Algebra Notes

Nikhil R.

Contents

1 Groups

1.1 Laws of Composition

Definition. A **law of composition** on a set S is a function $S \times S \to S$. We usually denote the element obtained using multiplication, addition, or no symbol: $p = a \circ b = a + b = ab$.

- The law is **commutative** if $\forall\ a, b \in S$, $ab = ba$.
- The law is **associative** if $\forall\ a, b, c \in S$, $(ab)c = a(bc)$.
- If $\exists\ e$ s.t. $ea = ae = a$ $(\forall\ a \in S)$ then e is called an **identity** (unique).
- An element a of S is **invertible** if $\exists b \in S$ s.t. $ab = ba = e$ (identity).

Example. Composing two functions is associative but not commutative.

Proposition. Given associativity, $(\forall\ n \in \mathbb{N})$ there is a unique way to write $\prod_{i=1}^{n} a_i$ given by $a_1 = a_1$, $a_1 a_2$ is given by the law, and $a_1 \ldots a_n = (a_1 ... a_i)(a_{i+1} ... a_n)$.

Proof. By induction. □

1.2 Groups and Subgroups

Definition. A **group** G is a set equipped with a law of composition such that:

1. The law is associative.
2. There is an identity e s.t. $ae = ea = a\ \forall a \in G$.
3. $\forall\ a \in G$, $\exists\ a^{-1}$ s.t. $a^{-1}a = aa^{-1} = e$.

We immediately inherit cancellation laws. The group is called **abelian** if the law of composition is commutative. The **order** of a group G is the number of elements it contains, denoted by $|G|$.

Example. $(\mathbb{R}_{\neq 0}, \times)$ for multiplication and $(\mathbb{R}, +)$ for addition.

Example. GL_n is the group of $n \times n$ invertible matrices with matrix multiplication.

Example. Let M be the set of permutations on a set T with composition of functions.

Example. S_n is the permutation on $\{1, 2, ..., n\}$, $|S_n| = n!$.

Example. S_2 is a group of order 2. This is completely determined since 1 must be in the group and by closure since $g \neq 1$, $g^2 \neq g$ so $g^2 = 1$.

Example. S_3 has order 6 and is the smallest group for which composition is not commutative. Namely, Let x be the cyclic permutation of $(1, 2, 3)$ and y the transposition of $(1, 2)$. Then, $S_3 = \{1, x, x^2, y, xy, x^2y\}$. This is because $x^3 = 1$, $y^2 = 1$, $yx = x^2y$ and $xy \neq yx$.

Example. Given an arbitrary set, T, the set of all bijections (automorphisms) on T denoted $\text{Sym}(T) = \text{Aut}(T)$ is a group.

Definition. A subset $H \subseteq G$ is a **subgroup** if:

1. It is closed: $a, b \in H \implies ab \in H$.
2. The identity is in H.
3. If $a \in H$ then $a^{-1} \in H$.

Example. $GL_n(\mathbb{R}) \leq \text{Aut}(\mathbb{R}^n)$ is the subgroup linear maps only of the larger group of all bijections.

1.3 Subgroups of Additive Group of Integers

Let's consider the group of integers under addition, noted $(\mathbb{Z}, +)$.

Proposition. Every subgroup is of the form $a\mathbb{Z} := \{n \in \mathbb{Z} : n = ka \text{ for } k \in \mathbb{R}\}$ for $a \in \mathbb{R}$.

Proof. Note that $a\mathbb{Z}$ is a group $\forall a \in \mathbb{R}$. Suppose $H \neq \{0\}$ is a subgroup. Let b be the smallest positive integer and we conclude $H = b\mathbb{Z}$, since if we take arbitrary $h \in H$ and write this as $h = mb + r$, $h + (-mb) \in H \implies r \in H \implies r = 0$ meaning $h = mb$. $\square$

Definition. Given $a, b \in \mathbb{Z}$, $\exists\ d \in \mathbb{Z}$ s.t. $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$. We call d the $\gcd(a, b)$. If $d = 1$ then we say a and b are **relatively prime**. We may also denote $m = \text{lcm}(a, b)$ given by $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$ since the intersection of two groups is also a group.

1.4 Cyclic Groups

Definition. Given $x \in G$ the smallest subgroup containing x is the **cyclic subgroup** $\langle x \rangle := \{..., x^{-2}, x^{-1}, 1, x, x^2, ...\}$. This may or may not be an infinite set.

Proposition. Let S denote the set of integers k s.t. $x^k = 1$. Then S is a subgroup of $(\mathbb{Z}, +)$. Namely, $x^r = x^s \iff r - s$ must be in S and $S = n\mathbb{Z}$ for some integer n.

- If $\langle x \rangle$ has infinite order, it is said to be infinitely cyclic.
- If $\langle x \rangle$ has order n, where $|\langle x \rangle| = n$ then we can write $\langle x \rangle = \{1, x, ..., x^{n-1}\}$.
- The identity is the only element of order 1.
- If $k = nq + r$ where n is the order of x and $q, r \in \mathbb{Z}$, then $x^k = x^r$.

- Given $k \in \mathbb{Z}$, we have $|\langle x^k \rangle| = n/d$ where $d = \gcd(k, n)$.

Definition. Subgroups of G **generated by a subset** $U \subseteq G$ are the smallest groups containing U. U is said to generate G if $\langle U \rangle = G$.

1.5 Isomorphisms

Example. $G_1 := \{\pm 1, \pm i\}$ under complex multiplication and $G_2 \leq S_4$ generated by $\langle \rho \rangle = \{e, \rho, \rho^2, \rho^3\}$ since $\rho^4 = 1$. Note that G_1 and G_2 have the same multiplication structure with a relabeling.

Definition. An **isomorphism** $f : G_1 \to G_2$ is a bijection where $f(x \cdot y) = f(x) \cdot f(y)$ $(\forall\ x, y \in G_1)$. In this case, we write $G_1 \cong G_2$.

Proposition. Every two cyclic groups of order n are isomorphic.

Proof. Let $G_1 = \langle x_1 \rangle$ and $G_2 = \langle x_2 \rangle$ both be of order n. Then $f : G_1 \to G_2$ s.t. $f(x_1^k) = x_2^k$ is a bijection. Also, $f(x_1^n \cdot x_1^m) = f(x_1^{n+m}) = x_2^{n+m} = x_2^n x_2^m$. □

Example (∞, noncyclic). Let $G_1 = (\mathbb{R}, +)$ and $G_2 := (\mathbb{R}_{>0}, \times)$ and f s.t. $x \mapsto e^x$. Since $(\forall x, y \in \mathbb{R})$ $f(x + y) = e^{x+y} = e^x e^y = f(x)f(y)$ and e^x is invertible on $\mathbb{R}_{>0}$.

Example (finite, noncyclic). Klein-4 Group $G_1 \subseteq S_4 := \{e, \tau_1, \tau_2, \tau_1\tau_2\}$. Note that $\tau_1\tau_2 = \tau_2\tau_1$ and $\tau_1^2 = \tau_2^2 = e$ so $(\tau_1 \cdot \tau_2)^2 = e$. Thus we may also write $GL_2(\mathbb{R}) \geq G_2 := \{I, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, -I\}$. Thus $G_1 \cong G_2$.

Example. Is Klein-4 isomorphic to $\{\pm 1, \pm i\}$? No, because Klein-4 has no elements of order 4.

Proposition. If two groups G_1 and G_2 are isomorphic, then:

- $|G_1| = |G_2|$
- G_1 abelian $\iff$ G_2 abelian
- G_1 and G_2 have the same number of elements of every order

Definition. Given G we may construct $\mathrm{Aut}(G)$ which is the set of isomorphisms on G. This is a group under composition of functions. In particular, it is a subset of $\mathrm{Sym}(G)$ which contains every bijection on G, including those that do not preserve the group structure.

1.6 Homomorphisms

Example. Note that $\det : GL_n(\mathbb{R}) \to (\mathbb{R}_{\neq 0}, \times)$ even though $\det(AB) = \det(A)\det(B)$, the determinant is not a bijection.

Definition. A **homomorphism** is a map $f : G_1 \to G_2$ s.t. $f(xy) = f(x)f(y)$.

- The **trivial homomorphism** is a map $f : G_1 \to G_2$ s.t. $x \mapsto e$.
- A composition of two homomorphisms is a third.

Example. $f : S_3 \to S_n$ given on a permutation on S_3 s.t. $f(\sigma)$ matches the permutation for 1,2,3 and leaves everything else untouched. This is injective.

Example. Let $f : (\mathbb{Z}, +) \to S_2$. Let even $\mapsto e$ and odd $\mapsto \sigma$. This is a homomorphism since $f(\text{even} + \text{odd}) = f(\text{odd}) = \sigma = e \cdot \sigma$ and similarly for the other possibilities.

Proposition. Given a homomorphism $f : G \to G'$:

- $f(e) = e'$
- $f(a^{-1}) = (f(a))^{-1}$

Definition. We define the **image** $\text{Im}(f) := \{g' = f(g) \text{ for } g \in G\} \leq G'$ and the **kernel** $\text{kernel}(f) := \{g : f(g) = e'\} \leq G$.

- If $\text{Im}(f) = G'$ and $\text{kernel}(f) = \{e\}$ then f is an isomorphism.
- The kernel is a **normal subgroup** of G, denoted $\text{kernel}(f) \trianglelefteq G$, because $(\forall\ g \in G)$ $(\forall\ h \in k(f))$, $ghg^{-1} \in \text{kernel}(f)$.

  Proof. $f(ghg^{-1}) = f(g)f(h)f(g^{-1}) = f(g)e'f(g)^{-1} = e' = f(e)$. □

Example. $G = GL_n(\mathbb{R}) \to G' = GL_1(\mathbb{R})$ where $f(A) = \det(A)$ is a homomorphism. Then $\text{kernel}(f) = SL_n(\mathbb{R})$ (the group of invertible matrices with determinant 1) is normal.

Example. $f : S_n \to GL_n(\mathbb{R})$, $\sigma \mapsto A_\sigma$ where A is the permutation matrix corresponding to σ. (This is an isomorphism.)

Example. If we combine examples 3 and 4 we get $S_n \to GL_n(\mathbb{R}) \to GL_1(\mathbb{R})$. The image of this composition is $\{\pm 1\} \subseteq GL_1(\mathbb{R})$ and kernel is the set of all even permutations (A_n).

Definition. We define the **center** subgroup of G as $Z(G) := \{z \in G : zg = gz\ (\forall g \in G)\}$.

- This is a normal abelian subgroup of G.
- $Z(G) = G \iff G$ is abelian.
- $Z(S_n) = \{e\}$ for $n \geq 3$.
- $Z(GL_n(\mathbb{R})) = \{\lambda I \text{ for } \lambda \in \mathbb{R}_{\neq 0}\}$.

Definition. The **natural homomorphism** is a map $f : G \to \mathrm{Aut}(G)$ defined by

$$(\forall\ g, h \in G),\ f(g)(h) := ghg^{-1}$$

Proof. $(\forall\ h, h' \in G)$, $f(g)(hh') = ghh'g^{-1} = ghg^{-1}gh'g^{-1} = f(g)(h) \cdot f(g)(h')$. So our proposed function indeed is in $\mathrm{Aut}(G)$. Then, $f(gg')(h) = gg'h(gg')^{-1} = g(g'h(g')^{-1})g^{-1} = f(g) \circ f(g')(h)$. □

Note that the kernel of the natural homomorphism is the set s.t. $ghg^{-1} = h$. But this is simply $gh = hg$. The kernel is $Z(G)$. The image of this function is called the **inner automorphism group** of G.

1.7 Cosets

Suppose $f : G \to G'$ is a group homomorphism and let $H \trianglelefteq G$ be the kernel of f. We know that f partitions the group into equivalence classes, given by the fibers of $\mathrm{Im}(f)$.

Proposition. One of the equivalence classes is H and all equivalence classes are of the form $aH := \{ah : h \in H\}$ for $a \in G$.

Proof. If $f(a) = f(b)$ then $f(a^{-1}b) = f(a^{-1})f(b) = (f(a))^{-1}f(b) = e'$. Thus $a^{-1}b \in H$. Thus $b = ah$ for some $h \in H$. The other direction is trivial. □

Definition. More generally, $\forall\ a \in G$ and any subgroup $H \leq G$ we define the **left cosets** of H in G as $aH := \{ah : h \in H\}$.

Proposition. Let H be a subgroup of G. The left cosets $aH := \{ah : h \in H\}$, given some $a \in G$, partition G. Moreover, for each $a \in G$, the map $\phi_a : H \to aH$ defined by $\phi_a(h) = ah$ is a bijection, so every left coset has the same number of elements as H.

Proof.

