size of product.*
Let the set $HK = \{hk : h \in H, k \in K\}$ for H, K subgroups of G. Then,

$$|HK| = \frac{|H| * |K|}{|H \cap K|}$$

5 Classifying Group Isomorphisms

Theorem 5.1. *If p is an odd prime, then any group G of order $2p$ satisfies either $G \cong \mathbb{Z}_{2p}, G \cong D_p$.*

Proof. The order of any element of G must divide $|G| = 2p$. Any element has order $1, 2, p, 2p$. If there were $a \in G$ of order $2p$, we'd be done: $\langle a \rangle$ has order $2p$, $G = \langle a \rangle$, G is cyclic of order $2p$. From now on assume all elements have only $1, 2, p$ as possible orders.

Lemma 5.2. *With these hypotheses, G has an element a of order p.*

The Sylow theorems are all about proving that a group will always have a subgroup of order p, p^2, etc. There is a beautiful theory here. Today we will do things ad-hoc.

Proof. Suppose every element has order 1 or 2. Then G is abelian. $b, c \in G$ order 2, bc is also of order 2. $(bc)^2 = e \to bcbc = e \to cb = b^{-1}c^{-1}$. We have $|G| \geq 6$ $(p \geq 3)$. Pick $b \in G$ of order 2, pick $c \in G$ s.t. $c \notin \langle b \rangle$. Then $\{e, b, c, bc\}$ is a subgroup of order 4. However, $4 \not| 2p$ since p is odd... This is a contradiction by Lagrange's Theorem. Thus we must have an element a of order p. □

Thus we may take $a \in G$ of order p; $|G| = 2p > p = |\langle a \rangle|$, so can choose $b \in G$, $b \notin \langle a \rangle$. Then $\langle a \rangle \cap \langle b \rangle$ has order $< p$. Yet $\langle a \rangle \cap \langle b \rangle$'s order must divide p which implies that $\langle a \rangle \cap \langle b \rangle$ has order 1. If b did have order p then $|\langle a \rangle \langle b \rangle| = \frac{|\langle a \rangle| \cdot |\langle b \rangle|}{|\langle a \rangle \cap \langle b \rangle|} = \frac{p \cdot p}{1} = p^2$. So G has at least p^2 distinct elements. But $p^2 \leq 2p$ since these elements are in G implying $p \leq 2$. So b has order 2. The same argument shows $ab, a^2b, a^3b, \cdots$ have order 2. This sounds dihedral! Define $f : D_p \to G$ by $R_{360/p} \to a$, $E \to b$. At this point you should have more details proving the isomorphism directly. But it is an isomorphism.

□

6 Groups Actions on Sets

Let S be a set.

Definition 6.1. An action of G on S is a homomorphism

$$T : G \to Sym(S)$$

where $Sym(S)$ is the group of all permutations of S. This implies

1. $T(a)$ is a permutation of S for all $a \in G$.

2. $T(ab) = T(a) \circ T(b)$

3. $T(a^{-1}) = T(a)^{-1}$

4. $T(e) = id$

Example 6.2. G acts on itself by left multiplication: $g \cdot x = gx$, $g \in G, x \in G$. We also have $(ab)x = a(bx)$ (first act by b, then act by a). This was the main observation in Cayley's theorem. It also acts on itself by right multiplication: let g act on x by $x \to xg^{-1}$. The action of ab is then $x \to x(ab)^{-1} = xb^{-1}a^{-1}$ which means first act by b and then act by a. In some sense, it keeps ab in order.

Example 6.3. G acts on itself by conjugation: $g \in G$ acts by $x \to gxg^{-1}$, and ab acts by $x \to (ab)x(ab)^{-1} = a(bxb^{-1})a^{-1}$, so it first acts by b and then acts by a, again preserving the order.

Example 6.4. The group Oc of rotations acts on the octahedron.

Remark 6.5. Let G act on S. The notation $T(g)(x)$ is abbreviated $g \cdot x$ or gx. Gallian defines an action to be only when $G \leq Sym(S)$. In effect, he requires T to be an injective homomorphism.

Definition 6.6. Stabilizer.
The stabilizer of an element $x \in S$ is stab(x) is the set of all $g \in G$ such that $gx = x$. It is a subgroup that fixes x.

Example 6.7. If $G = Oc$, the stab of a vertex is cyclic of order 4.

Definition 6.8. The orbit of $x \in S$ is

$$orb(x) = \{gx : g \in G\} = G \cdot x$$

Example 6.9. The orbit of a vertex of the octahedron under Oc is the set of 6 vertices. Note $6 \cdot 4 = 24$.

Example 6.10. The face center of the octahedron form an orbit of 8 elements; the stabilizer of each face center is cyclic of order 3. Note $8 \cdot 3 = 24$.

Example 6.11. The body center of the octahedron forms an orbit of order 1 point by itself. Take $stab = Oc$: $1 \cdot 24 = 24$.

Example 6.12. Let G act on itself by conjugation: $T(g)(x) = gxg^{-1}$ where $g \in G, xG$. Then we have $T(g) : X \to gxg^{-1}$. For this action, the orbit of x is the conjugacy class of x. The stabilizer is the centralizer $C(x) = \{g \in G : gx = xg\}$ (commute with x).

Definition 6.13. An action is transitive if it consists of only one orbit. G can carry every $x \in S$ to every $y \in S$.

Example 6.14. Oc acting on octahedron is not transitive. First we see that 6 vertices form one orbit and 12 edge-midpoints form another orbit. In fact there are uncountably many orbits.

Example 6.15. *Oc* does act transitively on the 6 **vertices** of the octahedron.

Remark 6.16. Note that the orbits form a partition of S. (Say $x \asymp y$ iff $\exists g \in G$ s.t. $g \cdot x = y$). It is also an equivalence relation. You can look at how the group moves things around and focus on one orbit at a time. This action is transitive.

Theorem 6.17. *Let $x \in S$ be a fixed starting point. Let H be the stabilizer of x. If G acts transitively on S, then there is a one-to-one correspondance between G/H and S given by $\phi : gH \to g \cdot x$. Anything you can do with vertices you can do with cosets.*

Proof. First, ϕ is well-defined. If $g_1H = g_2H$, we have to show that $g_1 \cdot x = g_2 \cdot x$. If $g_1H = g_2H$, then $g_2^{-1}g_1H = H$, which means that $g_2^{-1}g_1e \in H$, which shows that $g_2^{-1}g_1 \in H$. But this implies $g_2^{-1}g_1 \cdot x = x$. Finally, multiply by g_2 on both sides. $g_2g_2^{-1}g_1 \cdot X = g_2 \cdot X \to g_1 \cdot x = g_2 \cdot x$.

Now we have to prove injective and surjective. If $g_1x = g_2x$, we must show $g_1H = g_2H$. $g_1 \cdot x = g_2 \cdot x$ so $g_2^{-1}g_1 \cdot x = x$, which means that $g_2^{-1}g_1$ does not move x, thus it is in H. Therefore, $g_1 \in g_2H$. Since cosets form a partition, we have that $g_1H \cap g_2H \neq \emptyset$ at the element g_1, we must have $g_1H = g_2H$.

For surjectivity, take any $y \in S$. Since the action is transitive, $\exists g \in G$ s.t. $g \cdot x = y$. Then $\phi : gH \to y$. □

Example 6.18. How to classify all transitive actions of S_3? For instance, take any set of 5 points - can we get S_3 to carry every point to every point? Perhaps we can take two actions and they could be different?

You can classify all subgroups $H \subseteq S_3$, and secondly, for each H, understand the action on G/H.

Let's look at all subgroups of S_3:

Table 1: Subgroups of S_3

order of $\lvert H\rvert$	H
6	S_3
3	$\langle(123)\rangle = \{e, (123), (132)\}$
2	$\langle(12)\rangle; \langle(13)\rangle; \langle(23)\rangle$
1	$\{e\}$

Conjugation carries each subgroup of order 2 to each other subgroup. They're isomorphic, not equal.

Note that $H = stab(x)$ for some initial point x. Also let $\cdot$ be the action on one point. The corresponding transitive actions are

For $\langle(12)\rangle$, Cayley's Theorem gives that the action on 6 points must be on $G/\{e\} = G = S_3$). Act on G by left multiplication, which is transitive because $g \cdot g_1 = g_2$ for a g that carries g_1 to g_2, namely $g = g_2g_1^{-1}$.

In fact we are doing a form of representation theory. Usually we do linear representation and we get matrices and we do things with characters and the matrices act on a vector space. Then you get a finite list of irreducible representations. Actions can also be called permutation representations, but are not linear since they are acting on sets of points and not vector spaces.

Table 2: Transitive Actions of S_3

H	action
S_3	$\cdot$
$\langle(123)\rangle$	$H = A_3$. Action if a even, don't move the 2 points; if g odd, flip them.
$\langle(12)\rangle$	the standard action on S_3 that defines S_3 where $x = 1$
$\{e\}$	left multiplication on G

Theorem 6.19. *Orbit-stabilizer Theorem.*
Let G act on S. Let $x \in S$. Then $|G| = |orb(x)| \cdot |stab(x)|$.

Proof. Restrict the action to just the orbit of x. Then G acts transitively. Last theorem said that orb(x) was a one-to-one correspondance with $G/stab(x)$. Let $H = stab(x)$. Lagrange's theorem said $|G| = |H| \cdot |G/H|$ (recall $|G/H| = [G : H]$). This equals $|stab(x)| \cdot |orb(x)|$. □

6.1 Convex Polyhedra

For our purposes, a convex polyhedron (or convex polytope) is an intersection of closed half-spaces in $\mathbb{R}^n$ so the result is bounded and of full dimension n. An $\mathbb{R}^{n-1}$ is a wall separating 2 halves of $\mathbb{R}^n$, and an $\mathbb{R}^{n-2}$ is what you chain your dog to in $\mathbb{R}^n$.

Definition 6.20. Codimension is $n - k$, where k is the dimension of your object.

Definition 6.21. Every convex polytope P has a dual P^* with the following properties.

1. vertices of P correspond in a one-to-one way with $n-1$-dimensional faces of P^*.

2. edges of P correspond in a one-to-one way with $n-2$-dimensional faces of P^*.

3. i-dimensional faces of P corerspond in a one-to-one way with $n-i$ dimensional faces of P^*.

Whenever two faces meet here, the corresponding faces meet here.

Example 6.22. The dual of the octahedron in $\mathbb{R}^3$ is the cube. We have duality of vertices of the cube to faces of octahedron, and edges of cube to edges of octahedron.

Example 6.23. The dual of the tetrahedron is self-dual.

Example 6.24. The icosahedron and dodecahedron are dual.

In general, P^* cannot be inscribed in P. Instead, P^* is defined as follows: Move P so that the origin is in its interior; each closed half-space of P is defined by a normal vector v_i and a distance r_i. Let the point-vectors be defined as p_j. To create P^*, go to a separate copy of $\mathbb{R}^n$ and put in the closed half spaces $p_j^{\perp}$ and the points $\frac{1}{r_i}v_i$. You can also define this by the convex hull of the points.

The platonic solids are special; their dual polytopes can be inscribed in each other and in fact are closed under the dual operation. Note that this gives you that the automorphism groups of the platonic solids are therefore the same since Rot($cube$) =Rot(Oc) $\cong S_4$. We also have Rot($tetrahedron$) $\cong A_4$.

