Abstract Algebra

Krishna Agaram

Mentor: Swayam Chube

Summer of Science,
May-Jul 2023

Contents

Introduction

This report was made as part of the Summer of Science 2023 in Abstract Algebra, mentored by Swayam Chube.

This report is made to also serve as an introduction to **Group Theory** for a high-school student with little background assumed. It is in the semi-Inquiry-Based-Learning style, where some proofs have been given to introduce ways in which formal proofs are written, while other proofs are left as exercises after sufficient background to prove it is provided.

It serves as an introduction to the field of Group Theory, covering the basics of groups, subgroups, quotient groups, group actions, and Sylow's Theorems. To conclude, it covers some combinatorial results involving group theory - Burnside's Lemma and the Pólya Enumeration Theorem.

Glossary

(Some) Definitions

- binary operation. A function $\star : A \times A \to A$.
- group. A set G is a group under binary operation $\star$ if
  1. $\star$ is associative.
  2. G has an identity 1 - $1 \star g = g \star 1 = g \forall\ g \in G$.
  3. *Every* $g \in G$ is invertible - there exists $h \in G$ with $g \star h = h \star g = 1$.
- order. denoted $|\cdot|$.
  - *of a group*. Its cardinality.
  - *of an element* g *in group* G. The smallest positive integer n with $g^n = 1_G$. ∞ if no such n.
- centralizer. Let A be a subset of group G. $C_G(A) := \{g \in G \mid gag^{-1} = a\ \forall a \in A\}$.
- center. The set of elements that commute with all of G. $Z(G) := C_G(G)$.
- normalizer. Let A be a subset of group G. $N_G(A) := \{g \in G \mid gAg^{-1} = A\}$.

Special groups

- dihedral group.
$$D_{2n} \equiv \langle r, s \,|\, r^n = s^2 = 1 \rangle$$
.
- Heisenberg group. The operation is matrix multiplication.
$$H(\mathbb{F}) \equiv \left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \mid a, b, c \in \mathbb{F} \right\}$$
- Klein-4 group.
$$V \equiv \langle a, b \mid a^2 = b^2 = 1, ab = ba \rangle$$
Abelian. ab is usually denoted c. Isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.
- symmetric group. Operation is function composition.
$$S_n \equiv \{\sigma : [n] \to [n] \mid \sigma \text{ is bijective}\}$$
- quaternion group. Operation is multiplication over $\mathbb{C}$.
$$Q_8 \equiv \{\pm 1, \pm i, \pm j, \pm k\}$$
with $i^2 = j^2 = -1, ij = -ji = k$. Alternate matrix form:

List of all non-isomorphic groups of small order

1. $\{1\}$.
2. $\mathbb{Z}_2$.
3. $\mathbb{Z}_3$.
4. $\mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2$.
5. $\mathbb{Z}_5$.
6. $\mathbb{Z}_6, S_3$.
7. $\mathbb{Z}_7$.
8. $\mathbb{Z}_8, \mathbb{Z}_4 \times \mathbb{Z}_2, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, D_8, Q_8$.
9. $\mathbb{Z}_9, \mathbb{Z}_3 \times \mathbb{Z}_3$.
10. $\mathbb{Z}_{10}, D_{10}$.

Chapter 1

What is a group?

1.1 Symmetries

Suppose we remove a square region from a plane, move it in some way, then put the square back into the space it originally occupied. We try to describe in some reasonable fashion all possible ways in which this can be done. More specifically, we want to describe the possible relationships between the starting position of the square and its final position in terms of motions. However, we are interested in the net effect of a motion, rather than in the motion itself.

To begin, we can think of the square region as being transparent, with the corners marked on one side by $0, 1, 2, 3$. This makes it easy to distinguish between motions that have different effects. It is easy to see that there are 4 places for 0 to end up in, and in each of these either 1 is to the right of 0, or to the left of 0.

These 8 operations make up the *symmetries* of the square. Since they cover all possible motions, and the composition of two motions is a motion as well, we have that these operations are *closed* under composition. These operations together with the composition operator form what is called the *dihedral group of order 8* (D_8).

Treating the operations as functions we see that composition of operations is associative as well. D_8 also satisfies the existence of an identity and an inverse for every element. These properties - closure under group operator, associativity, existence of identity and existence of inverses - are precisely the ones that endow a set together with a binary operator the title of a group.

Definition 1.1 (Binary Operations).

(a) A binary operation $\star$ on a set G is a function $\star : G \times G \to G$. For $a, b, \in G$ we shall write $a \star b := \star(a, b)$.