- Each element of G lies in some coset. If $g \in G$, then $g = g \cdot e$ with $e \in H$, so $g \in gH$. Hence, the union of all left cosets equals G.
- Two cosets are either identical or disjoint. Let aH and bH be two left cosets. Suppose they intersect: choose $x \in aH \cap bH$. Then $x = ah_1 = bh_2$ for some $h_1, h_2 \in H$. Multiplying on the left by a^{-1} gives $a^{-1}b = h_1h_2^{-1} \in H$, since H is a subgroup. Therefore $b = a(a^{-1}b) \in aH$, so $bH \leq aH$. By symmetry, $aH \leq bH$, and hence $aH = bH$. Thus, any two left cosets are either equal or disjoint.
- The map ϕ_a is a bijection $H \to aH$. ϕ_a is surjective by definition: for every $y \in aH$, there exists $h \in H$ with $y = ah = \phi_a(h)$. ϕ_a is injective: if $\phi_a(h_1) = \phi_a(h_2)$, then $ah_1 = ah_2$. Multiplying on the left by a^{-1} gives $h_1 = h_2$. Hence ϕ_a is a bijection, and $|aH| = |H|$.

□

Corollary. If G is finite and $f : G \to G'$ is a homomorphism, then $|G| = |\,\mathrm{kernel}(f)| \cdot |\,\mathrm{Im}(f)|$.

Proof. The cosets are precisely the fibers of f and each has order $|\,\text{kernel}(f)|$. $\square$

Theorem (Lagrange). Given a finite group G and $g \in G$, the order of g divides the order of G. More generally, the order of any subgroup $H \leq G$ divides G.

Proof. We showed the cosets of H form a partition of G and each coset has the same size. $\square$

Definition. We define the **index** of any subgroup H in G as the number of equivalence classes in the partition, denoted $[G : H]$. Then, if G is finite, $|G| = |H| \cdot [G : H]$.

Example. $|A_n| = \frac{n!}{2}$ where A_n is the group of even permutations since we have $f : S_n \to \{\pm 1\}$ a homomorphism.

Corollary. If G is a finite group of order p where p is prime, then G is generated by any $g \neq e \in G$. Namely, G is cyclic.

Proof. The only two subgroups are $\{e\}$ and G. $\square$

Definition. We call a group **simple** if its only normal subgroups are $\{e\}$ and G. That is, every nontrivial homomorphism from G is injective.

Example. Abelian groups are simple if and only if they are cyclic of prime order. If not, abelian groups are never simple as every subgroup is normal.

Example. A_n is simple for $n \geq 5$. In fact, A_5 is the smallest nonabelian simple group.

1.8 Modular Arithmetic

Definition. Let's fix $n \in \mathbb{N}$, and define a **relation on** $\mathbb{Z}$ s.t. $a \sim b$ if $n \mid (a - b)$. This is clearly an equivalence relation. We denote this by $a \equiv b \pmod{n}$.

What is the structure of the equivalence classes? These are simply the cosets of the subgroup $n\mathbb{Z}$ in $\mathbb{Z}$. Namely, given $a \in \mathbb{Z}$, $\bar{a} = a + n\mathbb{Z}$ (recall that composition is addition here). We will denote the set of equivalence classes $\mathbb{Z}/n\mathbb{Z}$. In particular, there are n of them: $\bar{0}, \bar{1}, \bar{2}, ..., \overline{n-1}$.

We may define addition and multiplication operations on $\mathbb{Z}/n\mathbb{Z}$, given by $\bar{a} + \bar{b} := \overline{a+b}$ and $\bar{a} \cdot \bar{b} := \overline{ab}$.

Note that $(\mathbb{Z}/n\mathbb{Z}, +)$ is a group because $(\mathbb{Z}, +)$ was associative, the identity is $\bar{0}$ and inverses are given by $-\bar{a} = \overline{n-a}$. In fact, $f : (\mathbb{Z}, +) \to (\mathbb{Z}/n\mathbb{Z}, +)$ given by $a \mapsto \bar{a}$ is a group homomorphism that is surjective and has kernel $n\mathbb{Z}$. In particular, $(\mathbb{Z}/n\mathbb{Z}, +)$ is cyclic of order n, generated by $\langle \bar{1} \rangle$.

But is $(\mathbb{Z}/n\mathbb{Z}, \times)$ a group? No, because $\bar{0}$ does not have an inverse. However there is indeed a subset of $\mathbb{Z}/n\mathbb{Z}$ that does form a group under multiplication.

Proposition. $(\mathbb{Z}/n\mathbb{Z})^\times := \{\, \bar{a} \in \mathbb{Z}/n\mathbb{Z} : \gcd(a, n) = 1 \,\}$ is a group under multiplication.

Proof.

- Well-definedness. If $a \equiv b \pmod{n}$, then $n \mid (a-b)$, so $\gcd(a,n) = \gcd(b,n)$. Thus, the condition $\gcd(a,n) = 1$ depends only on the residue class $\bar{a}$, and $(\mathbb{Z}/n\mathbb{Z})^\times$ is well defined.
- Closure. If $\gcd(a,n) = 1$ and $\gcd(b,n) = 1$, then $\gcd(ab,n) = 1$. Hence, $\bar{a}\bar{b} = \overline{ab}$ also lies in $(\mathbb{Z}/n\mathbb{Z})^\times$.
- Identity. Since $\gcd(1,n) = 1$, $\bar{1}$ is in $(\mathbb{Z}/n\mathbb{Z})^\times$, and $\bar{1}\bar{a} = \bar{a}$ for all $\bar{a}$.
- Inverses. If $\gcd(a,n) = 1$, then by Bézout's identity there exist $r, s \in \mathbb{Z}$ such that $ar + ns = 1$. Thus $ar \equiv 1 \pmod{n}$, so $\bar{r}$ is the inverse of $\bar{a}$.

□

Example. What are the last two digits of 2^{1000}? We want $2^{1000} \pmod{100}$. Note that $2^{10} = 1024 \equiv 24 \pmod{100}$. Then $2^{20} = (2^{10})^2 \equiv 24^2 = 576 \equiv 76 \pmod{100}$. Then $76^2 = 5776 \equiv 76$, meaning we are stuck in a loop. So $2^{1000} = (2^{20})^{50} \equiv 76^{50} \equiv 76 \pmod{100}$.

1.9 Correspondence Theorem

Proposition. Let $H \leq G$. Then the following are equivalent:

1. $H \trianglelefteq G$
2. $gHg^{-1} = H \quad \forall\, g \in G$
3. $gH = Hg \quad \forall\, g \in G$
4. $\forall\, g \in G \quad \exists\, g' \in G$ such that $gH = Hg'$

Proof. (1. $\Rightarrow$ 2.) normality gives that the LHS is a subgroup of the RHS, but the action of conjugation is a bijection meaning the orders are the same. Thus we get the equality. (2. $\Rightarrow$ 3.) right multiplication is also a bijection so $gH = (gHg^{-1})g = Hg$. (3. $\Rightarrow$ 4.) take $g' = g$. (4. $\Rightarrow$ 1.) by contradiction. Assume H is not normal, meaning $\exists\, g \in G,\ h \in H$ such that $ghg^{-1} \notin H$. Suppose that for this g, $\exists\, k \in G$ such that $gH = Hk$. $g = ge \in gH \implies g \in Hk$. Then $\exists\, g = h'k$ for some $h' \in H$. Then $k = (h')^{-1}g$, meaning $gH = H((h')^{-1}g)$. But $H(h')^{-1} = H$, so we get $gH = Hg$. But then $gh \in Hg \implies gh = h''g$ for some $h'' \in H$ meaning $ghg^{-1} = h'' \in H$, which is a contradiction. Therefore, $\forall\, k \in G,\ gH \neq Hk$. □

Theorem (Correspondence). Let $\phi : G \to G'$ be a homomorphism, then:

- $H \leq G \implies \phi(H) \leq G'$
- $H' \leq G' \implies \phi^{-1}(H') \leq G$
- $H \trianglelefteq G \implies \phi(H) \trianglelefteq \mathrm{Im}(\phi)$ (the rest is not seen by ϕ, so normality may fail)
- $H' \trianglelefteq \mathrm{Im}(\phi) \implies \phi^{-1}(H') \trianglelefteq G$ (the rest is not seen by ϕ so this is sufficient)

In particular, kernel(ϕ) $\mapsto e'$ and $G \mapsto \mathrm{Im}(\phi)$. Further, there is a bijective correspondence between $\{H \leq G : H \geq \mathrm{kernel}(\phi)\} \longleftrightarrow \{H' \leq \mathrm{Im}(\phi)\}$. Namely, let $A := \{H \leq G : H \geq \mathrm{kernel}(\phi)\}$, $B := \{H' \leq G' : H' \leq \mathrm{Im}(\phi)\}$. Then,

$$\Phi : A \to B \text{ where } H \mapsto \phi(H)$$

$$\Psi^{-1} : B \to A \text{ where } H' \mapsto \phi^{-1}(H')$$

These are bijections and inverses of each other. The idea for containing kernel(ϕ) is that: $\phi^{-1}(\phi(H)) = H \cdot \mathrm{kernel}(\phi) = H$ if $H \geq \mathrm{kernel}(\phi)$. The other direction, $\phi(\phi^{-1}(H')) = H' \cap \mathrm{Im}(\phi) = H'$ since $H' \leq \mathrm{Im}(\phi)$.

1.10 Product Groups

Definition. Let $H, K \leq G$. Then we define the **set product** $HK := \{hk : h \in H, k \in K\}$. In general, this is not a subgroup of G.

Proposition. $HK \leq G$ if $K \leq H$, if $(\forall\ h \in H)(\forall\ k \in K)\ hk = kh$, or if either H, or K is normal. (There are other conditions to make $HK \leq G$, but these are some of them.)

Proof. $H \trianglelefteq G \Rightarrow (h_1k_1)(h_2k_2) = (h_1)(k_1h_2k_1^{-1})(k_1k_2) = (h_1h_3)k_3 \in HK$. □

Proposition. If H, K are finite, then $|HK| = \frac{|H||K|}{|H \cap K|}$.

Proof. Consider the map $\Phi : \{\text{ left cosets of } H \cap K \text{ in } H\,\} \longrightarrow \{\, hK :\ \ h \in H\,\}$ given by $\Phi\big(h(H \cap K)\big) = hK$. We will show that Φ is well-defined and bijective. Each coset hK has exactly $|K|$ elements, and are pairwise disjoint partitioning HK. Then since Φ is bijective, the order of the RHS is the same as the order of the LHS, which is $[H : H \cap K]$. Thus, $|HK| = [H : H \cap K] \cdot |K|$. But for finite groups, $[H : H \cap K] = \frac{|H|}{|H \cap K|}$ since $H \cap K \leq H$.

- Well-defined: if $h_1(H \cap K) = h_2(H \cap K)$ then $h_2^{-1}h_1 \in H \cap K \subseteq K$, so $h_1K = h_2K$.
- Injective: since $h_1, h_2 \in H$, $h_1K = h_2K \implies h_2^{-1}h_1 \in H \cap K \implies h_1(H \cap K) = h_2(H \cap K)$.
- Surjective: every coset hK with $h \in H$ is $\Phi\big(h(H \cap K)\big)$ by definition.

□

Definition. Let H, K be two groups. we define the **external direct product** $G := H \times_e K := \{(h, k) : h \in H, k \in K\}$.

- This is a group when the product is defined as $(h_1, k_1)(h_2, k_2) = (h_1h_2, k_1k_2)$.
- Also, $H \times \{e_K\} := \{(h, e_K) : h \in H\} \trianglelefteq G$ and $\{e_H\} \times K := \{(e_H, k) : k \in K\} \trianglelefteq G$.
- $G = (H \times \{e_K\}) \cdot (\{e_H\} \times K)$.
- $(H \times \{e_K\}) \cap (\{e_H\} \times K) = \{(e_H, e_K)\} = e_G$.

Definition. Let G be a group, with $H, K \trianglelefteq G$, s.t. $G = HK$ and $H \cap K = \{e\}$. Then, we write the **internal direct product** $G = H \times_i K$.

- Under this condition, $(\forall\, h \in H, \forall\, k \in K)\ hk = kh$. This means $G = H \times_i K = K \times_i H$.

  Proof. Take $h \in H, k \in K$ and consider $hkh^{-1}k^{-1}$. $hkh^{-1} \in K$ since $K \trianglelefteq G$ and $khk^{-1} \in H$ since $H \trianglelefteq G$. Then, $hkh^{-1}k^{-1} = h(kh^{-1}k^{-1}) \in H$ and $hkh^{-1}k^{-1} = (hkh^{-1})k^{-1} \in K$. So $hkh^{-1}k^{-1} \in H \cap K = \{e\}$, which means $hkh^{-1}k^{-1} = e \implies hk = kh$. □

Theorem. Suppose $G = H \times_i K$. Let $G' := H \times_e K$. Then $G' \cong G$ with isomorphism $\phi(h, k) = hk$.