To summarize, Rot(tetrahedron) $\cong A_4$, Rot(octahedron) = Oc $\cong S_4$, Rot(cube) = Oc since the cube is dual to the octrahedron.

Lemma 6.25. *A_n is generated by 3-cycles (which are even permutations: Every even permutation is some product of three cycles).*

Proof. Let g be any element of A_n. Write g in disjoint cycle notation. First, any k-cycle with $k \geq 3$ is a product of 3 cycles, and one transposition if the cycle is odd.

Example 6.26. $(abcdef) = (abc)(cdef) = (abc)(cde)(ef)$

Now suppose g is a product of 3-cycles and 2-cycles in some order. Then (...)(...)(..)(...)(...)(...)(..). We want to move the extra transposition to the right of the three cycle by conjugation. That is to say, if we have $(ab)(cde)$, not distinct values, we can say that this equals $(ab)(cde)(ab)^{-1}(ab)$. When you conjugate a 3-cycle, you get a 3-cycle. Thus, $(ab)(cde) =$ (...)(ab). Eventually, we will have (...)(...)(...)(..)(..)(..)(..) where we have several 3 cycles and an even number of two-cycles. Finally, any (..)(..) can be made from 3-cycles. In case one, we have $(ab)(ab) = e$ which is 0 three-cycles. Then when there is one element shared $(ab)(ac)$, with a, b, c distinct, we have $(ab)(ac) = (ba)(ac) = (bac)$. Finally, we have $(ab)(cd)$ all distinct. Just do $(ab)(cd) = (abc)(bcd)$ and we get two three cycles. □

Theorem 6.27. *Rot(icosahedron) $\cong A_5$.*

Proof. Basically you have 5 different tetrahedrons at the face centers at the top of the icosahedron. However, all of the tetrahedra will reflect each other: This gives us chirality. The rotations carry the five tetrahedra to others. Thus they permute the five tetrahedra, thus Rot(icosahedron) $\subseteq S_5$. Now we need to say that these permutations are only even permutations. Let's count how many there are: There are 20 faces; you can rotate around each face 3 times, this gives a total of $20 \cdot 3 = 60 = 5!/5$ which is the order of A_5. How do we know there is not some other subgroup of order 60 in S_5? It now suffices to show that every 3-cycle is in the rotation group. Pick a random position and consider a 3-cycle of it. Then there are 10 pairs of colors, and thus 30 edges in all. Thus all the 3-cycles are in the group, and these generate A_5 which has size 60, so we are done. □

Corollary 6.28. *Rot(dodecahedron) $\cong A_5$. Iscosahedron and dodecahedron are dual.*

Definition 6.29. Truncation of a polytope.
Cut off a small neighborhood of a vertex with a plane. If you do this in general, the rotation group gets smaller. If you only chop one vertex, you totally trash the rotation group! If you do the same thing to all of them, you don't get the same symmetries in general. For a Platonic solid, you can truncate so the new cut-face is symmetrical. Also, you can cut every vertex equally symmetrically and to the same depth. In that case, the rotation group does not change.

Definition 6.30. The cuboctahedron is where you truncate an octahedron or cube as deeply as possible (while remaining convex).

Claim 6.31. *The soccer ball is what you get if you truncate an icosahedron halfway at each vertex. Since the icosahedron has 20 faces, you will get 20 hexagons on a soccer ball. Therefore Rot(soccer ball) $\cong A_5$.*

7 Direct Products

Definition 7.1. The external direct product of groups $G_1, \cdots, G_n$ is denoted $G_1 \times G_2 \times \cdots \times G_n$ is the group with elements $(g_1, \cdots, g_n)$. Multiplying is defined term by term: $(g_1, \cdots, g_n) \cdot (h_1, \cdots, h_n) = (g_1h_1, \cdots, g_nh_n)$.

Claim 7.2. *This is a group and* $(g_1, g_2, \cdots, g_n)^{-1} = (g_1^{-1}, g_2^{-1}, \cdots, g_n^{-1})$*. Identity is* $(e_{G_1}, \cdots, e_{G_n})$*. We also note that* $|(g_1, g_2, \cdots, g_n)| = \text{lcm}(|g_1|, \cdots, |g_n|)$*.*

We use the same definition for rings: $R_1 \times R_2 \times \cdots \times R_n$ with + and $\cdot$ term-by-term. One school of thought says we should say $\bigoplus$ is used for finitely many terms and $\prod$ for ∞-products. $\bigoplus$ also tends to denote abelian.

Theorem 7.3. *Chinese Remainder Theorem.*
If m, n relatively prime, there is an isomorphism of rings $\mathbb{Z}_{mn} \to^{\cong} \mathbb{Z}_m \bigoplus \mathbb{Z}_n$ *given by* $x \mod (mn) \to (x \mod m, x \mod n)$*.*

Corollary 7.4. *On additive groups, if m, n relatively prime, then* $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \bigoplus \mathbb{Z}_n$*.*

Example 7.5. $\mathbb{Z}_2 \bigoplus \mathbb{Z}_3$ is cyclic of order 6, generated by $(1, 1)$. We have $(0, 0) = (6, 6)$, $(1, 1)$, $(0, 2) = (2, 2)$, $(3, 3) = (1, 0)$, $(4, 4) = (0, 1)$, $(5, 5) = (1, 2)$. If they were not relatively prime, they would coincide with each other earlier.

Theorem 7.6. *If m, n are not relatively prime, then the additive group* $\mathbb{Z}_m \bigoplus \mathbb{Z}_n$ *is not cyclic.*

Proof. Since m, n are not relatively prime, the $\text{lcm}(m, n) = L < mn$.

Lemma 7.7. $gcd(m, n) \cdot lcm(m, n) = mn$

Proof. For each prime p, say p^a is the highest power of p in m. Also say p^b is the highest power of p in n. Then note that the highest power in the gcd is $p^{\min(a,b)}$. In the lcm, the highest power is $p^{\max(a,b)}$. Thus for each p in the product, $p^a p^b$ is the power of p in mn. In the product, each of these is present since $\min(a, b) + \max(a, b) = a + b$, and thus we have equality. □

Now note that $s \cdot (x, y) = (sx, sy)$. Assume that there is an element (x, y) of order mn. Then $m \cdot (x, y) = (mx, my) = (0, my)$ and $n \cdot (x, y) = (nx, 0)$. Then $m|L, n|L$, so $L \cdot (x, y) = (0, 0)$. So (x, y) has order a divisor of L, which is a contradiction since $L < mn$. □

Example 7.8. No element of $\mathbb{Z}_8 \times \mathbb{Z}_2$ has order 16.

We now give a list of useful facts.

1. $U(p)$ is cyclic of order $p - 1$.

2. $U(p^n)$ is cyclic of order $\phi(p^n) = p^n - p^{n-1}$.

3. $U(2^n)$ is $\cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{n-2}}$ for $n \geq 2$, and is generated by $-1, 5$.

4. $U(mn) \cong U(m) \times U(n)$ if m, n relatively prime (This is just the Chinese Remainder Theorem). For instance, $U(72) = U(8) \bigoplus U(9) = \mathbb{Z}_2 \bigoplus \mathbb{Z}_2 \bigoplus \mathbb{Z}_6$. Each element has order a divisor of 6.

Remark 7.9. On Primitive Roots.

Definition 7.10. A primitive root a mod p generates $U(p)$.

We might ask for a fixed $a \in \mathbb{Z}$, for which p is a a primite root? McConnell's undergraduate thesis was about the case $a = 2$. You have to go to class field theory to get any answer, and there is no closed form. However, it is true that about 37% (Artin's constant) of p have $a = 2$ as a primitive root. This is also related to the generalized Riemannn Hypothesis.

8 Normal Subgroups

Let $H \subseteq G$. When do the left cosets of H form a group in their own right? Given $g_1, g_2 \in G$, we want a g_3 depending on g_1, g_2 so that $g_1H \cdot g_2H = g_3H$. Well the left hand side contains $g_1e \cdot g_2e$ and the right hand side contains g_3e. It is natural to let $g_3 = g_1 \cdot g_2$. That is, $(g_1H \cdot g_2)H = g_1g_2H$. The difficulty is that g_1hg_2 for all $h \in H$ may be representative of more than one coset. If they all lie in one coset, it implies $g_1hg_2 \in g_1g_2H$ for all $h \in H$. Then multiply on the left to get $hg_2 \in g_2H$ for all $h \in H$. Well, this just means that $g_2^{-1}hg_2 \in H$ for all $h \in H$. Thus, if multiplying cosets is to give us a group, we have that H must be **closed under conjugation**, since g_2 was arbitrary.

Definition 8.1. Let H be a subgroup of G. Then H is **normal** (or **self-conjugate**) if for all $g \in G$

$$g^{-1}Hg \subseteq H$$

A normal subgroup is a union of conjugacy classes. In the physical rotation setting, a subgroup which is normal typically has no arbitrariness.

Remark 8.2. We have $H \trianglelefteq G$ denotes a normal subgroup.

The idea is that if $H \trianglelefteq G$, then if you list the $h \in H$ in a certain sequence, then $g^{-1}hg$ runs through H also, but in a different order.

Theorem 8.3. *If $H \subseteq G$ then H is normal iff $Hg = gH$ for all $g \in G$.*

Proof. To show $Hg \subseteq gH$, pick $x \in Hg$. That is $\exists h_1 \in H$ with $x = h_1g$. Then $x = g(g^{-1}h_1g) = gh_2$ for some $h_2 \in H \in gH$ because of normality. Similarly $gH \subseteq Hg$. Thus $Hg = gH$ for all $g \in G$, and we have $g^{-1}Hg = g^{-1}gH = H$ is normal. □

Example 8.4. $G = D_n$, $H = \langle R \rangle$. Then $H \trianglelefteq G$. First we check it is self conjugate. Every $g \in G$ is a product of Rs and Es. $R^{-1}R^kR = R^k \in H$. Then $E^{-1}R^kE = R^{-k} \in H$. So it is self-conjugate under every element. Now we check the order. ER^k for $k = 0, 1, \cdots, n-1$. This is just $R^{-k}E$ for $k = 0, 1, \cdots, n-1$. If we change this to R^lE, then we have $l = 0, n-1, n-2, \cdots, 2, 1$. It's the same coset, just listed differently. Thirdly, check that $Hg = gH$. Then $He = eH$ and $HE = EH$ since $ER^k = R^{-k}E$.

Remark 8.5. If $H \subseteq \langle R \rangle$ in $G = D_n$, then $H \trianglelefteq G$. If H is generated by R^k (cyclic of order n/k) then $ER^kE = R^{-k} \in H$.

Example 8.6. $A_n \trianglelefteq S_n$. If $h \in A_n$ (even), $g \in S_n$ (is a product of k transpositions), then $g^{-1}hg = ()()...()(....)()()...()$, k transpositions surrounding an even cycle, means there are even $+2k$ total, which is still even.

Example 8.7. There is a normal subgroup $V \trianglelefteq S_4$ where $V = \{e, (12)(34), (13)(24), (14)(23)\}$. This is the conjugacy class of e unioned with the conjugacy class of shape (..)(..). It is a special case that for $n = 4$, V is closed under multiplication (it happens that in S_5 that you produce 3-cycles when multiplying).