(b) A binary operation $\star$ on a set G is associative if for all $a, b, c \in G$ we have $a \star (b \star c) = (a \star b) \star c$.

(c) If $\star$ is a binary operation on set G, we say elements a and b of G commute if $a \star b = b \star a$. We say $\star$ (or G) is commutative if $\forall a, b, \in G : a \star b = b \star a$.

Definition 1.2 (Group). A group is a set G, along with a binary operation $\star : G \times G \to G$ satisfying the following

(a) (Associativity) For every $a, b, c \in G$, $(ab)c = a(bc)$.

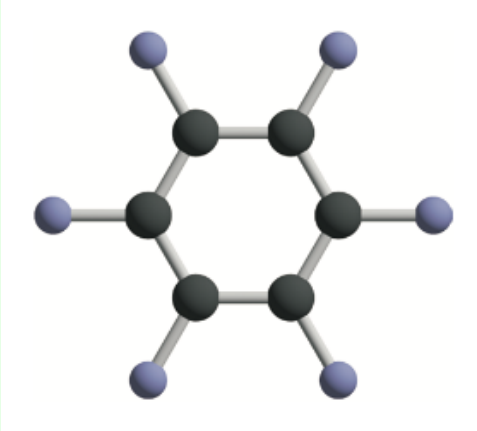
(b) (Identity) There is $e \in G$ such that for all $g \in G$, $e \star g = g = g \star e$.

(c) (Invertibility) For each $g \in G$, there is $h \in G$ such that $g \star h = e = h \star g$.

When $\star$ is a commutative binary operation, that is, $g \star h = h \star g$ for all $g, h \in G$, we say that G is an abelian group.

Henceforth, if the group operation is implicit, we shall simply state "G is a group" rather than "$(G, \star)$ is a group". Further, for a group operation denoted using multiplicative notation, we shall use 1 to denote the identity element, similarly, for additive notation, we shall use 0.

Example 1. The symmetries (actions in 3D space that preserve the figure) of a molecule of Benzene form a group under composition of actions.



A molecule of Benzene, C_6H_6

A simple consequence of the definition (that we would also expect):

Proposition 1.3. *Let G be a group. Then,*

1. *The identity element is unique.*
2. *The inverse of every element is unique.*

The fact that every element of a group can be inverted makes our life much easier, as you will come to appreciate.

1.1.1 Familiar Groups

Example 2.
- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ under $+$ but not $\mathbb{N}$ (inverse).
- $\mathbb{Q} \setminus \{0\}, \mathbb{R} \setminus \{0\}$ under $\times$ but not $(\mathbb{R} \setminus \mathbb{Q}) \setminus \{0\}$ ($\times$ not closed).
- $\mathcal{M}_{m \times n}(\mathbb{R})$ under matrix addition. The set $GL(n, \mathbb{R})$ of invertible $n \times n$ real matrices.
- $\mathbb{Z}_n$ under addition modulo n. $\mathbb{Z}_n^*$ under multiplication modulo n.
- If $(A, \star)$ and $(B, \diamond)$ are groups, then their *direct product* $(A \times B, \square)$ is a group where $(a, b)\square(a', b') := (a \star a', b \diamond b')$.
- For V a vector space, $(V, +)$ is an abelian group.
- $G = \{x \in \mathbb{R} \mid 0 \leq x < 1\}$ under $\star(x, y) := \{x + y\}$. Called the *real numbers modulo 1*.
- $G = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ under addition, $G \setminus \{0\}$ under multiplication.

1.2 Specification

How might we specify a group? That is, explain what the elements of the group are, and the exact input-output correspondence of the binary operation $\star$.

1.2.1 Cayley Tables

A Cayley table is a simple way to do this:

Definition 1.4 (Cayley/Multiplication table). Let $G = \{g_1, \ldots, g_n\}$ be a finite group with $g_1 = 1$. Then the multiplication table of G is the $n \times n$ array whose i, j entry is $g_i \star g_j$.

Note that the task of verifying that G and $\star$ satisfy the axioms of being a group using the Cayley table is usually fairly obvious to think of but typically tedious to do.

A couple of observations: All Cayley table are *Latin squares*. The Cayley table for G is symmetric iff G is abelian.

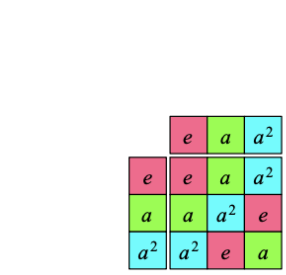
1.2.2 Presentations

Definition 1.5 (Generator). A subset S of G with the property that every element of G can be written as a (finite) product of elements of S and their inverses is called a set of generators of G. We write $G = \langle S \rangle$.