Proof.
- homomorphism: $\phi((h_1, k_1)(h_2, k_2)) = \phi(h_1h_2, k_1k_2) = h_1h_2k_1k_2$ By commutativity, this is $h_1k_1h_2k_2 = \phi(h_1, k_1)\phi(h_2, k_2)$.
- surjective since $G = HK$.
- injective since $hk = e \implies h = k^{-1}$ so $h, k^{-1} \in H \cap K$ meaning $h = k = e$.

□

1.11 Quotient Groups

From modular arithmetic, recall that the cosets of $\mathbb{Z}$ under addition formed a group. We now seek to generalize this idea. Exactly when can we put a group structure on the set of cosets $\{aH\}$ for $H \leq G$?

Let's first suppose $f : G \to G'$ is a surjective homomorphism and let $H := \text{kernel}(f)$. We can bijectively map $\text{Im}(f)$ to $\{aH\}$. Let $F : G \to G/H$ s.t. $a \mapsto aH$. This is a surjective homomorphism. Then, G/H inherits the same group structure as $\text{Im}(f)$ meaning $(aH)(bH) = (ab)H$. G/H is called the **quotient group** of G.

Can we do this for an arbitrary subgroup $H \leq G$? Not generally true. Suppose H is not normal in G. Then $\exists\, a \in G$ s.t. $aHa^{-1} \neq H \implies (\exists\, h \in H$ s.t. $aha^{-1} \notin H)$. Then for this h, consider the product $(aH)(a^{-1}H)$. Since $ah \in aH$ and $a^{-1}e \in a^{-1}H$, we should get our product $(ah)(a^{-1}e) = aha^{-1}$ to be in $(aa^{-1})H = H$, which is a contradiction. Thus the multiplication is not well-defined.

So what if $H \trianglelefteq G$? That is, suppose $(\forall\, a \in G)$, $aH = Ha$. Then our product definition $aH \cdot bH := (ab)H$ is indeed well-defined.

Proof. Let's take $a, b \in G$ and calculate the set of all products of cosets. $aH \cdot bH := \{ah \cdot bh' \in G : h, h' \in H\}$. We may use normality to rewrite $aH = Ha$. Then $aH \cdot bH = a(Hb)H = a(bH)H = (ab)HH$. Since H is a closed as a subgroup, $HH = H$. So indeed $aH \cdot bH = (ab)H$. □

Given this quotient group, the identity coset is $eH = H$ and the inverses are $a^{-1}H$.

Proposition. Every normal subgroup of G is the kernel of some homomorphism.

Proof. Suppose $H \trianglelefteq G$, and consider the group G/H. The homomorphism $F : G \to G/H$ s.t. $a \mapsto aH$ is surjective and satisfies $F[H] = H = e_{G/H}$. Thus, kernel$(F) = H$. $\square$

Theorem (First Isomorphism). Let $f : G \to G'$ be a group homomorphism, and let $H := \text{kernel}(f) \trianglelefteq G$. Then $G/H \cong \text{Im}(f) \leq G'$.

Proof. Define the map $\varphi : G/H \to \text{Im}(f)$ by $\varphi(aH) = f(a)$. We show it is an isomorphism:

- Well-defined. If $aH = bH$, then $b^{-1}a \in H = \ker(f)$, so $f(a) = f(b \cdot b^{-1}a) = f(b)f(b^{-1}a) = f(b) \cdot e = f(b)$.
- Homomorphism. For $aH, bH \in G/H$, $\varphi(aH \cdot bH) = \varphi(abH) = f(ab) = f(a)f(b) = \varphi(aH)\varphi(bH)$.
- Injective. If $\varphi(aH) = e' \in \text{Im}(f)$, then $f(a) = e'$, so $a \in H = \text{kernel}(f)$, and hence $aH = H$, the identity of G/H.
- Surjective. Every element of $\text{Im}(f)$ has the form $f(a)$ for some $a \in G$. For each such element, $\varphi(aH) = f(a)$. Therefore, φ is surjective onto $\text{Im}(f)$.

$\square$

Suppose G is a group and $H \trianglelefteq G$. Let K be a subgroup of G such that $H \leq K \leq G$. Then $H \trianglelefteq K$, so the quotient K/H is well-defined. Moreover, $K/H \leq G/H$. Conversely, the preimage of any subgroup of G/H under the natural projection $\pi : G \to G/H$ where $g \mapsto gH$ is a subgroup of G containing H. In particular, by the correspondence theorem, there is a bijective correspondence between subgroups of G containing H and subgroups of G/H.

1.12 The Commutator Subgroup

We want to find the condition under which a quotient group G/N is abelian. Namely, when do the cosets, commute?

For any $x, y \in G$, this means $(xN)(yN) = (yN)(xN)$. Using coset multiplication, this is $(xy)N = (yx)N$. This equality holds if and only if $(yx)^{-1}(xy) \in N$. Therefore, G/N is abelian if and only if $x^{-1}y^{-1}xy \in N$ for all $x, y \in G$.

Definition. A **commutator** of $x, y \in G$ is defined as $[x, y] = x^{-1}y^{-1}xy$. Then $[x, y] = e \iff x$ and y commute.

Definition. The **commutator subgroup**, denoted $[G, G]$, is the subgroup generated by all the commutators in G.

$$[G, G] = \langle \{[x, y] : x, y \in G\} \rangle$$

Proposition. $[G, G] \trianglelefteq G$.

Proof. We show that the conjugate of a commutator is also a commutator. For any $g \in G$, $g[x,y]g^{-1} = g(x^{-1}y^{-1}xy)g^{-1} = (gx^{-1}g^{-1})(gy^{-1}g^{-1})(gxg^{-1})(gyg^{-1}) = [gxg^{-1}, gyg^{-1}]$. Let a be any element in $[G,G]$. Then a is a product of commutators; namely, $a = \prod x_i$, where each x_i is a commutator. Its conjugate is $gag^{-1} = g(\prod x_i)g^{-1} = \prod(gx_ig^{-1})$. Since each gx_ig^{-1} is a commutator, gag^{-1} is also product of commutators, so is in $[G,G]$. $\square$

Theorem. Suppose N is a normal subgroup of G. Then the quotient group G/N is abelian if and only if the commutator subgroup $[G,G] \leq N$. In particular, $[G,G]$ is the smallest subgroup that makes the quotient abelian.

Proof.
- ($\Rightarrow$) Assume G/N is abelian. This implies $x^{-1}y^{-1}xy \in N$ for all $x, y \in G$. So every commutator is in N. The commutator subgroup $[G,G]$ is generated by these commutators. By definition, $[G,G]$ is the smallest group containing all the commutators of G, so $[G,G] \leq N$.
- ($\Leftarrow$) Assume $[G,G] \leq N$. We need to show $(\forall\ x, y \in G)\ x^{-1}y^{-1}xy \in N$. Consider a commutator $a = x^{-1}y^{-1}xy$. By definition, $a \in [G,G]$. Since $[G,G] \leq N$, we have $a \in N$.

$\square$

Corollary. Let $\phi : G \to A$ be a group homomorphism, where A is an abelian group. Then $[G,G] \leq \ker(\phi)$.

Proof. By FIT, $G/\ker(\phi) \cong \mathrm{Im}(\phi)$. But $\mathrm{Im}(\phi)$ is abelian since $\mathrm{Im}(\phi) \leq A$, which is abelian. Therefore, $G/\ker(\phi)$ is abelian. By the theorem, we must have $[G,G] \leq \ker(\phi)$. $\square$

2 Symmetries and Applications

2.1 Finite and Discrete Groups of Motions in $\mathbb{R}^2$

Definition. A **motion** is a transformation that preserves distance and angles. They are compositions of translations, rotations, and reflections.

Let $G_0 := O(2) = SO(2) \cup SO(2)r_l$, where $SO(2)$ are the rotations and $SO(2)r_l$ are the reflections about a line I. This group is not commutative.

Example. $r_l \cdot \mathrm{rot}(\theta) \cdot r_l^{-1} = \mathrm{rot}(-\theta) = \mathrm{rot}(\theta)^{-1}$.

Generally, the group of motions is $G := \mathbb{R}^2 \rtimes O(2)$, which includes translations. Its elements take 4 forms:

- **Translations:** $\det(g) = +1$, fixes no points
- **Rotations:** $\det(g) = +1$, fixes one point
- **Reflections:** $\det(g) = -1$, fixes a line
- **Glide Reflections:** $\det(g) = -1$, fixes no points.

Let's consider the finite subgroups of G. We must exclude translations, as they do not have finite order (you can keep going out in any direction and never come back).

Proposition. Any finite subgroup $\Gamma \subset G$ fixes a point P. That is, $(\exists\ P)$ s.t. $(\forall\ \gamma \in \Gamma)$, $\gamma(P) = P$.

Proof. Choose any $s \in \mathbb{R}^2$. The set $\{\gamma(s) : \gamma \in \Gamma\}$ is finite. Let $P := \frac{1}{|\Gamma|} \sum_{\gamma \in \Gamma} \gamma(s)$. Applying any element from Γ to P simply reorders the sum, leaving P fixed. $\square$

Thus, any finite subgroup of motions is isomorphic to a finite subgroup of $O(2)$ (the group of motions fixing the origin). The finite subgroups of $O(2)$ are:

- **Cyclic groups,** C_n: These consist only of rotations. For each n, there is a group of order n generated by a rotation of $2\pi/n$.
- **Dihedral groups,** D_n: These contain rotations and reflections. For each n, there is a group of order $2n$ generated by a rotation of $\theta = 2\pi/n$ (order n) and any reflection r (order 2). Its elements are $\{e, \ldots, \mathrm{rot}(\theta)^{n-1}, r, \ldots, r \cdot \mathrm{rot}(\theta)^{n-1}\}$.

We now consider discrete groups, which do not allow for arbitrarily small translations or rotations. It is possible to have infinite discrete groups, such as translations by an integer multiple of a given vector.

Let Γ be a discrete subgroup of G. We consider its translational part, $L := \Gamma \cap \mathbb{R}^2 = \{t_b \in \Gamma\}$, and its rotational/reflectional part, $\bar{\Gamma} := \Gamma/L \subset O(2)$.

There are 3 possibilities for the lattice structure of L:

- $L = \{0\}$ (trivial lattice, corresponds to finite groups).
- $L = \mathbb{Z}b$ for some $b \neq 0 \in \mathbb{R}^2$ (a "frieze" group).
- $L = \mathbb{Z}a + \mathbb{Z}b$ for linearly independent $a, b \in \mathbb{R}^2$ (a "crystallographic" or "wallpaper" group).

The rotational part $\bar{\Gamma}$ must preserve the lattice L.

Theorem (Crystallographic Restriction). Because of this constraint, if L is a 2D lattice ($L = \mathbb{Z}a + \mathbb{Z}b$), then $\bar{\Gamma}$ can only be C_n or D_n for $n \in \{1, 2, 3, 4, 6\}$.

2.2 Group Actions

Definition. Let G be a group and S a set. We say G **acts on** S, denoted $G \curvearrowright S$, if there is a map $G \times S \to S$, denoted $(g, s) \mapsto g \star s$, that satisfies

- $(\forall\ s \in S)\ e_G \star s = s$
- $(\forall\ s \in S)\ (\forall\ g, g' \in G)\ g' \star (g \star s) = (g'g) \star s$

Note that if we fix $g \in G$, the map $M_g : S \to S$ where $s \mapsto g \star s$ is a bijection with inverse $M_{g^{-1}}$. Thus, having a group action is equivalent to having a group homomorphism $\phi : G \to \mathrm{Sym}(S)$, given by $g \mapsto M_g$.

Definition. The **kernel of an action** is the set $k := \{g \in G\ :\ (\forall\ s \in S)\ g \star s = s\} \leq G$.

- In particular, $k \trianglelefteq G$ because it is precisely the kernel of the homomorphism ϕ. Namely, $k = \{g \in G \mid M_g = \text{Identity map}\}$.
- We call an action **faithful** if the kernel is the identity (equivalently if ϕ is injective).

Definition. The **orbit of an element** $s \in S$ is the subset $O_s := \{g \star s : g \in G\} \subseteq S$.

- The orbits partition S. Namely, the relation $s_1 \sim s_2 \iff (\exists\ g \in G)$ s.t. $g \star s_1 = s_2$ is an equivalence relation.
- We call an action **transitive** if there is only one orbit (in particular, if $O_s = S$).

Definition. The **stabilizer of an element** $s \in S$ is the subgroup $G_s := \{g \in G \mid g \star s = s\} \leq G$.