Remark 8.8. In linear algebra, if A is the $n \times n$ matrix of a linear transformation on a certain basis B, then recall conjugation in linear algebra: SAS^{-1} is the matrix on another basis $\tilde{B}$ and S is the change of basis matrix between B and $\tilde{B}$. So conjugation in linear algebra is **change of basis**. Conjugation is thus the generalization of change of basis to any group!

Claim 8.9. *If G is abelian, then every subgroup H is normal.*

Proof. Let G be abelian. Then $H \subseteq G$. For all $g \in G$, for all $h \in H$, $ghg^{-1} = hgg^{-1}$ and thus $gHg^{-1} = H$. □

Claim 8.10. *The center $Z(G)$ is an abelian subgroup of G, and thus $Z(G)$ is normal.*

Proof. Let $H = Z(G)$. For any $g \in G$ and for all $h \in H$, $ghg^{-1} = hgg^{-1} = h$ since h commutes with everybody (is **central**), and thus $gHg^{-1} = H$. □

Theorem 8.11. *Let $H \trianglelefteq G$. Then the set G/H of left cosets is a group under the law*

$$g_1Hg \cdot g_2H = g_1g_2H$$

*This group G/H is called the **quotient group**, or some people call it the **factor group**, or "$G \mod H$".*

Remark 8.12. The right cosets $H \setminus G$ are the very same group since $Hg = gH$.

Proof. First we must prove that the law is well-defined. $g_1h_1 \cdot g_2h_2 = g_1(g_2g_2^{-1}h_1)g_2h_2 = g_1g_2(g_2^{-1}h_1g_2)h_2 = g_1g_2h_3h_2 \in g_1g_2H$ since $h_3h_2 \in H$. We need normality to perform this operation. Then the rest of the proof is routine: $eH = H$ is the identity, $(gH)^{-1} = g^{-1}H$. □

Example 8.13. $G = D_n$, $H = \langle R \rangle$ which is cylic of order n. Then $G/H \cong \mathbb{Z}_2$. Elements of G/H are $H, E \cdot H$ where E is a reflection. The group law is $EH \cdot EH = E^2H = eH$.

Example 8.14. Let $G = D_4$, $H = Z(G) = \langle R^2 \rangle = \langle R_{180} \rangle$. Then $H \trianglelefteq G$. We claim $H/G \cong D_2$ is the dihedral group of the digon, the two-sided polygon. Modding out by R^2 is just identifying opposite points in the square with each other. Then $D_2 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Example 8.15. $S_4/V \cong S_3$. Recall S_4 is order 24, V is order 4 and S_3 is order 6.

V acts transitively on the set $\{1, 2, 3, 4\}$. In fact, the action is **uniquely transitive**: for all $a, b \in \{1, 2, 3, 4\}$ there is a unique element of V carrying a to b, namely $(ab)(cd)$ if $a \neq b$, or e if $a = b$. Let $g \in S_4$ be arbitrary. Say $g : 4 \to a$. There does not exist $h \in V$ carrying $4 \to a$. Then gh fixes 4. So $gh \in Sym(\{1, 2, 3\}) = S_3$. Then if we map $S_4/V \to^{\cong} S_3$ by the following: in the coset gV, choose the unique element $g_1 = gh$ with $g_2 \in S_3$; write g_1V instead of gV.

Example 8.16. $G = (\mathbb{Z}, +, 0)$. Any subgroup of G is normal since G is abelian. Any $H \subseteq G$ is $H = \langle n \rangle$ for some $n \in \mathbb{Z}$. Then $\mathbb{Z}/n\mathbb{Z}$ is the rigorous meaning of $\mathbb{Z} \mod n$. Then $1 + 3\mathbb{Z}$ is the coset which is the set of integers $\cong 1 \mod 3$.

In general, $a + n\mathbb{Z} = b + n\mathbb{Z}$ iff $n\mathbb{Z} = (b - a) + n\mathbb{Z}$ iff $b - a \in n\mathbb{Z}$ iff $n|(b-a)$ iff $a \equiv b \mod n$.

The idea is that G/H is a group related to G but with simpler structure. You're effectively connecting together some things which were not connected together before. Thus you are removing some complexity of the group. You can often draw conclusions about G from knowing H and G/H.

Example 8.17. H and G/H do not determine G even in order 4, the first non-prime order. Let $G_1 = \mathbb{Z}/4\mathbb{Z}$, $H = 2\mathbb{Z}/4\mathbb{Z}$. Then $G_1/H = \mathbb{Z}/2\mathbb{Z}$. Therefore, both H and G_1/H are cyclic of order 2, which is isomorphic to $\mathbb{Z}_2$. Then in the other case, let $G_2 = \langle a, b \rangle$ where a, b are of order 2 and commute. $G_2 = \{e, a, b, ab\}$, and $H = \langle b \rangle$. Then $H = \{e, f\}$, $aH = \{a, ab\}$, and G_2/H has order 2, generated by $a \mod H$. Again, $H, G_2/H$ are both $\cong \mathbb{Z}_2$. However, $G_1 \ncong G_2$, despite H and G_2/H being equivalent to H and G_1/H.

Recall that $Z(G)$, the center of G, is a normal subgroup of G.

Theorem 8.18. *If $G/Z(G)$ is cyclic, then G is abelian.*

Proof. Recall that if G is abelian only when $G = Z(G)$. Therefore, we will show that $G/Z(G)$ has only one element. Let us consider the elements of $G/Z(G)$: $eZ(G), xZ(G), x^2Z(G), \cdots, x^{n-1}Z(G)$. Then note that all these elements commute since $G/Z(G)$ is cyclic, and thus by the pullback map of the homomorphism $G \to G/Z(G)$, we must have that these elements commuted with each other. Since each of these elements already commutes with all of $Z(G)$ by definition, we must have that all elements of G commute and therefore G is abelian. □

Therefore we also see that if $G/Z(G)$ is cyclic, it must be trivial.

We note that the contrapositive statement is most useful:

Theorem 8.19. *If G is not abelian, then $G/Z(G)$ is not cyclic.*

We also have

Theorem 8.20. $G/Z(G) \cong \mathrm{Inn}(G)$.

8.1 Class Equation

Recall that the conjugacy classes in G are a partition of G. Now let G be finite and let its conjugacy classes have representatives $x_1, \cdots, x_k$. Thus, $G = \{gx_1g^{-1} | g \in G\} \sqcup \{gx_1g^{-1} | g \in G\} \sqcup \cdots \sqcup \{gx_kg^{-1} | g \in G\}$. If you've used up all elements of G, then you're done. Otherwise keep going. Then $|G| = |C_1| + \cdots + |C_k|$. C_i is the orbit of x_i under the action of G by conjugation. Then $|C_i| = \frac{|G|}{|stab(x_i)|}$. The stabilizer of x_i is the centralizer $C(x_i) = \{g \in G : gx_i = x_ig\}$. Then the class equation is given by

$$|G| = \sum_{i=1}^{k} \frac{|G|}{|C(x_i)|} \tag{2}$$

Definition 8.21. A p-group is a group of finite order p^n for p prime.

Then the application of the class equation to p-groups gives that

Theorem 8.22. *A non-trivial p-group has non-trivial center.*

Proof. We have $|G| = p^n$, $n \geq 1$. In particular, $|G| \equiv 0 \mod p$. In any group $\{e\}$ is a conjugacy class by itself: $geg^{-1} = gg^{-1} = e$. Note that $|C(x_i)|$ is a power of p for all $i \in [k]$ by Lagrange's Theorem. Therefore, $|G|/|C(x_i)|$ is also a power of p for all i. Powers of p^n mod p are 0 unless the power $p^n = 1$. The class equation says that $0 \equiv 1 + ? + \cdots + ?$, where all the question marks are either 1 or 0 mod p. At least p of the entries must be ones, otherwise there is no way we can get 0 from the sum of 1s. If x_i generates a conjugacy class of order 1, then $gx_ig^{-1} = x_i$ for all g, and $gx_i = x_ig$, which means $x_i \in Z(G)$. Thus since there are at least p of these such that $|\langle x_i \rangle| = 1$ as we said before, we must have $|Z(G)| \geq p$. □

To understand that a p-group G, let $G_1 = G/Z(G)$, strictly smaller than G. G_1 is a p-group, so $G_2 = G_1/Z(G_1)$, which is smaller than G_1. Since G was finite, this process stops after some number of steps j where $G_j = \{e\}$. Then you try to reconstruct G_{j-1}, G_{j-2}, G_{j-3}, and so on.

Theorem 8.23. *(Cauchy).*
If G is a finite abelian group and $p||G|$, p prime, then G has an element of order p.

Proof. Since G is abelian, all its subgroups are normal. Taking any $x \in G$, $x \neq e$. Say $|x| = n$, $n||G|$. Let q be some prime factor of n. Then $x^{n/q}$ has order q in G. If $q = p$, we are done, so suppose that $q \neq p$. Let $w = x^{n/q}$ and $H = \langle w \rangle$ of order q. G/H has order $\frac{|G|}{q}$, which is smaller than $|G|$ and is divisible by p. Then we proceed by strong induction on the size of G_i. Take for granted that $G_1 = G/H$ has an element y of order p, that is, coset yH has order p. Therefore $y^p \in H$, $y^p = w^k$ for $k = 0, \cdots, q-1$. If $k = 0$, then y really does have order p in G. If $k \neq 0$, then w^k has order q in G. Then $y^{pq} = w^{kq} = e$. Then, y^q must have order p since pq does not factor any more. □

8.2 Internal Direct Products

We have defined the internal direct product $G = G_1 \times G_2$ to be $G = \{(g_1, g_2)|g_1 \in G_1, g_2 \in G_2\}$. Identify G_1 with $\{(g_1, e)|g_1 \in G_1\}$. Informally, $G_1 \cong G_1 \times \{e\}$. Identify G_2 with $\{(e, g_2)|g_2 \in G_2\}$, $G_2 \cong e \times G_2$. Once you do this, note $G_1 \trianglelefteq G$ since $(x, y)(g_1, e)(x, y)^{-1} = (xg_1x^{-1}, yey^{-1}) = (xg_1x^{-1}, e)$. Similarly $G_w \trianglelefteq G$. Then, $G = G_1G_2 = \{(g_1, e) \cdot (e, g_2)|g_1 \in G_1, g_2 \in G_2\} = \{(g_{1,g} 2)\}$. Finally, $G_1 \cap G_2 = \{(e, e)\}$.

Definition 8.24. If G has subgroups H, K with

1. $H \trianglelefteq G$

2. $K \trianglelefteq G$

3. $G = HK$

4. $H \cap K = \{e\}$

Then we say H, K give G the structure of internal direct product.

In general, the condition is a bit more complicated:

Definition 8.25. If G has subgroups $H_1, H_2, \cdots, H_n$ all normal, then if

1. $G = H_1 H_2 \cdots H_n$
2. $(H_1 \cdots H_j) \cap H_{j+1} = \{e\}$ for all $j = 1, \cdots, n-1$.

$\prod_{i=1}^{n} H_i$ is an interal direct product representation of G and is isomorphic to $H_1 \times \cdots \times H_n$.