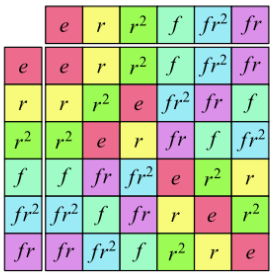
It is easily verified that $\langle S \rangle$ satisfies the group axioms and is thus actually a group. It is important to note that a set of generators is not unique. For example, $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle = \langle 1, -1 \rangle$.

Remark. For G finite, due to the existence of finite orders, it is not necessary to include the inverses of S.

Any equations in a general group G that the generators satisfy are called relations in G. Thus in D_8 we have the relations: $r^4 = 1, s^2 = 1$ and $rs = sr^{-1}$. Relations are most useful to simplify large products of elements in S.

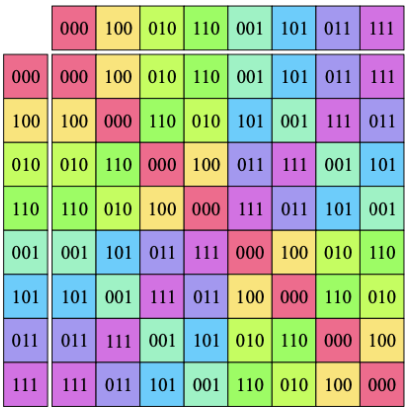


Cyclic group C_3 (or $\mathbb{Z}_3$)

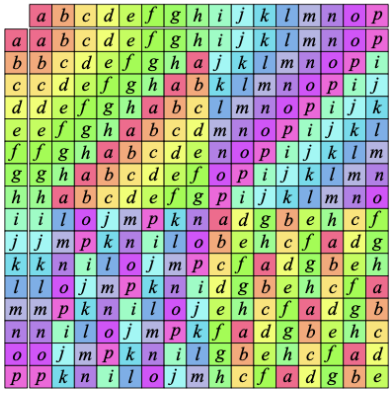


Symmetric group S_3

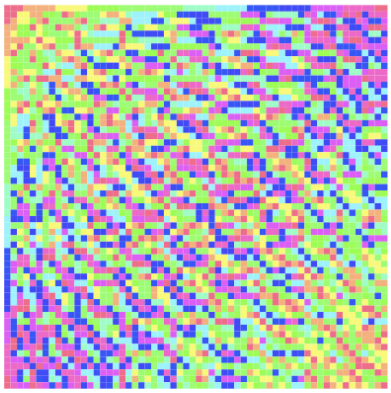
Direct product group $C_3 \times C_3$



Direct product group $C_2 \times C_2 \times C_2$



Quasihedral group with 16 elements



Alternating group A_5

Figure 1.1: The Cayley tables for a few common groups (some of which we will study later)

For abelian groups, the products in $\langle a_1, \ldots, a_n \rangle$ can be written $a_1^{k_1} a_2^{k_2} \ldots a_n^{k_n}$, but not so for non-abelian groups - here is where relations come in handy.

For example, consider element $rsr \in \langle r, s \rangle$. Knowing that $rs = sr^{-1}$, we can write $rsr = sr^{-1}r = s$ - a simplification of the product.

Giving a set of generators and some relations obeyed by the generators is a simple way to specify the elements of a group and their products - this is called a presentation of the group.

Definition 1.6 (Presentation). A presentation of a group G is a pair (S, R) where S is a set of generators of G and R is a set of relations in S. It is usually written $G = \langle S \mid R \rangle$.

Example 3. These groups will be introduced later.

- $D_{2n} = \langle r, f \mid r^n = f^2 = 1, rf = fr^{-1} \rangle$.
- $Q_8 = \langle i, j \mid i^2 = j^2 = -1, ij = -ji \rangle$.
- $S_3 = \langle a, b \mid a^2 = b^3 = 1, ab = ba^2 \rangle$.

1.2.3 Cayley Diagrams

Cayley diagrams provide a visual representation of groups. They are a way to represent the group operation as a graph. The vertices of the graph are the elements of the group, and there is an edge between g and h if $g \star h^{-1}$ is in the set of generators.

To draw a Cayley diagram, one starts with the identity, draws out all the elements that can be reached from the identity, then draws out all the elements that can be reached from those elements, and so on, till no new vertices are reached from the last elements added.