- In particular, the kernel of the action is the intersection of all the stabilizers: $k = \bigcap_{s \in S} G_s$.
- If $H := G_s$, then $g_1 \star s = g_2 \star s \iff g_1^{-1} g_2 \in H \iff g_1 H = g_2 H$.
- If $g \star s_1 = s_2$, then their stabilizers are conjugate: $G_{s_2} = g G_{s_1} g^{-1}$.

Proof. $h \in G_{s_2} \Rightarrow (g^{-1}hg) \star s_1 = (g^{-1}h) \star (g \star s_1) = g \star h \star (s_2) = g^{-}1 \star s_2 = s_1$ Thus $h \in G_{s_1}$ so $G_{s_2} \subseteq G_{s_1}$. Similarly, $gG_{s_1}g^{-1} \subseteq G_{s_2}$ since if $k = ghg^{-1} \in gG_{s_1}g^{-1}$, then $k \star s_2 = s_2$. □

Example. $G \curvearrowright G$ by left multiplication. The orbit of any element is G itself, so this is a transitive action. The stabilizer of any element is the identity, so this is a faithful action.

Example. $GL_n(V) \curvearrowright V \setminus \{0\}$ by matrix multiplication. This is transitive and faithful (certain matrices may fix eigenvectors, but taking the intersection and asking for a matrix that fixes every vector is only the identity matrix).

Example. $S_n \curvearrowright \{1, \ldots n\}$ by permuting the letter. Once again, this is transitive, but not faithful since the stabilizer of an element is isomorphic to S_{n-1}, which is not the identity unless $n = 2$.

Actions on Cosets. Suppose $H \leq G$ (not necessarily normal). Consider the set of left cosets $S = G/H$ (which is not a group unless H is normal in G). The natural action of G on S is given by $g \star (xH) = (gx)H$. This action is always transitive, and the stabilizer of the coset H is the subgroup H itself.

Theorem (Orbit–Stabilizer). Suppose $G \curvearrowright S$ via the action $\star$. Fix $s \in S$ and let $H := G_s$. Define the map $f : G/H \to O_s$ by $f(gH) = g \star s$. Consider the natural action $G \curvearrowright G/H$ by $*$, where $x * (gH) := (xg)H$. Then f is a well-defined bijection that also preserves the action $\star$. Namely, $(\forall\ x \in G)$ $(\forall\ gH \in G/H)$ $f(x * gH) = x \star f(gH)$.

Proof.

- Well defined: Suppose $gH = g'H$. Then there exists $h \in H$ such that $g' = gh$. Hence $f(g'H) = (gh) \star s = g \star (h \star s) = g \star s = f(gH)$ since $h \in G_s = H$.
- Injective: Suppose $f(gH) = f(g'H)$, meaning $g \star s = g' \star s$. Then $g^{-1}g' \star s = s$, so $g^{-1}g' \in G_s = H$. Thus $g' = gh$ for some $h \in H$, and hence $gH = g'H$.
- Surjective: Let $t \in O_s$. Then there exists $g \in G$ such that $t = g \star s$. Then $f(gH) = g \star s = t$, so f is surjective.
- Preserves actions $\star, *$: Suppose $x \in G$ and $gH \in G/H$. Then, $f(x*gH) = f((xg)H) = (xg) \star s = x \star (g \star s) = x \star f(gH)$.

□

Corollary. Consequently, $|G : G_s| = |O_s|$. In particular if G is finite then we may write $|G| = |G_s||O_s|$.

Proof. f from above is a bijection meaning $|G/H| = |O_s|$ as sets. But $H = G_s$ meaning $[G : G_s] = O_s$. □

2.3 Cayley's Theorem

Theorem. Let G be a finite group of order n. Then G is isomorphic to a subgroup of S_n.

Proof. Namely we use the fact that $G \curvearrowright G$ by left multiplication is a faithful action. Let this action be represented by the injective homomorphism $M : G \to \mathrm{Sym}(G)$. Since M is injective we have that $\mathrm{Kernel}(M) = \{e\}$. Also, we have that $\mathrm{Sym}(G) \cong S_n$. Then, by the first isomorphism theorem $G \cong G/\mathrm{kernel}(M) \cong \mathrm{Im}(M) \leq \mathrm{Sym}(G) \cong S_n$. □

2.4 Conjugacy Classes

Definition. The **normalizer** of a set (not necessarily subgroup) $S \subseteq G$, denoted $N_G(S)$, is the set of all elements in G that, when conjugating elements of S, leave the set S invariant. Namely, $N_G(S) = \{g \in G \mid gSg^{-1} = S\}$. (Here we may write subgroup, but we note that conjugation is a bijective map so the orders are preserved.)

Definition. The **centralizer** of $S \subseteq G$, denoted $C_G(S)$, is the set of all elements in G that commute with every element of S. Formally, $C_G(S) = \{g \in G \mid gx = xg,\ \forall x \in S\}$. In particular, we have that

- (a) $Z(G) = C_G(G)$
- (b) $x \in C_G(\{x\})$
- (c) $x \in Z(G) \to C_G(\{x\}) = G$
- (d) $T \subseteq S \subseteq G \Rightarrow Z(G) \subseteq C_G(S) \subseteq C_G(T)$
- (e) $C_G(C_G(S)) \supseteq S$ (Proof: S certainly commutes with all the elements it commutes with)
- (f) $C_G(C_G(C_G(S))) = C_G(S)$

  Proof. ($\subseteq$) by (e), $C_G(C_G(S)) \supseteq S$ meaning by (d) $C_G(C_G(C_G(S))) \subseteq C_G(S)$. ($\supseteq$) let $S' := C_G(S)$, then by (e) $S' \subseteq C_G(C_G(S')) \Leftrightarrow C_G(S) \subseteq C_G(C_G(C_G(S)))$. □

- (g) $C_G(C_G(S)) = S$ if and only if $S = C_G(A)$ for some $A \subseteq G$

  Proof. We have demonstrated the if direction by (f). For the other direction, assume $C_G(C_G(S)) = S$. Then S is indeed a centralizer of something, meaning by definition there is some set A such that $S = C_G(A)$. □

Definition. Now let's consider **groups acting on themselves by conjugation**. Namely, let $G \curvearrowright G$ by $(g \star h = ghg^{-1})$. Then,

- The kernel is $k = \{g \in G \mid ghg^{-1} = h\ (\forall\ h \in G)\} = Z(G)$
- The orbits are the **conjugacy classes**; namely, $(\forall\ x \in G)\ \mathrm{Cl}(x) := \{gxg^{-1} \mid g \in G\}$.

- The stabilizers are the centralizers; namely, $(\forall\ x \in G)\ G_x = \{g \in G \mid gxg^{-1} = x\} = C_G(\langle x \rangle)$.

Definition (Class Equation). G is the disjoint union of its conjugacy classes (given by the fact that the orbits partition the set, in this case G). Then, if $x_1, x_2, \ldots, x_t$ are a set of representatives for the conjugacy classes we have that $|G| = \sum_{i=1}^{t} |\mathrm{Cl}_g(x_i)|$. Note that if $x \in Z(G)$, then $\mathrm{Cl}_G(x) = \{x\}$. Thus $|G| = |Z(G)| + \sum |\mathrm{Cl}_{>1}|$.

Proposition. If $H \le G$ then the subgroup $H_G := \bigcap_{g \in G} gHg^{-1}$ is normal in G.

Proof. Suppose $h \in G$. $g \mapsto gh$ is a bijection so we simply reorder the terms in the intersection but still go through all of G. Namely, $hH_Gh^{-1} = h(\bigcap_{g \in G} gHg^{-1})h^{-1} = \bigcap_{g \in G} (hg)H(hg)^{-1}$. □

Theorem. If $H \le G$ such that $[G : H] = p$ where p is the smallest prime divisor of $|G|$, then $H \trianglelefteq G$.

Proof. Consider $H_G \trianglelefteq G$. It suffices to show that $H = H_G \Leftrightarrow [H : H_G] = 1$. Consider the set (not yet group) G/H, which has order p, meaning $|\operatorname{Sym}(G/H)| = p!$. Let $\sigma : G \to \operatorname{Sym}(G/H)$ by $g \mapsto \sigma_g : G/H \to G/H$ by $xH \mapsto gxH$. We note that $\mathrm{kernel}(\sigma) = H_G$ since $\{g \in G : (\forall\ x \in G)\ gxH = xH\}$ but $gxH = xH \Leftrightarrow x^{-1}gxH = H \Leftrightarrow x^{-1}gx \in H$. But this is equivalent to saying $(\forall\ x \in G)\ g \in xHx^{-1} \Leftrightarrow g \in H_G$. Then, by $|G| = |\mathrm{kernel}(\sigma)||\mathrm{Im}(\sigma)|$, we see that $[G : H_G] \mid p!$. Also $H_G \le H$, so $[G : H_G] = [G : H]\,[H : H_G] = p\,[H : H_G]$, hence p divides $[G : H_G]$. We have shown that any prime divisor of $[G : H_G]$ is $\le p$ (because $[G : H_G] \mid p!$), but by hypothesis any prime divisor of $[G : H_G]$ must be $\ge p$ (since it divides —G— and p is the smallest prime divisor of $|G|$). Therefore the only possible prime divisor of $[G : H_G]$ is p itself. But in particular, the exponent of p in $p!$ is 1. Since $[G : H_G]$ divides $p!$, we have $[G : H_G] = p$, meaning $H = H_G$. □

2.5 Conjugation on S_n

We represent elements of S_n as products of disjoint cyclic permutations. For example in S_3, let $x = (123)\ (1 \to 2 \to 3 \to 1)$ and $y = (12)(3)\ (1 \to 2 \to 1,\ 3 \to 3)$.

Theorem. Let $\sigma \in S_n$ be a t-cycle, $\sigma = (m_1, ..., m_t)$. For any $\tau \in S_n$, the conjugate $\tau\sigma\tau^{-1}$ is also a t-cycle; in particular,

$$\tau\sigma\tau^{-1} = (\tau(m_1), ..., \tau(m_t))$$

Proof. We need to show that the function $\tau\sigma\tau^{-1}$ maps $\tau(m_i)$ to $\tau(m_{i+1})$. $(\tau\sigma\tau^{-1})(\tau(m_i)) = \tau(\sigma(\tau^{-1}(\tau(m_i)))) = \tau(\sigma(m_i))$. Since σ maps $m_i \to m_{i+1}$ (and $m_t \to m_1$), the result is as desired. Thus, $\tau\sigma\tau^{-1}$ permutes the elements $\{\tau(m_1), ..., \tau(m_t)\}$ in a cycle, just as σ permutes $\{m_1, ..., m_t\}$. □

Corollary. Two permutations in cycle structure are conjugate if and only if they have the same **cycle structure** (i.e., the same number of cycles of each length). The conjugacy classes (orbits) are in 1-to-1 correspondence with the possible cycle structures.

Corollary. The center of S_n is trivial for $n \geq 3$. (For $n = 2$, S_2 is abelian, so $Z(S_2) = S_2$.)

Proof. Let $\sigma \in Z(S_n)$, so σ commutes with all permutations in S_n. Take any transposition $\tau = (i\ j)$. By the theorem, the conjugate $\tau\sigma\tau^{-1}$ has the same cycle structure as σ. Since σ is in the center, $\tau\sigma\tau^{-1} = \sigma$. Conjugating σ by all transpositions implies that all elements in each cycle of σ must remain fixed under any transposition, otherwise the cycle structure would change. For $n \geq 3$, the only permutation satisfying this is the identity permutation. $\square$

Example. $|S_6| = 720$. The classes of S_6 are

1. e; size: 1
2. $(\cdot\cdot)$; size: $\frac{6\cdot5}{2} = 15$
3. $(\cdot\cdot\cdot)$; size: $\frac{6\cdot5\cdot4}{3} = 40$
4. $(\cdot\cdot\cdot\cdot)$; size: $\frac{6\cdot5\cdot4\cdot3}{4} = 90$
5. $(\cdot\cdot\cdot\cdot\cdot)$; size: $\frac{6\cdot5\cdot4\cdot3\cdot2}{5} = 144$
6. $(\cdot\cdot\cdot\cdot\cdot\cdot)$; size: $\frac{6\cdot5\cdot4\cdot3\cdot2\cdot1}{6} = 120$
7. $(\cdot\cdot)(\cdot\cdot)$; size: $\frac{1}{2}(\frac{6\cdot5}{2}\frac{4\cdot3}{2}) = 45$
8. $(\cdot\cdot)(\cdot\cdot\cdot)$; size: $\frac{6\cdot5}{2}\frac{4\cdot3\cdot2}{3} = 120$
9. $(\cdot\cdot\cdot)(\cdot\cdot\cdot)$; size: $\frac{1}{2}(\frac{6\cdot5\cdot4}{3}\frac{3\cdot2\cdot1}{3}) = 40$
10. $(\cdot\cdot\cdot\cdot)(\cdot\cdot)$; size: $\frac{6\cdot5\cdot4\cdot3}{4}\frac{2\cdot1}{2} = 90$
11. $(\cdot\cdot)(\cdot\cdot)(\cdot\cdot)$; size: $\frac{1}{3!}(\frac{6\cdot5}{2}\frac{4\cdot3}{2}\frac{2\cdot1}{2}) = 15$

Definition (Alternating Group). Every permutation $\sigma \in S_n$ is a product of (not necessarily disjoint) transpositions. The **parity** (even or odd number of transpositions) is an invariant property of the permutation. As a result, we may define the **sign homomorphism** by $\text{sign} : S_n \to \{+1, -1\}$ where $\text{sign}(\sigma) = +1$ if σ is an even product and $\text{sign}(\sigma) = -1$ if σ is an odd product. The kernel of this map is the set of all even permutations, which we will call A_n. A_n is a normal subgroup of S_n and by the First Isomorphism Theorem, $S_n/A_n \cong \{+1, -1\}$, so $|A_n| = |S_n|/2 = n!/2$. It turns out that A_n is a non-abelian simple group for $n \geq 5$.