Theorem 8.26. *If you have an internal direct product, $G \cong H \times K$. The map is for $g \in G$, $g = hk$ for some $h \in H, k \in K$; $\phi(hk) = (h, k)$ is an isomorphism.*

Proof. Well-defined: If $g = hk$ and $g = h_1 k_1$, we must show $h = h_1$ and $k = k_1$. This is because $hk = h_1 k_1$. Then, ϕ is a homomorphism: $g_1 = h_1 k_1$, $g_2 = h_2 k_2$. $\phi(g_1 g_2) = \phi(h_1 k_1 h_2 k_2) = \phi(h_1 k_1 h_2 k_1^{-1} k_1 k_2) = \phi(h_1 h_3 k_1 k_2)$ where $h_3 = k_1 h_2 k_1^{-1} \in H$ since H is normal. Thus, this equals $(h_1 h_3, k_1 k_2)$ and we have $\phi(g_1) \cdot \phi(g_2) = (h_1, k_1) \cdot (h_2, k_2) = (h_1 h_2, k_1 k_2)$. We need to show $h_3 = h_2$. □

Then we have some immediate results which follow:

Theorem 8.27. *Groups of Order p^2.*
Let p be prime. A group of order p^2 is isomorphic to either $\mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \oplus \mathbb{Z}_p$. Thus, in all cases, groups of order p^2 are abelian.

9 Homomorphisms and the Isomorphism Theorems

Recall that a homomorphism is a map between two groups which preserves the algebraic operations. First, we give an important definition:

Definition 9.1. The kernel of a homomorphism $\phi : G \to G'$ is defined as

$$\mathrm{Ker}(\phi) = \{x : \phi(x) = e, x \in G\}$$

It is analagous to the nullspace from linear algebra.

We now note some important properties of homomorphisms and the kernel.

1. $\mathrm{Ker}(\phi)$ is a normal subgroup of G.
2. $\phi(a) = \phi(b)$ iff $a\mathrm{Ker}(\phi) = b\mathrm{Ker}(\phi)$.
3. The inverse map ϕ^{-1} from $g' \in G$ is the kernel $g\mathrm{Ker}(\phi)$, where $\phi(g) = g'$.

Now we come to the isomorphism theorems. $\phi : G \to G'$ denotes an isomorphism.

Theorem 9.2. *First Isomorphism Theorem.*
The map $\psi : G/\mathrm{Ker}(\phi) \to \phi(G)$, given by

$$\psi(g\mathrm{Ker}(\phi)) = \phi(g)$$

is an isomorphism. Thus $g\mathrm{Ker}(\phi) \cong \phi(g)$. This mapping is considered natural, and one can draw an appropriate commutative diagram.

Proof. Note that since the kernel is a normal subgroup, we can quotient by it and thus the elements of $G/\mathrm{Ker}(\phi)$ can be written $g_1\mathrm{Ker}(\phi), \cdots, g_n\mathrm{Ker}(\phi)$. Then the map is by definition one-to-one, since each $g_i\mathrm{Ker}(\phi)$ is mapped to $\phi(g_i)$, which are necessarily unique since $\phi(a) = \phi(b)$ iff $a\mathrm{Ker}(\phi) = b\mathrm{Ker}(\phi)$. We now show that ψ preserves algebraic operations:

$$\begin{aligned}\psi(g_1\mathrm{Ker}(\phi) \cdot g_2\mathrm{Ker}(\phi)) &= \psi\left(g_1 g_2\mathrm{Ker}(\phi)\right) \\ &= \phi(g_1 g_2) = \phi(g_1)\phi(g_2) \\ &= \psi(g_1\mathrm{Ker}(\phi)) \cdot \psi(g_2\mathrm{Ker}(\phi))\end{aligned} \tag{3}$$

□

Corollary 9.3. *Note this implies that $|\phi(G)|$ divides both $|G|$ and $|G'|$. This is because $\phi(G)$ is isomorphic to $g_1\mathrm{Ker}(\phi), \cdots, g_n\mathrm{Ker}(\phi)$, which are all distinct since the kernel is normal. Thus $|\phi(G)| = |G|/|\mathrm{Ker}(\phi)|$. Then, $\phi(G)$ must be a subgroup of G' and therefore its order must divide $|G'|$.*

Theorem 9.4. *Normal subgroups correspond to kernels. In particular, the normal subgroup N of G corresponds to the kernel $g \to gN$ from $G \to G/N$.*

Another corollary is useful for analyzing automorphisms.

Corollary 9.5. *Let $N(H)$ be the normalizer $\{x \in G : xHx^{-1} = H\}$ and $C(H)$ be the centralizer $\{x \in G : xh = hx \forall h \in H\}$. Then consider the map $\psi : N(H) \to \mathrm{Inn}(H) \leq \mathrm{Aut}(H)$*

$$\psi(g) = \phi_g$$

where $\phi_g(x) = gxg^{-1}$ is an inner automorphism. Then, ψ is a homomorphism with kernel $C(H)$ since for any g s.t. $\psi(g) = \phi_e$, we must have g commutes with all $x \in H$, i.e., the centralizer of H. Therefore,

$$N(H)/C(H) \cong \psi(N(H)) \leq \mathrm{Inn}(H) \leq \mathrm{Aut}(H)$$

We now state the second and third isomorphism theorems.

Theorem 9.6. *Second Isomorphism Theorem.*
If K is a subgroup of G and N is a normal subgroup of G, then

$$K/(K \cap N) \cong KN/N$$

Theorem 9.7. *Third Isomorphism Theorem.*
If M and N are normal subgroups of G and $N \leq M$, then

$$(G/N)/(M/N) \cong G/M$$

10 Classification of Finite Abelian Groups

Theorem 10.1. *Let G be a finite abelian group. Then $G \cong \mathbb{Z}_{d_1} \oplus \mathbb{Z}_{d_2} \oplus \cdots \oplus \mathbb{Z}_{d_k}$, with $d_i \in \mathbb{N}$ and $d_1|d_2, d_2|d_3, \cdots, d_{k-1}|d_k$. Furthermore, the d_i are uniquely determined by G. They are called the "elementary divisors".*

Example 10.2. Classify the abelian groups of order 8. How can you write 8 as an ascending product of powers of 2? Well, you could take 8. The next power of 2 is 4: so $2 * 4$. Then the last thing we can do is $2 * 2 * 2$. These are the only ways to make 8 as an ascending product, so the abelian groups of order 8 correspond to these: $\mathbb{Z}_8, \mathbb{Z}_2 \oplus \mathbb{Z}_4, \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Definition 10.3. A number-theoretic partition of $n \in \mathbb{N}$ is an expression $a_1 + a_2 + \cdots + a_k = n$, where $a_1 \leq a_2 \leq \cdots \leq a_k$.

Definition 10.4. The number of number-theoretic partitions of n is $\pi(n)$.

Corollary 10.5. *The number of abelian groups of order k^n, up to isomorphism, is $\pi(n)$.*

To find all abelian groups of order $n = p_1^{n_1} p_2^{n_2} \cdots p_m^{n_m}$, combine the partitions for each $p_i^{n_i}$.

Example 10.6. Find all abelian groups of order 360.
Well, $360 = 2^3 * 3^2 * 5$. The only partitions of 2^3 are $8, (2, 4), (2, 2, 2)$. The only partitions of 3^2 are $9, (3, 3)$. Finally, the only partition of 5 is 5. Therefore, there are $3 * 2 * 1 = 6$ abelian groups of order 360:

$$\begin{aligned} \mathbb{Z}_8 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5 &\cong \mathbb{Z}_{360}, \\ \mathbb{Z}_3 \oplus (\mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_8) &\cong \mathbb{Z}_3 \oplus \mathbb{Z}_{120}, \\ \mathbb{Z}_2 \oplus (\mathbb{Z}_4 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5) &\cong \mathbb{Z}_2 \oplus \mathbb{Z}_{180}, \\ (\mathbb{Z}_2 \oplus \mathbb{Z}_3) \oplus (\mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5) &\cong \mathbb{Z}_6 \oplus \mathbb{Z}_{60}, \\ \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus (\mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5) &\cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{90}, \\ \mathbb{Z}_2 \oplus (\mathbb{Z}_2 \oplus \mathbb{Z}_3) \oplus (\mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5) &\cong \mathbb{Z}_2 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_{30} \end{aligned} \tag{4}$$

Since G is finite, it is finitely generated: $G = \langle g_1, \cdots, g_m \rangle$. Since G is abelian, there is a (surjective) homomorphism $\phi : \mathbb{Z}^m \to G$, which is just $(a_1, \cdots, a_m) \to g_1^{a_1} \cdots g_m^{a_m}$. This is a homomorphism only because G is abelian: Use the fact that $(g_1 g_2)^k = g_1^k g_2^k$. Otherwise the algebraic properties are not preserved.

Now we have a major theorem in algebraic geometry and algebraic topology when it is generalized:

Theorem 10.7. *With the above notation, Ker(ϕ) is also finitely generated.*

Proof. Let $N \leq \mathbb{Z}^m$ be generated by $(|g_1|, 0, \cdots, 0), (0, |g_2|, 0, \cdots, 0), \cdots, (0, \cdots, 0, |g_m|)$. Then $N \subseteq \text{Ker}(\phi)$ because $g_1^{|g_1|} g_2^0 \cdots g_m^0 = eee \cdots e = e$. Mod N, every element of $\mathbb{Z}^m$ has a representative in the finite set $(a_1, \cdots, a_m)$ where $0 \leq a_1 |g_1|, 0 \leq a_2 \leq |g_2|, \cdots, 0 \leq a_m \leq |g_m|$. Thus the order of $(a_1, \cdots, a_m)$ is $\leq |g_1| \cdots |g_m|$. Let K be the subset of Ker(ϕ) satisfying the previous given condition. Then K is finite and has cardinality $\leq \prod_{i=1}^m |g_i|$. Then $\text{Ker}(\phi) = \langle K, N \rangle$. Therefore, the kernel is finitely generated since the kernel is generated by two things which are finitely generated. □

Now we turn the group classification into a matrix problem. Write the elements of $N \cup K$ as columns of an $m \times n$ matrix A. Then ψ is a map from $\mathbb{Z}^n \to \mathbb{Z}^m$, and ϕ is a surjective map from $\mathbb{Z}^m \to G$ and Ker(ϕ) =image(ψ).

Example 10.8. A group G is generated by g_1, g_2 where g_1 has order 2, g_2 has order 4, and $g_1 g_2^2 = e$. What is G? Well $g_1 = g_2^{-2}$ and $g_1 = g_2^2$, so g_1 is not necessary as a generator: the whole group is generated by g_2. Since g_2 is of order 4, $G = \langle g_2 \rangle \cong \mathbb{Z}_4$. But how do we do this in general?

Theorem 10.9. *Smith Normal Form (SNF). Let A be an $m \times n$ matrix over $\mathbb{Z}$. Then we can write*

$$A = PDQ \tag{5}$$

where P is $m \times m$, $det(P) = \pm 1$, and both P and P^{-1} have entries in $\mathbb{Z}$ ($P \in GL_m(\mathbb{Z})$). Q is $n \times n$, $det(Q) = \pm 1$, Q, Q^{-1} both have $\mathbb{Z}$ entries, D is $m \times n$, is all 0s except on diagonal, where it has the values $d_{11}, d_{22}, \cdots$, $d_{ii} \in \mathbb{Z}, d_{ii} > 0$ and $d_{11}|d_{22}, d_{22}|d_{33}, \cdots, d_{(k-1)(k-1)}|d_{kk}$. $k \leq \min m, n$, if k is less, then $d_{(k+1)(k+1)}$ and onwards $= 0$.