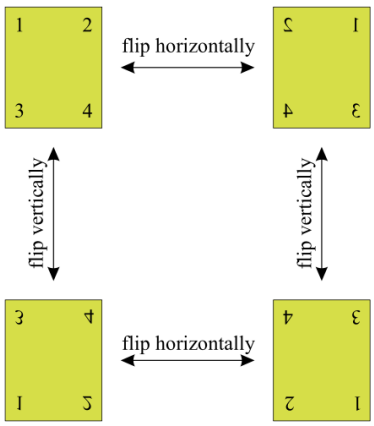
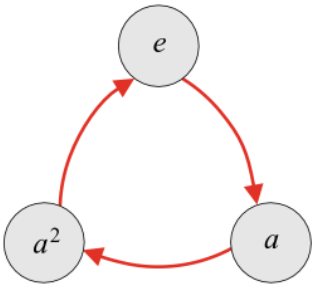
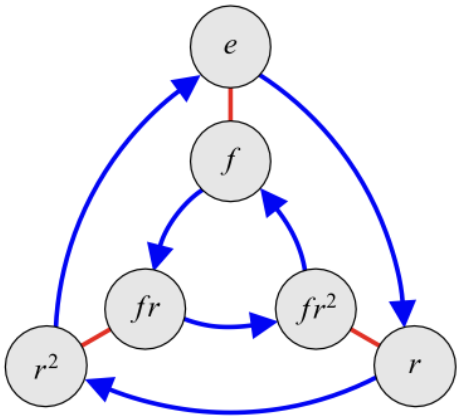


Figure 1.2: The Cayley diagram for the symmetries of a rectangle. The four vertices are labelled for convenience.

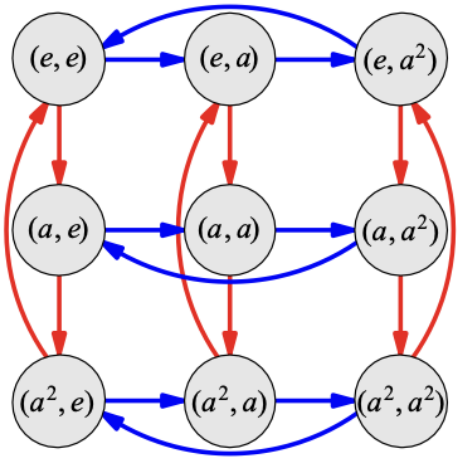
Note that the structure of the Cayley diagram of a group depends heavily on which set of generators is chosen. For example, the Cayley diagram of $C_3 \times C_3$ with generators (a, b) is a 3×3 grid (as in the picture above), while with generators (a, ab) it is a 3×3 grid with a diagonal line of edges.



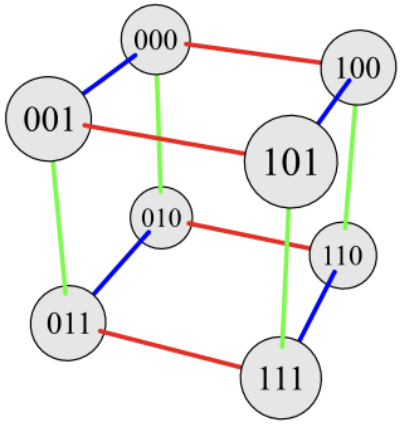
Cyclic group C_3 (or $\mathbb{Z}_3$)



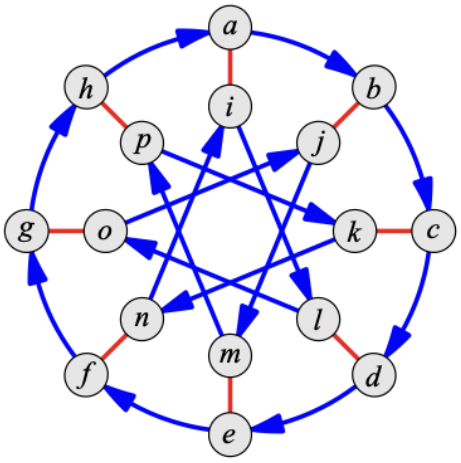
Symmetric group S_3



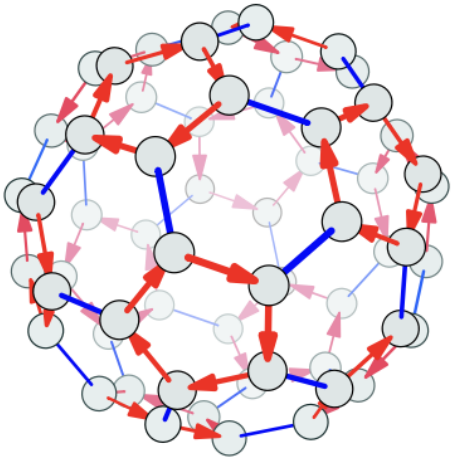
Direct product group $C_3 \times C_3$



Direct product group $C_2 \times C_2 \times C_2$



Quasihedral group with 16 elements



Alternating group A_5

Figure 1.3: Cayley diagrams of small, finite groups.