2.6 p-Groups

Theorem (Cauchy). Let G be a finite group and let p be a prime dividing the order of G. Then there exists an element $x \in G$ such that $\text{Order}(x) = p$.

Proof.

- Lemma: Suppose G is abelian. We prove Cauchy's theorem using induction on $|G|$.
  - Base Case: If $|G| = p$, then G is cyclic and any non-identity element has order p
  - Hypothesis: Assume the result holds for any abelian group of order less than $|G|$
  - Induction: If G is cyclic with $G = \langle g \rangle$, since $p \mid |G|$, let $x = g^{|G|/p}$. This case is straightforward, so assume G is not cyclic. Then take any $y \neq e \in G$ and let $H := \langle y \rangle \leq G$. If $p \mid |H|$, then by above, let $x = y^{|H|/p}$ and we are done. If $p \nmid |H|$, consider the quotient group G/H (since H is cyclic, it is normal). By Lagrange's Theorem, $|G| = |H| \cdot |G/H|$. Since $p \mid |G|$ but $p \nmid |H|$, it must be that $p \mid |G/H|$. Since G is abelian, G/H is abelian, and $|G/H| < |G|$, we may use the induction hypothesis to say that there exists a coset $gH \in G/H$ with $\text{Order}(gH) = p$. The order of gH in G/H, which is p, must divide the order of g in G. Thus, let $x = g^{\text{Order}(g)/p}$.
- General Case: Suppose G is non-abelian. Again, we proceed by induction on $|G|$, using $Z(G)$ and $G \curvearrowright G$ by conjugation.
  - If $p \mid |Z(G)|$, since $Z(G)$ is an abelian subgroup of G, by the lemma, there exists an $x \in Z(G) \leq G$ with order p. We are done.
  - If $p \nmid |Z(G)|$, we use the class equation: $|G| = |Z(G)| + \sum_{g_i \notin Z(G)} |\text{Class}(g_i)|$ where $\{g_i\}$ are a set of representatives for the classes of G. (Here we use the fact that the class contains more than one element if and only if its elements are not in $Z(G)$.) Since $p \mid |G|$, there must exist at least one g_i such that $p \nmid |\text{Class}(g_i)|$. For this g_i, we know $|\text{Class}(g_i)| = [G : C_G(g_i)] = |G|/|C_G(g_i)|$, where the centralizer is stabilizer for g_i. Rearranging, $|G| = |C_G(g_i)| \cdot |\text{Class}(g_i)|$. Since p divides G but doesn't divide $|\text{Class}(g_i)|$, p must divide $|C_G(g_i)|$. But since $g_i \notin Z(G)$, its centralizer $C_G(g_i)$ is a proper subgroup of G, so $|C_G(g_i)| < |G|$. We have found a proper subgroup $C_G(g_i)$ whose order is divisible by p. By the induction hypothesis, there exists $x \in C_g(g_i) \leq G$ with order p.

$\square$

Definition. There are two equivalent definitions for a p-**group** (though the second is more versatile as it holds for infinite groups as well):

1. A finite group G is a p-**group** if its order is a power of a prime p, i.e., $|G| = p^m$ for some $m \geq 0$.
2. A group G is a p-**group** if every element $g \in G$ has an order that is a power of p, i.e., $\forall\, g \in G, |\langle g \rangle| = p^{m(g)}$ for some fixed prime p.

Proof. Definition 1 $\Rightarrow$ Definition 2 because by Lagrange's Theorem, every element $g \in G$ has an order that is also a power of p, i.e., $|\langle g \rangle| = p^{m'}$ for some $m' \leq m$.. To prove Definition 2 $\Rightarrow$ Definition 1 (in the finite case), we use Cauchy's theorem and assume G is finite such that every element of G has an order that is a power of p. If $|G| \neq p^m$ for every $m \in \mathbb{N}_{\nvdash}$, then $\exists\ q \in \{\text{Primes}\}$ such that $q \mid |G|$ and by Cauchy, $x \in G$ with order q. But by assumption, $\text{Order}(x) = p^{m(x)} = q$, which is a contradiction. Thus $|G| = p^m$ for some $m \in \mathbb{N}_{\nvdash}$. □

Lemma. Let $x, y \in G$ be elements of a group such that $xy = yx$ and $\gcd(\text{ord}(x), \text{ord}(y)) = 1$. Then $\text{ord}(xy) = \text{ord}(x) \cdot \text{ord}(y)$. In particular, $\langle x, y \rangle \cong \langle x \rangle \times \langle y \rangle \cong \langle xy \rangle$.

Proof. Let $m = \text{ord}(x)$ and $n = \text{ord}(y)$. Since x and y commute, $(xy)^k = x^k y^k$ for all $k \in \mathbb{Z}$. Suppose $(xy)^r = e$. Then $x^r y^r = e$, meaning $x^r = (y^{-1})^r$. But because $\text{ord}(x)$ and $\text{ord}(y) = \text{ord}(y^{-1})$ are coprime, the only way a power of x equals a power of y is if $x^r = e$ and $y^r = e$. Therefore $m \mid r$ and $n \mid r$. Since $\gcd(m, n) = 1$, we have $mn \mid r$. The smallest such r is mn. Hence $\text{ord}(xy) = mn$. □

Proposition. If $G = C_p$, where p is prime, then $\text{Aut}(G) \cong C_{p-1}$.

Proof. Let $G = \langle g \rangle$ be cyclic of prime order p. Any automorphism $\varphi \in \text{Aut}(G)$ is determined by what it does to the generators, since from there, since $\varphi(g^m) = \varphi(g)^m$. For cyclic groups of prime order, every nonidentity element is a generator. In particular, let φ_k be such that $g \mapsto g^k$ where $k \in \{1, \ldots, p-1\}$. Thus, there are $p - 1$ choices for $\varphi(g)$, meaning $|\text{Aut}(G)| = p - 1$. $\text{Aut}(G)$ is abelian because $\varphi_k \circ \varphi_\ell = \varphi_\ell \circ \varphi_k$. By Cauchy's theorem, for each prime divisor q of $p-1$, there exists an element of order q in $\text{Aut}(G)$. Using the lemma, we can find an element of order $p - 1$ by writing $p - 1$ as its prime decomposition. If an abelian group has an element with the same order as the group, then the group is cyclic. □

Proposition. If P is a p-group and $|P| > 1$, then $|Z(P)| > 1$.

Proof. Using the class equation $|P| = |Z(P)| + \sum [P : C_P(g_i)]$. Each index $[P : C_P(g_i)]$ for $g_i \notin Z(P)$ is > 1 and must thus must be a power of p since it divides $|P|$. Thus p divides the sum. Since $p \mid |P|$, we must have $p \mid |Z(P)|$. Thus $|Z(P)| > 1$. □

Proposition. If $|P| = p^2$, then P is abelian.

Proof. From above we know $|Z(P)| > 1$. By Lagrange's theorem, $|Z(P)|$ is p or p^2. If $|Z(P)| = p^2$, $P = Z(P)$ and is abelian. If $|Z(P)| = p$, take $g \in P \setminus Z(P)$. The centralizer $C_P(g)$ contains $Z(P)$ and g, so $|C_P(g)| \geq p + 1$. Since the centralizer is a subgroup of G, $|C_P(g)| \mid p^2$, so $|C_P(g)| = p^2$, since there are no other options. This means $C_P(g) = P$, so $g \in Z(P)$, a contradiction. □

Proposition. If $|P| = p^2$, then $P \cong C_{p^2}$ or $P \cong C_p \times C_p$.

Proof. By Cauchy's Theorem, every element $g \neq e$ has order p or p^2. If there exists an element $x \in P$ with $\text{Order}(x) = p^2$, then $P = \langle x \rangle$ so $P \cong C_{p^2}$. Otherwise suppose no element has order p^2. Then every non-identity element must have order p. Since P is abelian (by the previous proposition), we can find $h \neq e \in P$ and $k \neq e \in P \setminus \langle g \rangle$. Let $H = \langle h \rangle$ and $K = \langle k \rangle$. Both H and K are subgroups of order p, and in particular, normal. $H \cap K$ must be a subgroup H By Lagrange, $|H \cap K|$ divides $|H| = p$. So $|H \cap K| = 1$ or p. But if $|H \cap K| = p$, then $|H \cap K| = |H| \implies H = K$, which is a contradiction. Therefore, $H \cap K = \{e\}$. Then, it follows that $|H||K| = p^2 = |P|$. Thus $P = \langle g \rangle \times \langle h \rangle \cong C_p \times C_p$. $\square$

Proposition. If G is a finite abelian group of order $n = \prod_{i=1}^{m} p_i^{a_i}$, then $G \cong G_{p_1} \times G_{p_2} \times \cdots \times G_{p_m}$. In particular, each G_{p_i} is a p_i-group. Each G_{p_i} can further be uniquely decomposed as $G_{p_i} \cong C_{p_i^{a_{i1}}} \times C_{p_i^{a_{i2}}} \times \cdots \times C_{p_i^{a_{ik_i}}}$ for some specific choice of $a_{i1} + \cdots + a_{ik_i} = a_i$ (up to permutation).

2.7 The Sylow Theorems

Let G be a finite group and p a prime. Let the order of G be $|G| = p^m \cdot k$, where $\gcd(p, k) = 1$. We say $H \leq G$ is a **Sylow p-subgroup** if $|H| = p^m$. $\mathrm{Syl}_p(G)$ denotes the set of all Sylow p-subgroups of G.

Example. If $p \nmid |G|$, then $m = 0$. The only subgroup of order $p^0 = 1$ is $\{e\}$. So, $\mathrm{Syl}_p(G) = \{\{e\}\}$.

Example. If $|G| = p^m$, then G itself is the only subgroup of order p^m. So, $\mathrm{Syl}_p(G) = \{G\}$.

Theorem (Sylow I). $\mathrm{Syl}_p(G) \neq \emptyset$. (A Sylow p-subgroup P exists.)

Sketch. We study $G \curvearrowright \{U \subseteq G : |U| = p^m\}$ by left multiplication and show that there is an element of S (namely, a subset of G) for which the stabilizer is a Sylow *p*-subgroup. $\square$

Proof. Let $S = \{U \subseteq G : |U| = p^m\}$ (U is a subset, not necessarily a subgroup of G). The size of this set is $|S| = \binom{p^m k}{p^m}$. Let $G \curvearrowright S$ by left multiplication ($g \cdot U = gU$). This is well-defined since $|gU| = |U|$. We claim $p \nmid |S| = \frac{(p^m k)(p^m k - 1) \ldots (p^m k - (p^m - 1))}{(p^m)(p^m - 1) \ldots (p^m - (p^m - 1))}$ since $\gcd(p, k) = 1$. Each numerator term has the form $p^m k - \ell$ for $0 \leq \ell < p^m$. Let p^{t_ℓ} be the highest power of dividing $p^m k - \ell$. so that we may rewrite $p^m k - \ell = p^{t_\ell}(p^{m - t_\ell} k - s)$ with $\gcd(p, s) = 1$. But then $p^m - l = p_l^t(p^{m - t_l} - s)$ so $\frac{p^m k - l}{p^m - l} = \frac{p^{m - t_l} k - s}{p^{m - t_l} - s}$, where p is not a divisor since $\gcd(p, s) = 1$. Doing this for $0 \leq \ell < p^m$, we see that $p \nmid |S|$. Now, applying the class equation, there must be some orbit O_U whose size is not divisible by p. Let H be the stabilizer for U. By the Orbit-Stabilizer Theorem, $|G| = |O_U| \cdot |H|$ so $p^m \mid |H|$. Now, let H act on the set U by left multiplication. (This is well defined since if $x \in U$ and $h \in H$, then $hx \in hU = U$, because H is the stabilizer of U.) This action partitions U into orbits of the form Hu, which are right cosets and thus are of equal size. Thus $|H| \mid |U| = p^m$. But from above, we also had $p^m \mid |H|$, meaning $|H| = p^m$. Thus $H = G_U$ is a Sylow p-subgroup. $\square$

Theorem (Sylow II). If Q is any p-subgroup of G, then Q is contained in some Sylow p-subgroup. Equivalently, $\exists\, g \in G$ such that $Q \leq gPg^{-1}$ where $P \in \mathrm{Syl}_p(G)$ is given from the first theorem. As a result, all Sylow p-subgroups are conjugate. If $Q \in \mathrm{Syl}_p(G)$, then $\exists\ g \in G$ such that $Q = gPg^{-1}$.