Remark 10.10. We will construct P, Q as a product of 3 kinds of elementary matrices. Each elementary matrix has entries in $\mathbb{Z}$ and so does its inverse. The elementary matrices are permutation matrices, row switch matrices, and unit (± 1) scaling (diletation) matrices (i.e. the matrices used for Gaussian elimination).

10.1 SNF: The Algorithm

The input is $A, m \times n$. Initialize $P = I_m, D = A, Q = I_n$. We'll overwrite (not in Haskell) P, D, Q as we go along, preserving the invariant that $A = PDQ$. Whenever we do a step to P, we will do a step to D so that the product will be the same. For instance, we will be applying row operations R_i. We also allow multiplication by a matrix $\begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ for multiplying negative numbers. Then, if we modify $D \to R_1 D R_2$ (multiplying on the left corresponds to rows and on the right corresponds to columns), then $PDQ = (PR_1^{-1})(R_1 D R_2)(R_2^{-1} Q)$ and $P' = PR_1^{-1}, Q' = R_2^{-1} Q$.

1. Let $c = 1$, the active region is the (c, c) entry to the (m, n) entry (presume by induction that we have done everything from $d_{11}, \cdots, d_{(c-1)(c-1)}$ entries, and everything outside of this block is 0 already as desired) (c stands for "corner", in this case, upper left corner).

2. Look for the smallest entry in non-negative absolute value, permute rows/columns so that it goes to the d_{cc} position (the pivot).

3. Now, you basically do the Euclidean algorithm. Subtract multiples of row c off of the rows below to make column c into the Euclidean remainders mod d_{cc}. If all the remainders are 0, continue. If not, put the smallest remainder into d_{cc} (the absolute value is not zero) by a permutation, and redo this step again until all remainders are 0 (like the Euclidean algorithm). If every a value is negative, multiply by a scaling matrix so that the value is not negative.

4. Do the same thing as in step 3 except for the columns.

5. Now, we have d_{cc} in position (c, c) still and everything to the left and below in the same row and column as d_{cc} are all 0. We still have the remaining block. If d_{cc} has non-zero remainder when divided into by any a_{ij} in the remaining block, add row j to row c and go back to step 4. Keep doing this until all the remaining values are divisible by d_{cc}.

6. At this point, every remaining entry a_{ij} is a multiple of d_{cc}. Every $\mathbb{Z}$-linear operation on the remaining block will preserve this property. The next pivot that the region spits out will be divisible by d_{cc} necessarily, so now we can just increment c and return to step 2. We stop once the remaining block in step 6 is all 0. You will certainly stop since the matrix is finite.

Proof. Let $A = PDQ$ map from $\mathbb{Z}^n \to \mathbb{Z}^m$, and $\mathbb{Z}^m \to G$ is a surjective map. P is an isomorphism from $\mathbb{Z}^m \to \mathbb{Z}^m$ since P, P^{-1} are over $\mathbb{Z}$, and the same is true for Q over $\mathbb{Z}^n$. WLOG change coordinates by P in $\mathbb{Z}^m$ and by Q in $\mathbb{Z}^n$. Then we basically have D as a map from $\mathbb{Z}^n \to \mathbb{Z}^m$, which by our algorithm retains the property that $d_{ii} | d_{(i+1)(i+1)}$. So $G \cong \mathbb{Z}_{d_{11}} \oplus \mathbb{Z}_{d_{22}} \oplus \cdots \oplus \mathbb{Z}_{d_{kk}}$ by the way we are doing matrix multiplication by D. □

We could have also proved the result this way:

Theorem 10.11. *Primary Decomposition.*
A finite abelian group G is a $\oplus$ of cyclic groups of prime power orders.

Example 10.12. $\mathbb{Z}_6 \oplus \mathbb{Z}_{60} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$ by the Chinese Remainder Theorem.

The uniqueness of Smith Normal Form, by some more ring theory and determinants, you can get. For the Primary Decomposition, you get uniqueness (see Gallian's book) in Ch 11 Lemma 4.

Corollary 10.13. *Converse of Lagrange's Theorem.*
If m divides the order of a finite Abelian group, then there exists a subgroup of order m.

11 Representation Theory

One book that we will follow, since it is a classic, is Linear Representations of Finite Groups, by J.P. Serre.

We have been rotating shapes in vector spaces since the first day of class. Then, given any group and any vector space, how many ways are there to make the group act on it? It has to fit in the dimension of the space. Are there infinitely dimensional ways (what is their dimensional equivalent), are there finitely many ways, how can we classify them?

It is traditional to start over algebraically closed fields. Recall that $\mathbb{C}$ is an algebraically closed field, that is, any polynomial over $\mathbb{C}$ of degree n has n roots, counting multiplicities. The reason we want to begin over algebraically closed field is because we want the eigenvalues of the matrices (linear transformations) if the eigenvalues exist so we can diagonalize and so on (these are found by roots of characteristic polynomials).

Let V be a finite dimensional vector space over $\mathbb{C}$.

Definition 11.1. $GL(V)$ is the group of invertible linear transformations from $V \to V$. We can fix a basis $\{e_1, \cdots, e_n\}$ of V. Then linear transformations and matrices are effectively the same thing; we can define a one-to-one map. Thus, we can say that $GL(V) = GL_n(\mathbb{C})$, the $n \times n$ invertible matrices.

Definition 11.2. Let G be a finite group. A linear representation of G on V (or in V) is a homomorphism of groups

$$\rho : G \to GL(V) \tag{6}$$

Example 11.3. $\rho(e) = I_n$, $\rho(g) = \rho(g)^{-1}$, etc.

If $n = \dim(V)$, say ρ has dimension n, or ρ has degree n (interchangeable). Now we have a vector space and a group acting on it. Let's think about all the other things we can do with vector spaces, and see if we can extend the property of the group acting on it. We can call V a G-space, since G is acting on it. What's the right definition of how to extend a linear map in G?

Definition 11.4. Let $\rho : G \to GL(V)$ and $\rho' : G \to GL(V')$, where G is the same group and we have different vector spaces (for today). ρ will denote a linear representation. A **map of representations**, or a **G-map**, or an **intertwining operator** (all equivalent), is a linear map $\tau : V \to V'$ such that $\tau \circ \rho(g) = \rho'(g) \circ \tau$ for all $g \in G$.

The way to understand it is as follows: $V \to^{\rho(g)} V$, and $V' \to^{\rho'(g)} V'$. Then we have arrows from $V \to^{\tau} V'$, and we have a square. This is called a **commutative diagram**. You have to get the same result regardless of which of the two paths you take. You can get really large commutative diagrams in algebraic topology. However, all we will need is squares.

Definition 11.5. ρ, ρ' are isomorphic (or similar, equivalent) as representations if there is a G-map $\tau : V \to V'$ that is an isomorphism of vector spaces. For such τ, τ^{-1} is also a G-map.

Now let us give some examples of representations.

Example 11.6. The **trivial representation** is send $\rho : G \to GL_1(\mathbb{C})$, where $\rho(g) = 1$ for all g. This does not do anything.

Example 11.7. If ρ is any degree-1 representation, then $\rho : G \to GL_1(\mathbb{C}) = \mathbb{C}^*$, which means take the punctured complex plane $(\mathbb{C} - \{0\})$. Let G be cyclic of order d. Let g be a generator of G. Then $\rho(e) = \rho(g^0) = 1 \in \mathbb{C}^*$. Therefore, $1 = \rho(g^d) = \rho(g)^d$. Thus, $\rho(g)$ is a d^{th} root of unity. By de Moivre's Theorem, the d^{th} roots of unity in $\mathbb{C}^*$ are the d numbers $e^{2\pi ik/d}$ for $k = 0, \cdots, d-1$. So we have pretty much classified the representations of the cyclic group, since ρ must send the generator g to one of those roots of unity. Explicitly, choose any ζ from the d^{th} roots of unity; get a representation $\rho_\zeta : \langle g \rangle \to \mathbb{C}^*$, $g \to \zeta$. In general, $g^k \to \zeta^k$, for all $k = 0, \cdots, d-1$.

Lemma 11.8. *All d of the ρ_ζ are inequivalent.*

Proof. Assume $\rho_\zeta \cong \rho_{\zeta'}$, and assume the isomorphism is called τ. Then $\rho_\zeta(g^0) = 1, \rho_{\zeta'}(g^0) = 1$. The commutative square had to be valid for the same τ and all g. So $\tau : 1 \to 1$ and τ is multiplied by a scalar, since we are dealing with one-dimensional vector spaces. So τ is the identity, since the only scale you can multiply 1 by to get 1 is 1. So $\rho_\zeta(g) = \zeta$, and $\rho_{\zeta'}(g) = \zeta'$, so $\tau(\zeta) = \zeta'$, and they were equal after all. □

Definition 11.9. The d d^{th} roots of unity are a subgroup of $\mathbb{C}^*$ of cyclic order d. You can also show that ρs are themselves an abelian group under multiplication, and you get $\rho_\zeta * \rho_{\zeta'} = \rho_{\zeta\zeta'}$. This group is called the dual of G, $\hat{G}$. $G, \hat{G}$ are both cyclic of order d, and you can make a table that makes them look like the same group!

Table 3: $G \cong \hat{G}$

$g^0 = e$	ρ_1 (trivial representation)
g	ρ_w (let $w = e^{2\pi i/d}$)
g^2	ρ_{w^2}
$\vdots$	$\vdots$
g^{d-1}	$\rho_{w^{d-1}}$

However, the isomorphism $G \cong \hat{G}$ is not **canonical**: This means that the isomorphism depends on the particular generators g, w. The correspondance is really a **dual-pairing**, not directly an isomorphism. $\rho_{\omega^l}(g^k) = \omega^{kl}$. Say for example $d = p$, an odd prime. Replace g by another generator $h = g^2$. The natural way to keep the pairing the same is compute 2^{-1} mod p and let $\psi = \omega^{2^{-1}}$. Then $\rho_{\psi^l}(h^k) = \omega^{(2k)(2^{-1}l)} = \omega^{kl}$, since $h^k = g^{2k}, \psi^l = \omega^{2^{-1}l}$. Since we have to have this ψ, which can get complicated, this is not "simple" and therefore not canonical.

The standard example which will work on the next problem set is as follows: Although $G \cong \hat{G}$ is non-canonical, you can take the dual of the dual $\hat{G} \cong \hat{\hat{G}}$ and get a canonical isomorphism from $G \cong \hat{\hat{G}}$.

We can relate the idea of the dual back to linear algebra. In linear algebra, the dual space V^* of a vector space V over a field F is the annihilator functionals which applied to any element of V map it to 0. Similarly, we can consider V^{**}, the double-dual. Again, $V \cong V^{**}$ canonically, but $V \cong V^*$ is not canonical. In practical terms, we can think of the members of V as column vectors, the members of V^* as row vectors who have a dot product of zero with the members of V (orthogonal space), and the members of V^{**} as column vectors again. Thus, the $V \to V^{**}$ map is canonical because it's an identity map. For instance, in the case where V is three-dimensional, $(x, y, z) \to (x, y, z)^T$ is not canonical. Consider that (x, y, z) must act on any subspace of V, for instance denoted by some matrix A^{-1}. then $(x, y, z)A^{-1}A(x, y, z)^T = 0$, but we must include the A, A^{-1} in here. Then, $((x, y, z)A^{-1})^T = (A^{-1})^T(x, y, z)$, which means in our isomorphism we must map by $(A^{-1})^T$, which may not be trivial, and thus the mapping is not canonical.