1.3 Order

The **order of a group** is defined to be its cardinality. We also define the order of an element:

Definition 1.7 (Order). The order of element $x \in G$ is the smallest positive integer n with $x^n = 1$. If no such n exists, x is said to have infinite order. The order of x in G is denoted $|x|$.

The identity e always has order 1. For the group $(\mathbb{Z}, +)$, no other element has finite order. Every element of $(\mathbb{Z}_n^*, \star)$ has finite order. In fact, every element x of finite group G has a finite order, which follows by noting that $\{x^k \mid x \in \mathbb{Z}\}$ is a subset of G and thus $\exists i < j : x^i = x^j \implies x^{j-i} = 1$. Thus the set $\{n \in \mathbb{N} \mid x^n = 1\}$ is nonempty, and hence has a minimum element - precisely the (finite) order.

Some easy results that follow from elementary number theory:

Proposition 1.8. *Let $x \in G$ have finite order n. Then*

1. *if $x^h = 1$, then $n \mid h$.*
2. $|x^k| = \frac{n}{(n,k)}$.

1.4 Homomorphisms and Isomorphisms

In this section we make precise the notion of when two groups 'look the same", that is, have *exactly* the same group-theoretic structure. This is the notion of an isomorphism between two groups. We first define the notion of a homomorphism about which we shall have much more to say later.

Definition 1.9 (Homomorphism). Let G and H be groups. A function $\phi : G \to H$ is called a homomorphism if $\phi(xy) = \phi(x)\phi(y)\ \forall x, y \in G$.

If there is a homomorphism ϕ from G to H, G and $\operatorname{img}\phi$ are essentially relabelling of the same group; the group operation may change in the relabelling but retains properties of the original group operation. ϕ respects and links the group structures of G and $\operatorname{img}\phi \subseteq H$.

Definition 1.10. A homomorphism $\phi : G \to H$ is called an isomorphism if it is bijective. In this case, we say that G and H are isomorphic, and write $G \cong H$.

Here, $\operatorname{img}\phi = H$ so that G and H are essentially the same group upto relabelling. Note also that the inverse of an isomorphism is also an isomorphism, and the composition of two isomorphisms is an isomorphism.

Example 4.

- $\phi : \mathbb{Z} \to \mathbb{Z}_n$ defined by $\phi(x) = x \pmod n$ is a homomorphism.
- $\phi : (\mathbb{R}, +) \to (\mathbb{R} - \{0\}, \times)$ defined by $\phi(x) = e^x$ is a homomorphism.

- $\phi : (\mathbb{R} - \{0\}, \times) \to (\mathbb{R} - \{0\}, \times)$ defined by $\phi(x) = x^2$ is **not** a homomorphism.

1.4.1 Isomorphism classes

Different relabellings of the same group structure may appear in different areas of science, and it is often most useful to know that two groups are isomorphic. Thus arises the problem of classification - putting groups into (a preferably small) set of possible structures.

More formally, one sees that the relation $\cong$ defined on the set of all groups by $G \cong H$ iff G and H are isomorphic is an equivalence relation. The equivalence classes of this relation are called the isomorphism classes of groups. The classification problem is now the determination of the different isomorphism classes.

For example, here is a classification of groups of order 6 that we will establish later.

Proposition 1.11. *There are two isomorphism classes of groups of order 6. Any group G of order 6 is either isomorphic to $\mathbb{Z}_6$ or S_3.*

When are two groups not isomorphic? The (contrapositive of the) following easy proposition gives a simple criterion to check.

Proposition 1.12. *Let G and H be isomorphic groups (and consider isomorphism ϕ). Then the following hold:*

1. $|G| = |H|$.
2. *G is abelian iff H is abelian.*
3. *For every $x \in G$, $|x| = |\phi(x)|$.*

1.5 A zoo of groups

1.5.1 Cyclic Groups

A group is cyclic if it is generated by one element; that is, it is of the form $\langle x \rangle$. Cyclic groups are abelian. We finally see why the order of an element is called its order:

Proposition 1.13. *Let $H = \langle x \rangle$. Then $|H| = |x|$ (where if one side of this equality is infinite, so is the other), where $|\cdot|$ represents the order. More specifically,*

1. *If $|x| = n < \infty$, then $1, x, \ldots, x^{n-1}$ are all the distinct elements of H, and*
2. *Otherwise, $x^a \neq x^b \; \forall a \neq b \in \mathbb{Z}$ and so $|H| = \infty$.*

Corollary 1.14. Let $H = \langle x \rangle$. Then $H = \langle x^k \rangle$ iff $\gcd(|x|, k) = 1$.