Sketch. We study $Q \curvearrowright \{gP : g \in G\}$ by left multiplication and show that there is a coset for which the stabilizer contains Q, where the stabilizer is conjugate to P. $\square$

Proof. Let $P \in \mathrm{Syl}_p(G)$, which exists, by the first theorem, and let Q be any p-subgroup. Let $S = \{gP : g \in G\}$ be the set of left cosets of . The size of is $|S| = [G : P] = k$. We know $p \nmid= |S| = k$. Let Q act on S by left multiplication: $x \cdot (gP) = (xg)P$. This action partitions S meaning $|S| = k = \sum |\text{Orbits}|$. The size of any orbit must divide $|Q|$, so all orbit sizes are powers of p. But since $p \nmid k$, at least one orbit must have size $1 = p^0$ (a fixed point). Let gP be this fixed point. Thus, $(\forall\ x \in Q)\ x \cdot (gP) = (xg)P = gP$. $(xg)P = gP \implies (g^{-1}xg)P = P \implies g^{-1}xg \in P \implies x \in gPg^{-1}$. Thus $Q \leq gPg^{-1}$. Now, if Q was also a Sylow p-subgroup, then $|Q| = |P| = |gPg^{-1}|$. Thus $Q = gPg^{-1}$. $\square$

Theorem (Sylow III). $|\mathrm{Syl}_p(G)| \mid k$ and $|\mathrm{Syl}_p(G)| \equiv 1 \pmod p$

Sketch. We study $G \curvearrowright \mathrm{Syl}_p(G)$ by conjugation and show that only P is stabilized by itself. $\square$

Proof. Let $S = \mathrm{Syl}_p(G)$. Let G act on S by conjugation ($g \cdot P = gPg^{-1}$). We know this is a transitive action so there is only one orbit. Since $G_P = N_G(P)$, by the orbit-stabilizer theorem, $|S| = |O_P| = [G : N_G(P)]$. By Lagrange's theorem, $k = [G : P] = [G : N_G(P)] \cdot [N_G(P) : P]$. Thus $|S| \mid k$. Now to prove the second statement, consider $P \curvearrowright S$ by conjugation. This partitions S with $|S| = \sum |\text{Orbits}|$. The orbit of P itself is $O_P = \{xPx^{-1} : x \in P\} = \{P\}$, which has size 1. For any other $P' \in S$ ($P' \neq P$), its orbit $O_{P'}$ must have size > 1. Suppose not; then $xP'x^{-1} = P'$ for all $x \in P$, which means $P \leq N_G(P')$. But trivially $P' \leq N_G(P')$ so P and P' are both Sylow p-subgroups of $N_G(P')$. By the second theorem, all Sylow p-subgroups of $N_G(P')$ must be conjugate. Since P' is normal in its normalizer, conjugation should leave it invariant so $P = yP'y^{-1} = P'$ gives us a contradiction. Thus, for $P' \neq P$, the orbit size $|O_{P'}|$ is > 1. Since the orbit size must divide $|P| = p^m$, we have $p \mid |O_{P'}|$ for all $P' \neq P$. Thus $|S| = |O_P| + \sum |O_{P' \neq P}|$ so $|S| \equiv 1 \pmod p$. $\square$

2.8 Further Results on p-Groups

Theorem. Let $|G| = pq$ where $p > q$ are primes. Then G has a normal Sylow p-subgroup. Also, if G is nonabelian, then $q \mid (p-1)$ and G has exactly p Sylow q-subgroups.

Proof.

- Let $n_p(G)$ be the number of Sylow p-subgroups. $n_p(G)$ must divide q, so $n_p(G) = 1$ or q. By the Sylow counting theorem, $n_p(G) \equiv 1 \pmod p$. Since $p > q$ and $q > 1$, it must be that $q \not\equiv 1 \pmod p$. Therefore, the only possibility is $n_p(G) = 1$, so the Sylow p-subgroup P is unique and normal in G.

- The quotient G/P has order q, which is prime, so G/P is abelian. Defining $G' = [G, G]$, we then have that $G' \leq P$. Now, if G also had a normal Sylow q-subgroup Q, then G/Q would be abelian and $G' \leq Q$. If both were normal, $G' \leq P \cap Q = 1$, so G would be abelian. Therefore, if G is nonabelian, Q cannot be normal, so $n_q(G) > 1$. Since $n_q(G)$ divides p, we have $n_q(G) = p$. By Sylow counting, $n_q(G) \equiv 1 \pmod{q}$, which implies $p \equiv 1 \pmod{q}$, so $q \mid (p-1)$.

□

Theorem. Let $|G| = p^2q$ where p and q are primes. Then G has a normal Sylow p-subgroup or a normal Sylow q-subgroup.

Proof. Let $n_p(G)$ and $n_q(G)$ be the number of Sylow p- and q-subgroups. If $n_q(G) = 1$, we are done. Otherwise, $n_q(G) > 1$, which implies $p \neq q$. By Sylow's third theorem $n_q(G)$ divides p^2, so $n_q(G) \in \{p, p^2\}$.

- Case 1: $n_q(G) = p$. Sylow counting gives $p \equiv 1 \pmod{q}$, so $p > q$. $n_p(G)$ divides q, so $n_p(G) = 1$ or q. Since $n_p(G) \equiv 1 \pmod{p}$ and $p > q$, we cannot have $n_p(G) = q$. Therefore $n_p(G) = 1$, so the Sylow p-subgroup is normal.
- Case 2: $n_q(G) = p^2$. Let Q_1, Q_2 be distinct Sylow q-subgroups. Their intersection is trivial. Each contains $q-1$ nonidentity elements, giving $p^2(q-1)$ elements of order q. Let X be the remaining elements including the identity: $|X| = p^2q - p^2(q-1) = p^2$. Any Sylow p-subgroup S of order p^2 must lie in X, so $S = X$. Thus, the Sylow p-subgroup is unique and normal.

□

Theorem. Let $|G| = p^3q$ where p and q are primes. Then G has a normal Sylow p-subgroup or a normal Sylow q-subgroup, or $p = 2$, $q = 3$ and $|G| = 24$.

Proof. Assume $p \neq q$ and that G has no normal Sylow subgroups, so $n_p(G) > 1$ and $n_q(G) > 1$. Since $n_p(G)$ divides q and $n_p(G) \equiv 1 \pmod{p}$, we must have $n_p(G) = q$, implying $q > p$. $n_q(G)$ divides p^3 and $n_q(G) \equiv 1 \pmod{q}$. Consider the possibilities:

- Case 1: $n_q(G) = p$. This would require $p \equiv 1 \pmod{q}$, impossible since $q > p$.
- Case 2: $n_q(G) = p^3$. The number of elements of order q is $p^3(q-1)$. Let X be the remaining elements: $|X| = |G| - p^3(q-1) = p^3$. Any Sylow p-subgroup S of order p^3 must lie in X, so $S = X$, making it normal. Contradiction.
- Case 3: $n_q(G) = p^2$. Then $p^2 \equiv 1 \pmod{q}$, so $q \mid (p^2-1) = (p-1)(p+1)$. Since $q > p$, we must have $q \mid (p+1)$. The only consecutive primes satisfying this are $p = 2$, $q = 3$, giving $|G| = 24$.

□

Lemma. Let a finite p-group P act on a finite set Ω. Let $\Omega_0 = \{\alpha \in \Omega : x * \alpha = \alpha \quad \forall\, x \in P\}$. Then $|\Omega| \equiv |\Omega_0| \pmod{p}$.

Proof. The orbits partition $\Omega = \Omega_0 \cup (\Omega - \Omega_0)$. Ω_0 is the set of fixed points (orbits of only one element) and $\Omega - \Omega_0$ is the union of nontrivial orbits. By the Orbit-Stabilizer Theorem, each orbit size divides $|P|$, so nontrivial orbit sizes are powers of p. Thus, $|\Omega - \Omega_0|$ is divisible by p, giving $|\Omega| \equiv |\Omega_0| \pmod p$. □

Theorem. Suppose $1 < N \triangleleft P$ where P is a finite p-group. Then $N \cap Z(P) > 1$. In particular, a nontrivial finite p-group has a nontrivial center.

Proof. P acts on N by conjugation. Let $\Omega = N$. The fixed points $\Omega_0 = N \cap Z(P)$. By the lemma, $|N| \equiv |N \cap Z(P)| \pmod p$. Since $|N| > 1$ and divisible by p, $|N \cap Z(P)|$ is divisible by p and thus nontrivial. Taking $N = P$ gives $Z(P) > 1$. □

Corollary. If P is a finite simple p-group, then $|P| = p$.

Proof. By the theorem, $Z(P) > 1$. Since $Z(P) \triangleleft P$ and P is simple, $Z(P) = P$, so P is abelian. A simple abelian group is cyclic with prime order, so $|P| = p$. □

Corollary. Let P be a finite nontrivial p-group. Then P has a subgroup of index p, and every such subgroup is normal.

Proof. Choose a maximal normal subgroup $N \triangleleft P$. By the Correspondence Theorem, P/N is simple and a p-group, so $|P/N| = p$ by the above corollary. Thus, P has a subgroup of index p. But every subgroup of index p is normal. □

Corollary. Let $|G|$ be finite and $p^e \mid |G|$. Then G has a subgroup of order p^e.

Proof. Let P be a Sylow p-subgroup of order p^a with $e \leq a$. By above, P has subgroups of every order $p^k \leq p^a$, giving a subgroup of order p^e in G. □

Theorem. Let $H < P$ where P is a finite p-group. Then $N_P(H) > H$.

Proof. By induction on $|P|$, note $Z(P) \leq N_P(H)$.

- Case 1: $Z(P) \not\leq H$. There exists $z \in Z(P)$ with $z \notin H$. Then $N_P(H)$ contains H and z, so $N_P(H) > H$.
- Case 2: $Z(P) \leq H$. $Z(P) > 1$. Consider $P/Z(P)$, a smaller p-group. Let $H/Z(P) < P/Z(P)$. By induction, $N_{P/Z(P)}(H/Z(P)) > H/Z(P)$. Corresponding subgroup M in P satisfies $H < M \leq N_P(H)$, so $N_P(H) > H$.

□

3 Group Representations

3.1 Definitions

Definition. A **representation** of a group G on a complex vector space V is a homomorphism $\rho : G \to GL(V)$ We denote the set of representations of G on V as $\mathrm{Rep}_{\mathbb{C}}(G) := \{\rho : G \to GL(V)\}$.

- The dimension of V is called the **degree** or **dimension** of the representation. A representation is called **linear** (or one-dimensional) if $\deg(\rho) = \dim(V) = 1$. In this case, $GL(V) \cong \mathbb{C}^\times$.
- We say a representation is **faithful** if the homomorphism ρ is injective. The **kernel** of the representation is $\{g \in G \mid \rho(g) = I_V\}$. Thus, a representation is faithful if $\ker(\rho) = \{e\}$.
- It is straightforward to see that if a group G is generated by a set S, then we only need to define the representations on the elements of S, and this contains the necessary information for the entire representation.

If we choose a basis β for the vector space V with dimension n, we obtain an isomorphism $GL(V) \cong GL_n(\mathbb{C})$. The representation ρ then yields a **matrix representation** $R : G \to GL_n(\mathbb{C})$ given by $g \mapsto [\rho(g)]_B$. The condition that ρ is a homomorphism translates to matrix multiplication: $R_{gh} = R_g R_h$.

Example (Trivial Representation). For any group G, $\rho(g) = 1$ (or the identity operator I) for all g. This is a one-dimensional representation.

Example (S_3 Sign Representation). $\Sigma : S_3 \to GL_1(\mathbb{C})$. $\Sigma(g) = 1$ if g is even, and -1 if g is odd.