Example 11.10. If $f : G \to H$ is any homomorphism of groups, and $\rho : H \to GL(V)$ is a representation, then $\rho \circ f$ is a representation of G on V. This is especially useful if $N \trianglelefteq G$, $G \to G/N \to GL(V)$. For instance, S_n/A_n is cyclic of order 2, generated by g. There are two reps of $\langle g \rangle$ on degree 1.

Table 4: $G \cong \hat{G}$

.	e	g
ρ_1	1	1
ρ_{-1}	1	-1

Pulling these back through $S_n \to S_n/A_n \to \{\pm 1\}$ gives the trivial representation of S_n, and the sign representation, $sgn : S_n \to \{\pm 1\} \subseteq \mathbb{C}^*$ by $sgn(\text{even perm}) \to 1, sgn(\text{odd perm}) \to$

-1.

We can also consider $G = A_4$. Recall $V = \{e, (12)(34), (13)(24), (14)(23)\}$, which is isomorphic to the Klein-4 group, and is normal in A_4. Here A_4/V is cyclic of order 3, and we will get three representations. The trivial representation, $\rho_\omega, \rho_{\omega^2}$ which all map to $\mathbb{C}^*$. How will we see these as representations of A_4. Then, take each face of a tetrahedron, and divide each face into three section. Color each of these a separate color; black, white and red. Then ρ_ω is: Pick a face called the front face, act on the tetrahedron by $g \in A_4$; if g sent (B W R) to (B W R), $\rho_w(g) = 1$ - nothing changes about the colors. If it's (B W R) to (B R W), $\rho_\omega(g) = \omega$. If its (B W R) to (R W B), then $\rho_\omega(g) = \omega^2$.

Example 11.11. Rotations and reflections of bodies in $\mathbb{R}^n$ (or $\mathbb{C}^n$) give representations. For instance, rotations of the tetrahedron are a representation of A_4 on $\mathbb{R}^3$. Often you can embed $\mathbb{R}^3 \to \mathbb{C}^3$ by sending a real basis vector to the same basis vector (complex values 0) in $\mathbb{C}^3$.

Theorem 11.12. *Any representation of A_4 is a $\oplus$ (direct sum) of copies of the three degree-1 representations we've seen, and the degree-3 representation from the tetrahedron.*

Definition 11.13. $\rho : G \to GL(V)$. Let $W \subseteq V$ be a subspace. Say W is **stable** (or invariant) under the representation if $\rho(g) \cdot W = W$ for all $g \in G$.

Definition 11.14. ρ is **irreducible** if it has no stable subspaces besides V and $\{0\}$.

Example 11.15. Let $G = A_4$. Let $\mathbb{C}^4$ have basis $e_1, \cdots, e_4$. Let $g \in A_4$ act by $\rho(g) : e_i \to e_{g_i}$ for $i = 1, 2, 3, 4$. Then, let $g = (123)$ is the following matrix, which acts on columns:

$$\begin{bmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

which is a **permutation representation**. The vector $[1111]^T$ is stable: $\rho(g) \cdot \{\alpha * [1111]^T : \alpha \in \mathbb{C}\} = \{\alpha * [1111]^T : \alpha \in \mathbb{C}\}$ for all g. In other words, the line $W = \mathbb{C} \cdot [1111]^T$ is stable, which also works in $\mathbb{R}^4$. In $\mathbb{R}^4$, in which we have a standard dot product. All $\rho(g)$ matrices are orthogonal and preserves the standard dot product (this is very clear for permutation matrices as its columns are orthonormal). The perpendicular complement $W^\perp$ of W must also be stable. Abstractly speaking, $W^\perp \cong \mathbb{R}^3$. By symmetry, all four axes $\mathbb{R} \cdot e_1, \cdots, \mathbb{R} \cdot e_4$ must orthogonally project to $W^\perp$ and $\binom{4}{2}$ pairs must project to the same angle. Well, this is literally the tetrahedron: We have four lines which have that all $\binom{4}{2}$ pairs have the same angles! ≈ 109.... The origin is at the center of the tetrahedron, and the 4 lines are through the centers of each of the faces. So $W^\perp$ is **equivalent** to the tetrahedral rotation representation.

11.1 Constructing Representations

Let V be a vector space over $\mathbb{C}$, with basis $e_1, \cdots e_n$ and W be a vector space over $\mathbb{C}$ with basis $f_1, \cdots f_m$. G is a finite group, and $\rho : G \to GL(V)$ and $\rho' : G \to GL(W)$ are representations.

Definition 11.16. Direct Sum.

$$V \oplus W = \{(v, w) : v \in V, w \in W\} \tag{7}$$

In terms of representations, we have

$$(\rho \oplus \rho')(g) : (v, w) \to (\rho(g) \cdot v, \rho'(g) \cdot w) \tag{8}$$

We can write this in terms of matrices as

$$\left[\begin{array}{c|c} \rho(g) & 0 \\ \hline 0 & \rho'(g) \end{array}\right] \cdot \begin{bmatrix} v \\ w \end{bmatrix}$$

11.1.1 Tensor Product

Definition 11.17. The tensor product $V \otimes W$ is an nm dimensional vector space with basis $e_i \otimes f_j$. The product must be bilinear: $(a_1 e_1 + \cdots + a_n e_n) \otimes (b_1 f_1 + \cdots + b_n f_n) = \sum_{i=1,\cdots,n;j=1,\cdots,m} (a_i b_j) e_i \otimes f_j$. In matrix language, we can represent the tensor product of two vectors in $\mathbb{R}^n, \mathbb{R}^m$ as a matrix in $\mathbb{R}^{m \times n}$:

$$\begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix} \cdot \begin{bmatrix} b_1 & b_2 & \cdots b_m \end{bmatrix} = \begin{bmatrix} a_1 b_1 & a_1 b_2 & \cdots & a_1 b_m \\ \vdots & \vdots & \vdots & \vdots \\ a_n b_1 & a_n b_2 & \cdots & a_n b_m \end{bmatrix}$$

The representations act by

$$\rho(g) \cdot \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix} \cdot \begin{bmatrix} b_1 & b_2 & \cdots b_m \end{bmatrix} \rho'(g)^T$$

which defines

$$(\rho \otimes \rho')(g) : v \otimes w \to (\rho(g)v) \otimes (\rho'(g)w) \tag{9}$$

11.2 Dual Space

Definition 11.18. V^* is the space of linear functions $f : V \to \mathbb{C}$. This is a vector space: $f + g$ is linear, cf is linear. Write coordinates on V as a column vector $[a_1 \cdots a_n]^T$; then, a linear map is $c_1 a_1 + \cdots + c_n a_n$. In other words, coordinates of V^* are rows.

We want to define a representation ρ^* on V^* so that the pairings are preserved. If $\rho(g) = A$, a matrix, then the representation is $A[a_1, \cdots, a_n]^T$. Then, the way to preserve the mapping $(c_1, \cdots, c_n)$ is to multiply it on the right by A^{-1}. ρ^* acts on rows by $\rho(g)^{-1}$ on the right. This is another illustration of what non-canonical means. If you act on one of them by A, you have to act by the inverse on the other.

If you want to treat both V and V^* as columns, then $\rho^*(g) = (\rho(g)^{-1})^T$. So you need both the -1 and the transpose to make ρ^* a homomorphism:

$$\begin{aligned} \rho^*(gh) &= \big(\rho(gh)^{-1}\big)^T \\ &= \big(\rho(h)^{-1}\rho(g)^{-1}\big)^T \\ &= (\rho(g)^{-1})^T(\rho(h)^{-1})^T \end{aligned} \tag{10}$$

Then we define $\mathrm{Hom}(V, W)$ which is the space of all linear maps $V \to W$ which is isomorphic to the space of all $m \times n$ matrices over $\mathbb{C}$.

Definition 11.19. $\mathrm{Hom}(V, W) \cong V^* \otimes W$, canonically, where $\otimes$ is tensor product.

Proof. The i^{th} row of a matrix is an element of V^*, and $(i^{th}\text{ row}) \cdot [a_1, \cdots, a_n]^T = c_i$. For the other direction, the map sends $a_1v_1 + \cdots a_nv_n$ to $c_1f_1 + c_2f_2 + \cdots + c_nf_n$. For each element $(f_1, \cdots, f_m)$ of a basis of W, we've chosen an element of V^*: $\sum_{i=1}^{m}(V^*)_i \otimes f_i \in V^* \otimes W$. □

Therefore, ρ and ρ' give a representation on $\mathrm{Hom}(V, W)$ as follows: For $\phi \in \mathrm{Hom}(V, W)$, send it to $W \leftarrow^{\rho'(g)} W \leftarrow^{\rho} V \leftarrow^{\rho(g)^{-1}} V$. That is, $\phi \to \rho'(g) \circ \phi \circ \rho(g)^{-1}$.

Definition 11.20. For any representation V of G, V^G denotes the invariant subspace of G, i.e. $\{v \in V : \rho(g) \cdot v = v, \forall g \in G\}$. Recall that a $G-$map, or intertwining operator, is $\tau : V \to W$ such that $V \to^{\rho(g)} V$ and $W \to^{\rho'(g)} W$, and $V \to^{\tau} W$. Then, $\mathrm{Hom}_G(V, W)$ is the space of G-maps.

Theorem 11.21. *$\mathrm{Hom}_G(V, W) \cong \mathrm{Hom}(V, W)^G$, canonically.*

Proof. Let $\tau \in \mathrm{Hom}(V, W)$ and let it be invariant under the action of G on $\mathrm{Hom}(V, W)$. Then, $V \to^{\rho(g)^{-1}} V$ and $W \to^{\rho'(g)} W$, and $V \to^{\tau} W$. This is basically the same diagram as the definition of G-map, since $\rho(g)$ is an isomorphism, we can just switch the direction of the arrow and change inverse to not an inverse. □

11.3 Irreducible Representations

There are two notions of "smallest possible representation".

1. **irreducible**: A space $W \subseteq V$ is stable under ρ if $\rho(g) \cdot W \subseteq W$ for all $g \in G$. V is irreducible if it has no stable subspaces besides $\{0\}$ and itself.

2. **indecomposable**: V is decomposable if $V \cong V_1 \oplus V_2$ where $\dim(V_1) > 0$, $\dim(V_2) > 0$. So, $\rho \cong \rho_1 \oplus \rho_2$.

In many areas of math, these are not the same notion, and irreducible is finer than indecomposable.

Example 11.22. $G = (\mathbb{R}, +, 0)$ (not finite). Then we have a representation $\rho : G \to GL_2(\mathbb{R})$ and $a \to \left[\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right]$, which is a horizontal shear. Here, the x-axis is stable for the ρ. No other subspace is stable! Thus we cannot decompose as $V_1 \oplus V_2$ since there is no stable V_2 where V_1 is the x-axis. The x-axis is one dimensional and is therefore irreducible (only other subspace must be the subspace $\{0\}$).

Definition 11.23. A group is simple if it has no normal subgroups besides itself and the trivial subgroup.