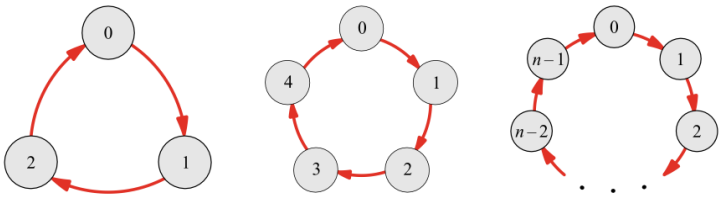


Figure 1.4: The Cayley diagrams of cyclic groups C_3, C_5, C_n.

Proposition 1.15. *Let* G *be a group of order* n*. Then* G *is cyclic iff* $\exists x \in G : |x| = n$.

Cyclic groups are very simple, and have a full classification:

Theorem 1.16. *All cyclic groups are isomorphic to either* $\mathbb{Z}$ *or* $\mathbb{Z}_n$ *for some* n*. Thus, the classification of cyclic groups is complete.*

Proof. Let G be cyclic with generator x. If G is infinite, then the function $\phi : G \to \mathbb{Z}$ defined by $\phi(x^k) = k$ is an isomorphism, so $G \cong \mathbb{Z}$. Otherwise, let $|G| = n$. Then the function $\phi : G \to \mathbb{Z}_n$ defined by $\phi(x^k) = k$ for $0 \leq k < n$ is an isomorphism, so $G \cong \mathbb{Z}_n$. □

We shall now move to the richness of non-abelian groups. First, what does it mean to be abelian? The figure says it all.

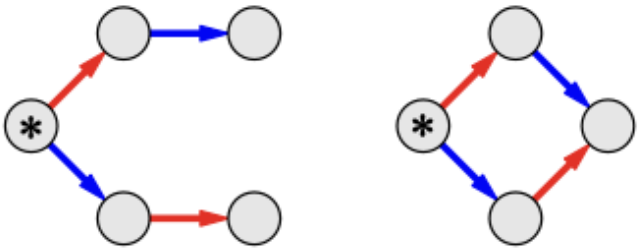


Figure 1.5: On the left is a pattern that never appears in Cayley diagrams for abelian groups: from the node marked *, following a red and then blue arrow does not reach the same node as following a blue and then red. The pattern on the right will always appear instead.

1.5.2 Dihedral Groups

Definition 1.17 (Dihedral Group). The dihedral group D_{2n} is the group of symmetries of a regular n-gon. It has $2n$ elements, n rotations and n reflections. The rotations are generated by r, and the reflections by f. The relations are $r^n = f^2 = 1$ and $rf = fr^{-1}$.

A presentation of D_{2n} is $\langle r, f \mid r^n = f^2 = 1, rf = fr^{-1} \rangle$.
In general, one has for the generators of D_{2n}:

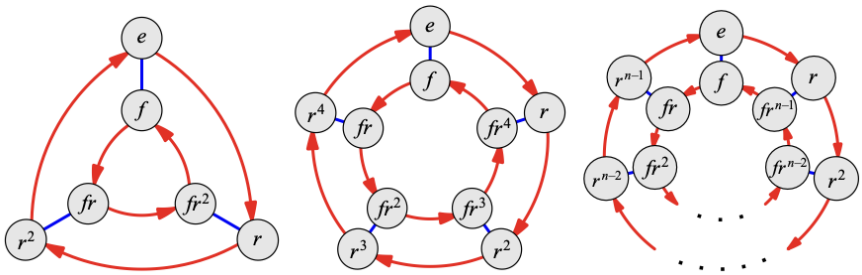


Figure 1.6: The Cayley diagrams of D_6, D_{10}, D_{2n}.

Proposition 1.18. *Any element of* D_{2n} *can be written in the form* $r^k f^j$ *for* $0 \leq k \leq n-1$ *and* $0 \leq j \leq 1$.

Proof. Exercise. □

1.5.3 Symmetric Groups

Definition 1.19 (Symmetric Group). The symmetric group S_n is the group of permutations of the set $\{1, 2, \ldots, n\}$. The group operation is composition of permutations.

More generally, one can define S_A for (possibly infinite) set A. A permutation on set A is defined as a bijection $\sigma : A \to A$. The set of all permutations on A is a group under function composition. It is denoted S_A, the symmetric group on A.