Example (S_3 Standard Representation). S_3 is isomorphic to the dihedral group D_3 (symmetries of a triangle). It has a 2-dimensional representation on $\mathbb{R}^2$ (or $\mathbb{C}^2$) that translates to the physical rotation and reflection of the vertices given by:

- Rotation x: $\rho(x) = \begin{pmatrix} \cos(2\pi/3) & -\sin(2\pi/3) \\ \sin(2\pi/3) & \cos(2\pi/3) \end{pmatrix}$
- Reflection y: $\rho(y) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

3.2 Characters

Definition. The **character** of a representation $\rho : G \to GL(V)$ is the complex-valued function $\chi_\rho : G \to \mathbb{C}$ defined by: $\chi_\rho(g) = \mathrm{trace}(\rho(g))$

Proposition. The character is independent of the choice of basis.

Proof. The trace of a linear operator is well-defined because similar matrices have the same trace ($\text{trace}(P^{-1}AP) = \text{trace}(A)$). It is clear that a change of basis induces a similar matrix. $\square$

Proposition. The character χ_ρ is a class function. That is, it is constant on conjugacy classes.

Proof. Let $g' = hgh^{-1}$. Then $\chi(g') = \text{trace}(\rho(hgh^{-1})) = \text{trace}(\rho(h)\rho(g)\rho(h)^{-1})$. Since $\text{trace}(AB) = \text{trace}(BA)$, $\text{trace}(\rho(h)\rho(g)\rho(h)^{-1}) = \text{trace}(\rho(h)^{-1}\rho(h)\rho(g)) = \text{trace}(\rho(g)) = \chi(g)$. $\square$

Example. Characters of S_3. The conjugacy classes of S_3 are $\{1\}$, $\{x, x^2\}$ (order 3 elements), and $\{y, xy, x^2y\}$ (order 2 elements).

Character	1	x	y
trivial	1	1	1
sign	1	1	-1
standard	2	-1	0

Remark. $\chi(e)$ is always the dimension of the representation.

3.3 Sums of Representations

Definition. Let $\rho_V : G \to GL(V)$ and $\rho_W : G \to GL(W)$ be two representations. A **homomorphism of representations** is a linear map $T : V \to W$ such that for all $g \in G$ and $v \in V$:

$$T(\rho_V(g)(v)) = \rho_W(g)(T(v))$$

In particular, ρ_V are the set of bijections on V and ρ_W on W. T maps from V to W in a way that the order of composition does not matter. If T is invertible, the representations are **isomorphic** to each other. (In particular, the dimensions of V and W are the same.)

Definition (Direct Sum). Recall that the direct sum of two vector spaces $V \oplus W$ is a new vector space where every vector is represented as a unique sum of a vector from V plus a vector from W. Let ρ_V and ρ_W be representations on V and W. Then their **direct sum** $\rho_V \oplus \rho_W$ is a representation on $V \oplus W$ defined by:

$$(\rho_V \oplus \rho_W)(g)(v + u) = \rho_V(g)(v) + \rho_W(g)(w)$$

In terms of matrices, if we choose a basis β_V for V and β_W for W, then $\beta := \beta_V \cup \beta_W$ is a basis for $V \oplus W$. Then the matrix of the direct sum has a block diagonal form:

$$[\rho_V \oplus \rho_W]_{\mathcal{B}} = \begin{pmatrix} [\rho_V(g)]_{\beta_V} & 0 \\ 0 & [\rho_W(g)]_{\beta_W} \end{pmatrix}$$

Then it is straightforward to see that the character of a direct sum is the sum of the characters.

$$\chi_{\rho_V \oplus \rho_W} = \chi_V + \chi_W$$

Definition. Let $\rho : G \to GL(V)$ be a representation. A subspace $W \subseteq V$ is **G-invariant** if $\rho(g)w \in W$ for all $g \in G$ and $w \in W$. The restriction $\rho|_W : G \to GL(W)$ is then a **subrepresentation**.

In particular if ρ has no nontrivial, proper G-invariant subspaces, then we say ρ is **reducible**.

Lemma. If W is invariant, extend a basis of W to a basis of V. In this basis, each $\rho(g)$ has the form:

$$R_g = \begin{pmatrix} A_g & * \\ 0 & B_g \end{pmatrix}$$

- A_g represents the subrepresentation on W.
- Since W is invariant, the map $\bar{\rho} : V/W \to V/W$ defined by $\bar{\rho}(g)(v+W) = \rho(g)(v)+W$ is well-defined; its matrices correspond to B_g.

Our goal is to make R_g block diagonal. For any subspace $W \subseteq V$, we can write $V = W \oplus W^\perp$ relative to some inner product. The $(*)$ block is zero if and only if $W^\perp$ is invariant under G. By defining a G-invariant inner product, the corresponding $W^\perp$ becomes G-invariant, giving a block-diagonal decomposition.

3.4 Unitary Representations and Maschke's Theorem

Definition. A **Hermitian form** on a complex vector space V is a map $\langle \cdot, \cdot \rangle : V \times V \to \mathbb{C}$ satisfying (i), (ii), and (iii) below. If it also satisfies (iv), we call the map an **inner product**.

- (i) Conjugate linearity in the first argument: $\langle c_1u_1 + c_2u_2, w\rangle = c_1^*\langle u_1, w\rangle + c_2^*\langle u_2, w\rangle$
- (ii) Linearity in the first argument: $\langle u, c_1w_1 + c_2w_2\rangle = c_1\langle u, w_1\rangle + c_2\langle u, w_2\rangle$
- (iii) Conjugate symmetry: $\langle u, v\rangle = \overline{\langle v, u\rangle}$.
- (iv) Positive definiteness: $\langle u, u\rangle > 0$ for $u \neq 0$.

Definition. A representation ρ is **unitary** if there exists an inner product on V that is invariant under G. That is, for all $g \in G$ and $u, v \in V$:

$$\langle \rho_g(u), \rho_g(v)\rangle = \langle u, v\rangle$$

Proposition. The following definitions are equivalent:

1. ρ is unitary (as defined above)
2. $\rho_g^* = \rho_g^{-1}$ for all $g \in G$, where the adjoint satisfies $\langle \rho_g(u), v\rangle = \langle u, \rho_g^*(v)\rangle$.

Proof. ($1 \Rightarrow 2$) Assume $\langle \rho_g(u), \rho_g(v)\rangle = \langle u, v\rangle$. Then $\langle \rho_g(u), v\rangle = \langle \rho_g(u), \rho_g(\rho_g^{-1}v)\rangle = \langle u, \rho_g^{-1}(v)\rangle$. By definition of the adjoint, $\langle \rho_g(u), v\rangle = \langle u, \rho_g^*(v)\rangle$, so $\rho_g^*(v) = \rho_g^{-1}(v)$ for all v. Hence $\rho_g^* = \rho_g^{-1}$. ($2 \Leftarrow 1$) Assume $\rho_g^* = \rho_g^{-1}$. Then $\langle \rho_g(u), \rho_g(v)\rangle = \langle u, \rho_g^*(\rho_g(v))\rangle = \langle u, \rho_g^{-1}\rho_g(v)\rangle = \langle u, v\rangle$. □

Proposition. If ρ is a unitary representation and W is a G-invariant subspace, then the orthogonal complement $W^\perp$ is also G-invariant.

Proof. If $v \in W^\perp$, we must show $\rho_g(v) \in W^\perp$. That is, for any $w \in W$, $\langle \rho_g(v), w\rangle = 0$. Since ρ a representation $\rho_g^{-1} = \rho_{g^{-1}}$. Since ρ is unitary, $\rho_g^* = \rho_{g^{-1}}$ so $\langle \rho_g(v), w\rangle = \langle v, \rho_{g^{-1}}(w)\rangle$. Since W is invariant, $\rho_{g^{-1}}(w) \in W$. Since $v \in W^\perp$, this inner product is 0. Thus $\rho_g(v) \perp W$. $\square$

Corollary. Every unitary representation is a direct sum of irreducible representations.

Proof. If V is irreducible, we are done. If V is reducible, pick a nontrivial invariant subspace W. By above, $W^\perp$ is invariant, giving $V = W \oplus W^\perp$. Apply the same argument recursively to W and $W^\perp$. Since V is finite-dimensional, this terminates after finitely many steps, producing a decomposition. $\square$

Our goal is thus to show that there is a G-invariant inner product that makes any representation unitary.

Theorem (Construction of Invariant Form). Let ρ be a representation of a finite group G. There exists a G-invariant inner product on V.

Proof. Start with any positive definite form $\{\cdot,\cdot\}$ (we know the standard inner product on $\mathbb{C}$ exists, so we may start with that). Define a new form by averaging over the group:

$$\langle u, v\rangle := \frac{1}{|G|}\sum_{g\in G}\{\rho_g(u), \rho_g(v)\}$$

This new form is clearly an inner product (since it is a sum of inner products). ρ is also unitary under $\langle\cdot,\cdot\rangle$. In particular, $\langle \rho_h(u), \rho_h(v)\rangle = \frac{1}{|G|}\sum_{g\in G}\{\rho_g(\rho_h(u)), \rho_g(\rho_h(v))\}$. But since ρ is a homomorphism this is $= \frac{1}{|G|}\sum_{g\in G}\{\rho_{gh}(u), \rho_{gh}(v)\}$ and since $g \mapsto gh$ is a bijection, we simply reindex to get $= \frac{1}{|G|}\sum_{gh\in G}\{\rho_{gh}(u), \rho_{gh}(v)\} = \frac{1}{|G|}\sum_{g\in G}\{\rho_g(u), \rho_g(v)\} =: \langle u, v\rangle$ $\square$

Theorem (Maschke). Every representation of a finite group G on a finite-dimensional complex vector space is isomorphic to a direct sum of irreducible representations.

Proof. Use the invariant form constructed above to make the representation unitary. Then by the corollary above, we have shown that we can write the decomposition as

$$\rho \cong \bigoplus_i n_i\rho_i$$

where ρ_i are the distinct irreducible representations and n_i are their multiplicities. (In particular, we may have to reorder the irreducible representations, but this doesn't change the isomorphism class of the representation.) $\square$

Example (Permutation Representation of S_3). Let S_3 act on basis vectors e_1, e_2, e_3 by permutation. The vector $v = (1,1,1)^T$ is clearly invariant under all permutations. $W =$

span(v) is an invariant subspace (the trivial representation). By Maschke's Theorem, there is a complementary invariant subspace $W^\perp$ (vectors whose components sum to 0, because any permutation does not change the sum of the components), which corresponds to the standard representation (which deals with the plane $x_1+x_2+x_3=0$). Thus $\rho_{\text{perm}} \cong \rho_{\text{trivial}} \oplus \rho_{\text{standard}}$.

3.5 The Main Theorem

Proposition. $\text{Char}_{\mathbb{C}}(G)$, the set of all characters on G, is a $\mathbb{C}$-vector space.

Proof. A character is a class function and the set of all class functions forms a $\mathbb{C}$-vector space since this set is closed under addition and scalar multiplication by $\mathbb{C}$. Then, we show that the characters are a subspace of the set of class functions. In, particular, if χ_1, χ_2 are characters, then $\chi_1+\chi_2$ is the character of the direct sum representation. For any $c \in \mathbb{C}$, the function $c\chi_1$ lies in the $\mathbb{C}$-span of characters. Thus the $\mathbb{C}$-linear span of all characters is closed under addition and scalar multiplication, so the set of all characters forms a $\mathbb{C}$-subspace. □

We may then define a Hermitian inner product on this space:

$$\langle \chi, \chi' \rangle = \frac{1}{|G|} \sum_{g \in G} \chi^*(g)\chi'(g)$$

Since characters are class functions, we can group terms by conjugacy classes. Let C_i be the classes with representatives g_i. Then,

$$\langle \chi, \chi' \rangle = \frac{1}{|G|} \sum_{\text{classes } i} |C_i| \cdot (\chi^*(g_i)\chi'(g_i))$$

Definition. We say a character χ is **irreducible** if it comes from an irreducible representation. Then, the following two sets are in bijection to each other:

- $\text{Irrep}_{\mathbb{C}}(G) := \{\rho \in \text{Rep}_{\mathbb{C}}(G) : \rho \text{ irreducible}\}/\cong$
- $\text{IrrChar}_{\mathbb{C}}(G) := \{\chi \in \text{Char}_{\mathbb{C}}(G) : \chi \text{ irreducible}\}$

Corollary. Let ρ, ρ' be representations with characters χ, χ'. Then $\rho = \rho' \Leftrightarrow \chi = \chi'$.

Proof. We use Maschke's theorem to decompose both representations into their irreducible decomposition. Then since the characters form an orthonormal basis, any character χ can be decomposed uniquely as $\chi = \sum n_i \chi_i$, where $n_i = \langle \chi, \chi_i \rangle$ by orthonormal decomposition. The other direction is trivial. □

Theorem (Main Theorem).