Simple groups are like prime numbers, since you can't quotient it out anymore. Simple is more like irreducible than decomposable. For instance, $\mathbb{Z}_4$ is not decomposable since $\mathbb{Z}_4 \ncong \mathbb{Z}_2 \oplus \mathbb{Z}_2$. However, $0 \lhd 2\mathbb{Z}_2 \lhd \mathbb{Z}_4$, and thus $2\mathbb{Z}_2$ is irreducible.

Now, recall that

Definition 11.24. A Hermitian inner product is a pairing $V \times V \to \mathbb{C}$ denoted $\langle v|w\rangle$ (as in quantum mechanics) (a braket). This is linear in v: $\langle v_1 + v_2|w\rangle = \langle v_1|w\rangle + \langle v_2|w\rangle$. Also, $\langle cv|w\rangle = c\langle v|w\rangle$. It's only semilinear in w: $\langle v|w_1+w_2\rangle = \langle v|w_1\rangle+\langle v|w_2\rangle$, but $\langle v|cw\rangle = \overline{c}\langle v|w\rangle$, where $\overline{c}$ is the complex conjugate. Finally, the operation is positive definite: $\langle v|v\rangle > 0$ for all $v \in V$, $v \neq 0$.

Example 11.25. If $v = [z_1 \cdots z_n]^T$ in coordinates on $\{e_i\}$, $w = [w_1, \cdots, w_n]^T$. The standard product is just $z_1\overline{w}_1 + \cdots z_n\overline{w}_n$. This is positive definite since $\langle v|v\rangle = z_1\overline{z}_1 + \cdots + z_n\overline{z}_n = |z_1|^2 + \cdots + |z_n|^2 > 0$ unless all $z_i = 0$.

Theorem 11.26. *Weyl's Unitary Trick.*
There exists a Hermitian inner product on V which is invariant under ρ, i.e. $\langle v|w\rangle = \langle \rho(g) \cdot v|\rho(g) \cdot w\rangle$ for all $g \in G$.

Proof. Let $[\cdots|\cdots]$ be any Hermitian inner product on V, e.g. the standard one. Let $\langle\cdots|\cdots\rangle$ be the average

$$\langle v|w\rangle = \frac{1}{|G|}\sum_{g\in G}[\rho(g) \cdot v|\rho(g) \cdot w] \tag{11}$$

First, $\langle\cdots|\cdots\rangle$ is invariant. For all $h \in G$, $\langle \rho(h) \cdot v|\rho(h) \cdot w\rangle = \frac{1}{|G|}\sum_{g\in G}[\rho(gh) \cdot v|\rho(gh) \cdot w]$ but $g \to gh$ is a permutation of G. So all we did was permute the average, but that doesn't change the average since you just add it up and divide. So it's invariant. It's also still an inner product: linear on the left because sums are linear. It's also semilinear in w again because of the sums. It's also still positive definite: If you take the average of a bunch of positive numbers, it is still positive. Note that G must be finite; otherwise our algebra would not work out (you might get infinity when you sum). □

Corollary 11.27. *Any linear representation of the finite group G over $\mathbb{C}$ is a $\oplus$ of irreducible representations.*

Proof. If $W \subseteq V$ is a stable subspace under ρ, then $W^\perp$ (defined using the invariant $\langle\cdots|\cdots\rangle$) is also stable. Proceed by induction on decreasing dimension. If W is irreducible, stop. If not, find a stable $W_1 \subset W$ and then W will split as $W_1 \oplus W_1^\perp$. If either is not irreducible, split further. If either is irreducible, you are done with that side. □

Definition 11.28. Any mathematical theory is **completely reducible** if all indecomposables are irreducibles.

We have just proved that linear representations over $\mathbb{C}$ is a completely reducible theorem.

11.4 Characters and Character Tables

11.4.1 Preliminaries

Throughout, G is a finite group, V, W are vector spaces over $\mathbb{C}$, $\rho : G \to GL(V)$, $\dim(V) = n$, $\rho' : G \to GL(W)$, $\dim(W) = m$, and a G-map τ takes $V \to W$ in the commutative diagram sense (for all $g \in G$, $V \to^{\rho(g)} V$ and $W \to^{\rho'(g)} W$.

Lemma 11.29. *The kernel and image of a G-map are G-stable.*

Proof. For kernel, we suppose $\tau(v) = 0$. Then for all g, $\tau(\rho(g) \cdot v) = \rho'(g)\tau(v) = \rho'(g) \cdot 0 = 0$. Thus, $\rho(g) \cdot v \in \mathrm{Ker}(\tau)$, as desired, for all $v \in \mathrm{Ker}(\tau)$. Also $\mathrm{Ker}(\tau) \subseteq \{\rho(g) \cdot v : \tau(v) = 0\}$ since choosing $g = e$ gives $\rho(e) \cdot v = v$. Thus $\mathrm{Ker}(\tau) = \{\rho(g) \cdot v : \tau(v) = 0\}$ for all $g \in G$.

For the image, let $\tau(v) = w$, where $v \in V$ and $w \in W$. Then for all g, $\tau(\rho(g) \cdot v) = \rho'(g)\tau(v) = \rho'(g)w \in W$ for all $g \in G$, since $\rho'(g) \in W$ and $w \in W$. Then, since $\rho'(e)$ is identity in W, we have $W \subseteq \{\rho'(g)w : w \in W\} = \{\tau(\rho(g) \cdot v) : v \in V\}$. Thus, $W = \{\tau(\rho(g) \cdot v) : v \in V\}$, and is stable with respect to the representation of G. □

Lemma 11.30. *Schur's Lemma.*
This is the biggest bang for your buck you can get, since the proof is simple but has a lot of consequences. You can use this in representing things in Hilbert spaces as well. Let V, W be irreducible representations of G. Let $\tau : V \to W$ be a G-map. Then

1. *Either $V \cong W$ or $\tau = 0$.*

2. *If $V = W$, then $\exists \lambda \in \mathbb{C}$ s.t. $\tau = \lambda \cdot I$ (scalar multiple of the identity matrix).*

This is taking first take two irreducible representations, and τ is trying to intertwine. If the representations are different, you can't have a τ that reconciles them. However, if they are congruent, then there is a way to intertwine them, but the only way is to multiply them by a scalar, and this commutes with anything. Only the easiest possible way to intertwine them will ever work.

Proof. $\mathrm{Ker}(\tau)$ is a G-stable subspace of V. Irreducible means that $\mathrm{Ker}(\tau) = V$ or $\{0\}$. If the kernel is V, then everyone dies! and goes to zero. So you're done. If the kernel is 0, then only 0 goes to 0 and τ is injective. $\mathrm{Im}(\tau)$ is G-stable, and W is irreducible. Therefore, $\mathrm{Im}(\tau) = \{0\}$ or W. If the image is 0, then $\tau = 0$ and we're done. Else, τ is surjective. Therefore, either τ is 0 or it is bijective, and hence has an inverse function τ^{-1}. We claim that τ^{-1} is an isomorphism of representations. In other words, we want to prove τ^{-1} intertwines. We can say $\tau^{-1} : W \to V$. τ^{-1} intertwines iff $\rho(g) \circ \tau^{-1} = \tau^{-1} \circ \rho(g)$, iff $\rho(g) = \tau^{-1} \circ \rho'(g) \circ \tau$, iff $\tau \circ \rho(g) = \rho'(g) \circ \tau$, which is given (definition of commutative diagrams).

Now we prove the second statement. If $\tau : V \to V$ and is 0, then we're done and $\lambda = 0$. If not, then there is at least one eigenvalue λ and one non-zero eigenvector, $\tau(v) = \lambda v$. Note that here we need $\mathbb{C}$ is algebraically closed. There's two assumptions we made about the field: First that there are no mod p components, and secondly algebraic closure. You can do it over the other fields later, but first you have to do it over $\mathbb{C}$ to learn what the patterns are, and then you can extend them. Now, λI is certainly intertwining, since scalars commute. Differences of intertwining operators are also intertwining, so $\tau - \lambda I$ is intertwining. But $(\tau - \lambda I)(v) = \tau(v) - \lambda v = \lambda v - \lambda v = 0$. So $\mathrm{Ker}(\tau - \lambda I) \neq \{0\}$, but it's also G-stable and irreducible. It's not 0, therefore the kernel is the whole thing, i.e. V. Thus $\tau - \lambda I = 0$ and $\tau = \lambda I$. Note that $\{\lambda I | \lambda \in \mathbb{C}\}$ is a one dimensional vector space. □

11.4.2 Characters

This theory is in large part due to Frobenius, in the late 1800s. Frobenius saw the importance of the trace operator. Let's recall some facts about trace. If vector space V has a basis $\{e_i\}$, then you can write each $\rho(g)$ as a matrix A.

Definition 11.31. Trace.
Trace$(A) = \sum_{i=1}^{n} A_{ii}$. If you change the basis, well we have $A \to SAS^{-1}$, where S is invertible and in $GL_n(\mathbb{C})$. Then Trace(A) =Trace(SAS^{-1}). This eventually gives you that the characteristic polynomial, which by definition is $\det(\rho(g) - \lambda I)$, where λ is some variable. Then this is $\lambda^n - (\text{Trace}(\rho(g)))\lambda^{n-1} + \cdots + (-1)^n \det(\rho(g))$. Thus it's easy to see that the characteristic polynomial is invariant under conjugation by S. (Also, if you prove/recall the circular property of trace, we simply have Trace(SAS^{-1}) = Trace$(AS^{-1}S)$ = Trace(A)). As another side note, the terms we left out in the characteristic polynomial expansion are interesting in algebraic geometry. Anyways, we can rewrite the characteristic polynomial as $(\lambda - r_1)\cdots(\lambda - r_n)$, where the r_i are roots of the polynomial. This equals $\lambda^n - (r_1 + \cdots + r_n)\lambda^{n-1} + \cdots + (-1)^n(r_1 \cdots r_n)$. A corollary is that Trace$(\rho(g)) = \lambda_1 + \cdots + \lambda_n$, where λ_i are the eigenvalues of $\rho(g)$, counted with multiplicities (This can be easily seen by calculating the the trace of $A^T A$ using the SVD decomposition, and noting that the squares of singular values are eigenvalues).

Definition 11.32. The **character** of ρ is $\chi(g) =$ Trace$(\rho(g))$, for all $g \in G$. It's denoted χ_ρ, χ_V. The properties are

1. $\chi(e) = n$. This is the dimension of the representation, and is clear from the fact that the identity matrix has n ones on the diagonal.

2. $\chi(hgh^{-1}) = \chi(g)$ for all $h \in G$. $\rho(hgh^{-1}) = \rho(h) \cdot \rho(g) \cdot \rho(h)^{-1}$. Thus Trace$(LHS)$ =Trace$(\rho(g))$, since conjugation by $S = \rho(h)$ does not change the trace.

3. $\chi(g^{-1}) = \overline{\chi(g)}$. If λ_j is an eigenvalue of $\rho(g)$, then $\frac{1}{\lambda_j}$ is an eigenvalue of $\rho(g^{-1})$. Now, $\chi(g) = \lambda_1 + \cdots + \lambda_n$. Therefore, $\chi(g^{-1}) = \frac{1}{\lambda_1} + \cdots + \frac{1}{\lambda_n}$. This looks kind of ugly. However, since G is finite, g has finite order d. Therefore $g^d = e$. That means that $\lambda_j^d = 1$. Since we are over the complex numbers, all eigenvalues are d^{th} roots of unity, and in particular, $\frac{1}{z} = \overline{z}$, and thus $\frac{1}{\lambda_j} = \overline{\lambda}_j$. Thus $\chi(g^{-1}) = \overline{\lambda}_1 + \cdots + \overline{\lambda}_n = \overline{\lambda_1 + \cdots + \lambda_n} = \overline{\chi(g)}$.