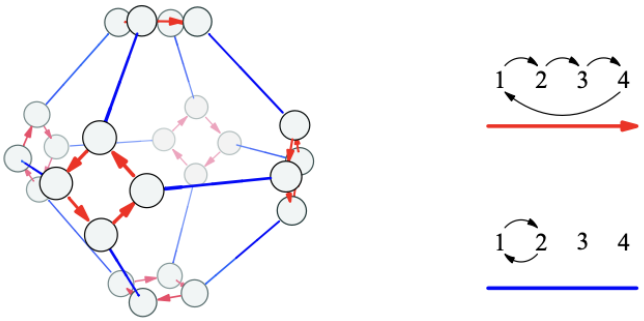


Figure 1.7: A Cayley diagram for S_4 emphasizing the connection between S_4 and the symmetries of an octahedron.

1.5.4 The Alternating Group

Definition 1.20 (Alternating Group). The alternating group A_n consists of all even permutations - that is, it is the group formed by the squares of elements in S_n.

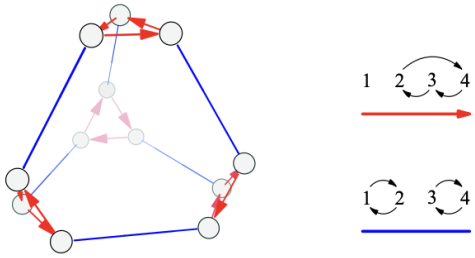


Figure 1.8: A Cayley diagram for A_4 on a truncated tetrahedron. Coincidence that a tetrahedron looks like half an octahedron?

Exercise.

- Prove that A_n is a group under function composition.
- Prove that $|A_n| = \frac{n!}{2}$.

1.5.5 The Quaternion Group

Definition 1.21 (Quaternion Group). The quaternion group Q_8 is the group of quaternions, defined as the set $\{\pm 1, \pm i, \pm j, \pm k\}$ with the relations $i^2 = j^2 = k^2 = -1, ij = k, jk = i, ki = j$.

A presentation for the Quaternion group is $\langle i, j \mid i^2 = j^2 = k^2 = -1, ij = k, jk = i, ki = j \rangle$. Consider the alternate representation of Quaternions as 2×2 matrices:

$$
\begin{aligned}
1 &\mapsto \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I \\
i &\mapsto \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} = iZ \\
j &\mapsto \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = iY \\
k &\mapsto \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} = iX
\end{aligned}
$$

Here X, Y, Z are the Pauli matrices, most useful in Quantum Mechanics.

1.6 Subgroups

An *object* or a mathematical object is any entity we define. For example, D_8 is an object, "of type `group`". Every group is an object. The set of natural numbers is an object. The natural number 1 is also an object. Let's move on.

Sub-objects are ubiquitous in Math. A sub-object of object $\mathcal{O}$ is a subset of $\mathcal{O}$ that also obeys some property that $\mathcal{O}$ obeys. Sub-objects greatly help understand the structure of the object itself.

Definition 1.22 (Subgroup). A subset H of a group G is said to be a subgroup of G if

1. $\star|_{H\times H}$ is a binary operation on H. That is, H is closed under $\star|_{H\times H}$.
2. $(H, \star|_{H\times H})$ is a group.

The binary operation $\star|_{H\times H}$, defined by $\star|_{H\times H} : H \times H \to G, \star|_{H\times H}(x, y) = \star(x, y) \forall x, y \in H$ is called the restriction of $\star$ to $H \subseteq G$.

The fact "H is a subgroup of G" is denoted $H \leq G$.

It is easy to check that the following conditions are necessary and sufficient for H to be a subgroup of group G:

Proposition 1.23. $H \subseteq G$ *is a subgroup iff:*

(a) H *is closed under* $\star$ - $\forall h, k \in H : hk \in H$.

(b) H *is closed under inversion:* $\forall h \in H : h^{-1} \in H$.

(c) And of course, $H \neq \varnothing$.

Note that for finite groups, due to the existence of finite orders (and thus inverses), condition (b) may be omitted. In fact, the two can be combined into a single requirement:

Theorem 1.24 (The subgroup criterion). $H \subseteq G$ *is a subgroup iff:*

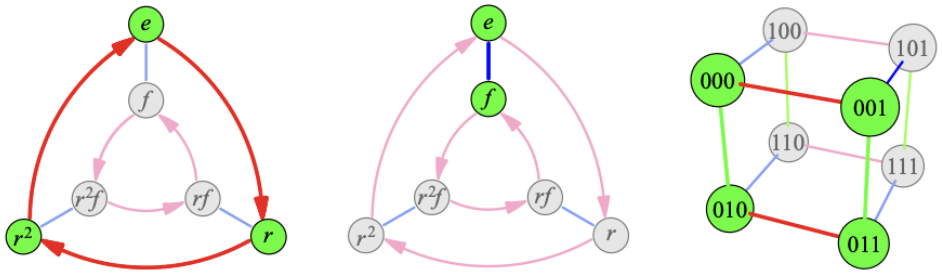
(a) $H \neq \varnothing$

(b) $\forall g, h \in H : gh^{-1} \in H$.