- Row Orthonormality. The irreducible characters are orthonormal. $\langle \chi_i, \chi_j \rangle = \delta_{ij} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases}$.

- Column Orthonormality: Let $\mathrm{Irr}(G)$ be the set of irreducible characters of G. If g and h are elements of G, then $\sum_{\chi \in \mathrm{Irr}(G)} \chi(g)\overline{\chi(h)} = \begin{cases} 0 & \text{if } g, h \text{ are not conjugate} \\ |C_G(g)| & \text{if } g, h \text{ are conjugate} \end{cases}$.
- Number of Irreducible Characters: The number of isomorphism classes of irreducible representations (which is in bijection to the irreducible characters) equals the number of conjugacy classes of G.
- Dimensional Sum: The sum of the squares of the degrees of the irreducible characters equals the order of the group. $|G| = \sum_{\chi \in \mathrm{IrrChar}_{\mathbb{C}}(G)} (\chi(e))^2$
- Divisibility: The degrees of the irreducible characters $\chi(e)$ divide the order of the group $|G|$.

3.6 Linear Characters

Proposition. Let ρ be a representation of degree n (so $\chi(e) = n$). If g is an element of order m, then $\chi(g)$ is a sum of n roots of unity of order m.

Proof. Let $\rho : G \to GL_n(\mathbb{C})$ be the representation. Pick a basis β for the vector space such that we have the matrix $M := [\rho(g)]_{\mathcal{B}}$. From linear algebra, we know the trace is the sum of the eigenvalues $\lambda_1, \dots, \lambda_n$. Since g has order m, $g^m = e$. Since ρ is a homomorphism, this implies: $M^m = \rho(g^m) = \rho(e) = I_n$. If λ_i is an eigenvalue of M, then λ_i^m is an eigenvalue of $M^m = I_n$. Thus $\lambda_i^m = 1$. Therefore, each eigenvalue is an m-th root of unity, and $\chi(g) = \sum_{i=1}^n \lambda_i$. □

Definition. A character χ is called **linear** if its degree is 1, i.e., $\chi(e) = 1$. In this case, the representation maps into $GL_1(\mathbb{C}) \cong \mathbb{C}^\times$, which is abelian.

Proposition. Let G be a finite abelian group. Then every irreducible character of G is linear.

Proof. Let k be the number of conjugacy classes. Since G is abelian, every element is its own conjugacy class, so $k = |G|$. We know that $|G| = \sum_{i=1}^k d_i^2$, where d_i are the degrees of the irreducible characters. Since we have $|G|$ summands and they must sum to $|G|$ with $d_i \geq 1$, the only solution is $d_i = 1$ for all i. Thus $\chi(e) = 1$ for all irreducible characters. □

Definition. The **Dual Group** (or Character Group) of G, denoted $\hat{G}$, is the set of all linear characters of G.

$$\hat{G} := \{\chi : G \to \mathbb{C}^\times\}$$

Proposition. $\hat{G}$ forms a group under function multiplication.

Proof. Operation: Define $(\chi_1 \cdot \chi_2)(g) = \chi_1(g)\chi_2(g)$. Since $\mathbb{C}^\times$ is abelian, this remains a homomorphism. Identity: The trivial character ($g \mapsto 1$) is the identity. Closure: The product of two degree 1 representations is degree 1. Inverse: $\chi^{-1}(g) = 1/\chi(g) = \chi(g)^*$ (since $\chi(g)$ is a root of unity, its inverse is simply the complex conjugate). □

Lemma. $\widehat{C_n} \cong C_n$.

Proof. Let $C_n = \langle a \rangle$. A character χ is determined by $\chi(a)$. Since $a^n = 1$, $\chi(a)^n = 1$. Thus $\chi(a)$ must be an n-th root of unity ($e^{2\pi ik/n}$). This gives n distinct characters, forming a cyclic group isomorphic to the roots of unity, and thus to C_n. $\square$

Lemma. $\widehat{H \times K} \cong \hat{H} \times \hat{K}$.

Proof. Define a map $\Phi : \hat{H} \times \hat{K} \to \widehat{H \times K}$ where $(\chi_h, \chi_k) \mapsto \chi$ such that $\chi(hk) = \chi_h(h)\chi_k(k)$. This is an isomorphism. $\square$

Theorem. If G is a finite abelian group, then $G \cong \hat{G}$.

Proof. We use the Fundamental Theorem of Finite Abelian Groups, which states $G \cong C_{n_1} \times \cdots \times C_{n_k}$ (product of cyclic groups). Using the two above lemmas, we obtain that:

$$\hat{G} \cong \widehat{\prod C_{n_i}} \cong \prod \widehat{C_{n_i}} \cong \prod C_{n_i} \cong G$$

$\square$

We now examine the relationship between linear characters and the commutator subgroup $[G, G]$. Since linear characters map to the abelian group $\mathbb{C}^\times$, the commutator subgroup must be in the kernel: $[G, G] \leq \ker(\chi)$.

Theorem. There is a bijection between the linear characters of G and the irreducible characters of the abelianization $G/[G, G]$.

$$\text{LinChar}_{\mathbb{C}}(G) \longleftrightarrow \text{IrrChar}_{\mathbb{C}}(G/[G, G])$$

Proof. Since $[G, G]$ is in the kernel, any linear character χ of G factors through the quotient $G/[G, G]$. Conversely, any character of the abelian quotient $G/[G, G]$ can be lifted to a linear character of G. $\square$

We say a group is **perfect** if $G = [G, G]$. For such groups, the abelianization is trivial. It is straightforward to see that if a group is nonabelian simple, then it is perfect. As an example, A_5 is perfect.

3.7 Algebraic Integers and the Center of a Character

Definition. A number $\vartheta \in \mathbb{C}$ is an **algebraic number** if it is a root of a polynomial $P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ with coefficients $a_i \in \mathbb{Q}$. A number $\vartheta \in \mathbb{C}$ is an **algebraic integer** if it is a root of a **monic** polynomial with integer coefficients: $P(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \quad$ where $a_i \in \mathbb{Z}$. If α and β are algebraic numbers (or integers), then their sum and product are also algebraic numbers (or integers).

Lemma. If a rational number $q \in \mathbb{Q}$ is an algebraic integer, then q is a standard integer ($q \in \mathbb{Z}$).

Proof. Let $q = r/s$ where $\gcd(r, s) = 1$. Since q is an algebraic integer, it satisfies a monic polynomial equation with integer coefficients: $0 = \left(\frac{r}{s}\right)^n + a_{n-1}\left(\frac{r}{s}\right)^{n-1} + \cdots + a_0$. Multiplying by s^n gives $r^n = -(a_{n-1}r^{n-1}s + \cdots + a_0 s^n) = -s(a_{n-1}r^{n-1} + \cdots + a_0 s^{n-1})$. This implies s divides r^n. Since $\gcd(r, s) = 1$, it must be that $s = 1$. Therefore $q = r \in \mathbb{Z}$. $\square$

Proposition. Let G be a finite group and χ be a character of a representation of G. For any $g \in G$, the value $\chi(g)$ is an algebraic integer.

Proof. $\chi(g)$ is the trace of the representation matrix $\rho(g)$. The matrix $\rho(g)$ has finite order, so its eigenvalues are roots of unity. Roots of unity are roots of $x^n - 1 = 0$, which is monic with integer coefficients, so they are algebraic integers. Since $\chi(g)$ is the sum of these eigenvalues, and sums of algebraic integers are algebraic integers, $\chi(g)$ is an algebraic integer. $\square$

Definition. Let χ be a character of G. The **center of the character** is defined as:

$$Z(\chi) := \{g \in G : |\chi(g)| = \chi(e)\}$$

Proposition. $|\chi(g)| = \chi(e)$ if and only if $\rho(g) = \lambda I$ for some $\lambda \in \mathbb{C}$ with $|\lambda| = 1$.

Proof. ($\Leftarrow$) If $\rho(g) = \lambda I$, then $\chi(g) = \text{trace}(\lambda I) = \lambda \cdot \dim(V)$. Thus $|\chi(g)| = |\lambda| \cdot \chi(e) = \chi(e)$. ($\Rightarrow$) By the Spectral Theorem, $\rho(g)$ is diagonalizable with eigenvalues $\lambda_1, \ldots, \lambda_n$ on the unit circle, and the trace is the sum of the eigenvalues. By the triangle inequality, $n = |\sum \lambda_i| \leq \sum |\lambda_i| = n$ implies that all λ_i are equal to some λ. Thus $\rho(g)$ is similar to λI, and since scalar matrices commute with everything, $\rho(g) = \lambda I$. $\square$

Theorem. $Z(\chi)$ is a normal subgroup of G.

Proof.

- Subgroup: $e \in Z(\chi)$ since $\chi(e) = \chi(e)$. If $g_1, g_2 \in Z(\chi)$, then $\rho(g_1) = \lambda_1 I$ and $\rho(g_2) = \lambda_2 I$. Then $\rho(g_1 g_2) = \lambda_1 \lambda_2 I$, so $|\chi(g_1 g_2)| = |\lambda_1 \lambda_2| \chi(e) = \chi(e)$. Inverses hold similarly.
- Normality: Since characters are class functions, $|\chi(ghg^{-1})| = |\chi(h)|$. Thus $h \in Z(\chi) \iff ghg^{-1} \in Z(\chi)$.

$\square$

Remark. $Z(\chi)$ is not necessarily abelian (in particular, it contains the kernel of χ, which may not be abelian), but if the representation is faithful, $Z(\chi)$ maps to the center of the image, which is abelian.

Proposition. Let χ be an irreducible character. If $\gcd(|\text{Cl}_G(g)|, \chi(e)) = 1$ and $\chi(g) \neq 0$, then $g \in Z(\chi)$.

Proof. Requires Galois Theory. $\square$

3.8 Burnside's Theorem

Using character theory and the properties of algebraic integers, Burnside proved that any group of order $p^a q^b$ (where p, q are primes) is solvable. This is a famous result where representation theory solved a pure group theory problem. In particular, we can show the following.

Theorem (Burnside). If G is a finite group of order $p^a q^b$ for primes p, q, then G is not non-abelian and simple. (Equivalently, G is abelian or not simple.)

Proof.

- If G is abelian, we are done. Assume G is nonabelian. Consider $[G, G] \trianglelefteq G$. If this is proper in G, we have found a nontrivial (since G is nonabelian) proper subgroup in G so we are done. Thus we assume $[G, G] = G$ and find a nontrivial proper normal subgroup to show that G is not simple.

- Let P be a Sylow p-subgroup ($P \neq \{e\}$ since G is not trivial). Since P is a p-group, $Z(P) \neq \{e\}$. Choose $g \in Z(P)$ with $g \neq e$. Since g commutes with everything in P, $P \leq C_G(g)$. Thus $|G : C_G(g)|$ is coprime to p. Therefore, the size of the conjugacy class $|\mathrm{Cl}_G(g)| = q^\beta$ for some β.

- We apply column orthogonality of the characters to the class containing e (which is just e) and the class containing $g \neq e$.

$$0 = \sum_{\chi \in \mathrm{Irr}(G)} \chi(e)\chi(g) = 1 + \sum_{\chi \in \mathrm{Irr}(G)^*} \chi(e)\chi(g)$$

- We next claim that there exists a nontrivial irreducible character such that $\chi(g) \neq 0$ and $q \nmid \chi(e)$. For the sake of contradiction, suppose for all nontrivial irreducible characters where $\chi(g) \neq 0$, we have $q \mid \chi(e)$. Then we can rearrange the orthogonality relationship as

$$\frac{-1}{q} = \sum_{\chi \neq 1} \frac{\chi(e)}{q} \chi(g)$$

  The RHS consists of algebraic integers (since $\chi(e)/q$ would be an integer by assumption, and $\chi(g)$ is an algebraic integer). However, $-1/q$ is a rational number, meaning both have to be an integer. But since q is prime, $-1/q$ is not an integer, hence we get a contradiction. For this character χ, we have $\chi(g) \neq 0$ and $\gcd(|\mathrm{Cl}_G(g)|, \chi(e)) = 1$. By the proposition, $g \in Z(\chi)$.

- Now we must show that this is nontrivial and proper. Since $g \neq e$, $Z(\chi) \neq \{e\}$. Since G is simple, we must have $Z(\chi) = G$. If $Z(\chi) = G$, then $\rho(g) = \lambda_g I$ for all g. Since ρ is irreducible, this implies ρ maps to an abelian group (scalars commute), or simply that $\dim(\chi) = 1$. But if $\dim(\chi) = 1$, then χ is a linear character. Since $G = [G, G]$, the only linear character is the trivial one (since we showed the linear characters are in bijection with the irreducible characters of $G/[G, G]$), which is a contradiction.

$\square$