Definition 11.33. A **class function** on G is a function that takes a constant value on each conjugacy class.

Corollary 11.34. *Characters are class functions. This follows from property* 2 *of characters, since conjugation doesn't do anything to the value of a character.*

Now we give some properties about how characters act when we combine vector spaces.

Lemma 11.35. $\chi_{V \oplus W} = \chi_V + \chi_W$.

Proof. The representation of the direct sum space is just

$$\left[\begin{array}{c|c} \rho(g) & 0 \\ \hline 0 & \rho'(g) \end{array}\right]$$

which is clearly maintaining the trace along each, and summing traces is obvious. □

Lemma 11.36. $\chi_{V^*} = \overline{\chi}_V$

Proof. ρ^* acts on V^* as $\rho(g^{-1})^T$, and from property 3 we have $\chi(g^{-1}) = \overline{\chi(g)}$. The transpose doesn't change the trace, so we are done. □

Lemma 11.37. $\chi_{V\otimes W} = \chi_V \cdot \chi_W$.

Proof. We saw before that there exists a G-invariant Hermitian inner product $\langle\cdot,\cdot\rangle$ on V. You can change coordinates so that $\langle\cdot,\cdot\rangle$ becomes the standard Hermitian inner product (dot product over complex numbers, the only difference is you conjugate the second term). Then all $\rho(g)$ are **unitary**, which just means that $\rho(g^{-1}) = \overline{\rho(g)}^T$. These are like orthogonal matrices in complex numbers. We're basically saying everything can be done as rotations or reflections. Unitary matrices are also diagonalizable. That means you can choose an eigenbasis for this particular g $v_1, \cdots, v_n$ of V so that $\rho(g)\cdot v_i \to \lambda_i v_i$ for $i = 1, \cdots, n$. Do the same for W, and then we get $\rho(g) : w_j \to \mu_j w_j$ for $j = 1, \cdots, m$. Then the basis for the tensor product $V \otimes W$ is just $v_i \otimes w_j$, $i = 1, \cdots, n; j = 1, \cdots, m$, and thus $\dim(V \otimes W) = nm$. $\rho(g)$ acts by $v_i \otimes w_j \to \lambda_i\mu_j(v_i \otimes w_j)$. Then as a matrix in lexicographic order (order by i, then by j, for $\lambda_i\mu_j$), we have that this action has an $nm \times nm$ matrix whose diagonal entries are $\lambda_1\mu_1, \cdots, \lambda_1\mu_m, \lambda_2\mu_1, \cdots, \cdots, \lambda_n\mu_m$, and thus the trace is $\sum_{i=1}^n \sum_{j=1}^m \lambda_i\mu_j = (\lambda_1 + \cdots + \lambda_n)(\mu_1 + \cdots + \mu_n) = \chi_V(g)\cdot\chi_W(g)$. □

Remark 11.38. Note that we have $\chi_{Hom(V,W)} = \chi_{V^*\otimes W} = \chi_{V^*}\cdot\chi_W = \overline{\chi}_V \cdot \chi_W$.

11.4.3 Projections

Definition 11.39. Let A be any vector space and B be any subspace. A **projection** onto B is a linear map from $\phi : A \to B$ such that

1. $\text{Im}(\phi) = B$

2. $\phi^2 = \phi$. A general projection map from $\mathbb{R}^3 \to \mathbb{R}^2$ means to slide down some parallel lines (for instance, rays of the sun) onto a table. Intuitively, a point in the table won't move. Projection onto a table entails not moving points on the table, but moving other points to the table. $\phi^2 = \phi$ comes in as follows: If you do ϕ again, well, nothing will change! Since you already projected everything onto the tabletop! $\text{Ker}(\phi)$ is the subspace you project along. $A = \text{Ker}(\phi) \oplus \text{Im}(\phi)$. In the sun analogy, $\text{Im}(\phi)$ is the tabletop and $\text{Ker}(\phi)$ is the rays from the sun which go through the origin.

Now let V be any representation such that $V \cong V_1^{\oplus k_1} \oplus V_2^{\oplus k_2} \oplus \cdots \oplus V_i$ which are are the irreducible representations of G. WLOG V_1 is the trivial representation of G (where everything maps to 0). Note that V^G, the invariants under ρ, $= V_1^{\oplus k_1}$, by Schur's Lemma (or, if anything were fixed in there, then it must stay stable, but everything else is moving). Can we get a formula for projecting onto the trivial part?

Theorem 11.40. *First Projection Formula.*
The map $\phi : \frac{1}{|G|}\sum_{g\in G}\rho(g)$, which is the average of all representation maps on V, is a projection onto V^G.

Proof. First we prove that $\text{Im}(\phi) \subseteq V^G$. Let $v \in V$. For any $h \in G$, we claim that $\rho(h)\cdot\phi(v) = \phi(v)$. This holds because multiplying all the $g \in G$ by h just permutes the sum! So the average does not change. Specifically, $\rho(h)\cdot\phi(v) = \frac{1}{|G|}\sum_{g\in G}\rho(hg)\cdot v$. Now we show that $V^G \subseteq\text{Im}(\phi)$. Let $v \in V^G$. Then $\phi(v) = \frac{1}{|G|}\sum_g \rho(g)\cdot v = \frac{1}{|G|}\sum_g v = \frac{1}{|G|}|G|v = v$, since $\rho(g)$ fixes $v \in V^G$ by definition. Thus ϕ also fixes v for v in the space we are projecting onto, a necessary property for projections. Note that if the field were $\mathbb{Z}_p$, and if $p||G|$, then you couldn't do this since this whole averaging formula is dividing by 0! As a side note, representation theory can be done $\mod p$, and is called modular representation theory and is harder, but you can't do it the way we're doing it here. After you fix a group, only finitely many paramters divide its order; these are the "annoying primes".

Now we want to prove that $\phi^2 = \phi$. This is just fun with combinatorics. We have $\phi^2(v) = \frac{1}{|G|}\sum_{h\in G}\rho(h)\left(\frac{1}{|G|}\sum_{g\in G}\rho(g)\cdot v\right) = \frac{1}{|G|^2}\sum_{(h,g)\in G\times G}\rho(hg)\cdot v$. Then let $t \in G$ where $hg = t$. Now we can write $\frac{1}{|G|^2}\sum_{t\in G}\sum_{g\in G}\rho(t)\cdot v$ where you have that $h = tg^{-1}$. Then, this equals $\frac{1}{|G|^2}\sum_{t\in G}|G|\cdot\rho(t)\cdot v = \frac{1}{|G|}\sum_{t\in G}\rho(t)\cdot v = \phi(v)$, and we are done. □

Remark 11.41. ϕ is a projection. Trace$(\phi) = \dim(V^G)$. For any projection of A onto B, take a basis in B, and extend to basis of A along Ker(ϕ). Then we can write $\phi = \left[\begin{smallmatrix} I & 0\end{smallmatrix}\right]$. Thus, Trace$(\phi) = \dim(B)$.

Now everything comes together. Now let V, W be two irreducible representations of G. By Schur's Lemma, $\dim(\mathrm{Hom}_G(V,W)) = 1$ if $V \cong W$, and 0 otherwise. Then, $\dim(\mathrm{Hom}_G(V,W)) = \dim(\mathrm{Hom}(V,W)^G)$. This is equal to the trace of the projection $\phi = \frac{1}{|G|}\sum_{g\in G}\rho(g)$ onto $\mathrm{Hom}(V,W)^G$, where ρ are representations on $\mathrm{Hom}(V,W)$ by the previous theorem. The trace of ϕ is the average of Trace$(\rho(g))$ over G, and thus the average of the characters: Trace$(\phi) = \frac{1}{|G|}\sum_g \chi_\rho(g)$, which can be written as $\frac{1}{|G|}\sum_{g\in G}\chi_{\mathrm{Hom}(V,W)}(g)$. Recalling that $\mathrm{Hom}(V,W) \cong V^* \otimes W$, this expression equals $\frac{1}{|G|}\sum_{g\in G}\chi_{V^*\otimes W}(g) = \frac{1}{|G|}\sum_{g\in G}\overline{\chi_V(g)}\cdot\chi_W(g)$. Let's write it all out, letting ϕ be the projection onto $\mathrm{Hom}(V,W)^G$:

$$\begin{aligned}1 \text{ or } 0 = \dim\left(\mathrm{Hom}_G(V,W)\right) &= \dim\left(\mathrm{Hom}(V,W)^G\right) = \mathrm{Trace}(\phi)\\ &= \frac{1}{|G|}\sum_{g\in G}\chi(g) = \frac{1}{|G|}\sum_{g\in G}\overline{\chi_V(g)}\cdot\chi_W(g)\end{aligned} \tag{12}$$

where the value is 1 if $V \cong W$ and 0 otherwise. Thus, we have the Main Theorem.

Theorem 11.42. *The characters of the representations of G carry a Hermitian inner product*

$$\langle\theta,\psi\rangle = \frac{1}{|G|}\sum_{g\in G}\overline{\theta(g)}\cdot\psi(g) \tag{13}$$

*The characters of irreducible representations are an **orthonormal set**. So you get an orthonormal basis!*

Thus, each representation of finite group G can be expressed as a vector of dimension $|G|$ of the characters of the elements of G. Since characters are class functions, we can express this vector in shorthand by writing down only the values of the characters for each conjugacy class, and writing the number of elements in the conjugacy class in parentheses. Note that if we did not write down the characters in this compact form, the character matrix of dimensions (# representations) $\times|G|$ would have redundant columns. Another interesting fact is that the number of conjugacy classes is equivalent to the number of irreducible representations and this number is also the dimension of the character table matrix (expressed in the compact form).

In terms of this language, the previous theorem simply states that under the defined Hermitian inner product, these character vectors of irreducible representations are orthonormal. Since direct sums of irreducible representations define any linear representation of the finite group G, the character vectors of irreducible representations give an orthonormal basis for linear representations.

11.4.4 Character Table of S_3

The columns are the conjugacy classes of S_3. There is only one e, 3 conjugates for (12), and 2 conjugates in the conjugacy class of (123). Well, we must have that the number of the conjugacy classes equals the dimension of the character-space. There is a trivial representation (the first row), the sign representation (second row), and the standard representation, which is the representation on the triangle. Well the identity has trace 2 since we are dealing with I_2, and this is the dimension of the space we're acting on. Then note that a flip has matrix $\left[\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right]$, so the trace is 0. Finally, rotation is $\begin{bmatrix} \cos(120) & -\sin(120) \\ \sin(120) & \cos(120) \end{bmatrix}$. The trace of this is just Trace($\begin{bmatrix} -1/2 & -\sqrt{3}/2 \\ \sqrt{3}/2 & -1/2 \end{bmatrix}$) $= -1$.

Table 5: Character Table of S_3

.	e	(..)	(...)
trivial	1	1	1
sign	1	-1	1
standard	2	0	-1