Proof. Exercise. □

1.6.1 Visualizing Subgroups

Subgroups can be fairly easily discerned from the Cayley diagram of a group. A subgroup is just a subset of the vertices of the Cayley diagram that is closed under the group operation and inversion.



A copy of C_3 in the group S_3 | A copy of C_2 in the group S_3 | A copy of V_4 in the group $C_2 \times C_2 \times C_2$

Figure 1.9: A few easy-to-spot subgroups V_4 is the Klein 4-group.

1.6.2 Subgroups of Cyclic Groups

Subgroups of Cyclic groups are very simple - they are all cyclic. This is a consequence of the following theorem:

Proposition 1.25. *Every subgroup of a cyclic group is cyclic. Let* $G = \langle x \rangle$ *have order* n*. If* $H \leq G$*, then* $H = \{1\}$ *or* $H = \langle x^k \rangle$*, where* k *is the smallest positive integer such that* $x^k \in H$*.*

Proof. Let $H \leq G$. If $H = \{1\}$, we are done. Otherwise, there exists $d \in \mathbb{Z} - \{0\}$ with $x^d \in H$. We may wlog assume that $d > 0$, for if $x^d \in H$, then $x^{-d} \in H$. Now take k be the smallest such positive integer. We claim that $H = \langle x^k \rangle$. Let $x^j \in H$. Then $j = qk + r$ for some $q, r \in \mathbb{Z}$ with $0 \leq r < k$. Then $x^j = x^{qk+r} = x^{qk}x^r = (x^k)^q x^r$. Since $x^k \in H$ and $x^r \in H$, we have $x^j \in H$. Thus $H = \langle x^k \rangle$. □

1.6.3 Standard subgroups

Straight from the group

Definition 1.26 (Center). The center of a group G is the set of all elements that commute with every other element in G, that is,

$$Z(G) = \{g \in G : \forall h \in G,\ gh = hg\}$$

Definition 1.27 (Centralizer). For a subset $A \subseteq G$, the centralizer of A, denoted by $C(A)$ is the set of all elements that commute with every element in A.

$$C(A) = \{g \in G : gag^{-1} = a\ \forall a \in A\}$$

We use $C(g)$ to denote $C(\{g\})$.

Definition 1.28 (Normalizer). The normalizer of A, denoted by $N(A)$ is the set of all elements that commutes with A as a set - not necessarily element by element.

$$N(A) = \{g \in G : gAg^{-1} = A\}$$

where $gAg^{-1} = \{gag^{-1} : a \in A\}$.

Exercise. Prove that $Z(G)$, $C(A)$ and $N(A)$ are subgroups of G.

From homomorphisms

Definition 1.29 (Image). The image of a homomorphism $\phi : G \to H$ is the set of elements in H that are mapped to by some element of G.

$$\operatorname{img} \phi = \{\phi(g) : g \in G\}$$

Definition 1.30 (Kernel). The kernel of a homomorphism $\phi : G \to H$ is the set of elements that map to the identity in H.

$$\ker \phi = \{g \in G : \phi(g) = 1\}$$

Exercise. Prove that $\operatorname{img} \phi$ and $\ker \phi$ are subgroups of H and G respectively.

1.6.4 The Lattice of Subgroups of a group

Definition 1.31 (Poset). A partially ordered set (or poset) is a set P together with a binary relation $\leq$ that satisfies the following axioms:

1. **Reflexivity**: $a \leq a$.
2. **Antisymmetry**: If $a \leq b$ and $b \leq a$, then $a = b$.
3. **Transitivity**: If $a \leq b$ and $b \leq c$, then $a \leq c$.

Definition 1.32. Let P be a poset and $S \subseteq P$.

- **Supremum.** An element $a \in P$ is the supremum of S if
  1. $a \geq x \; \forall x \in S$.
  2. If $b \geq x \; \forall x \in S$, then $b \geq a$.
- **Infimum.** An element $a \in P$ is the infimum of S if
  1. $a \leq x \; \forall x \in S$.
  2. If $b \leq x \; \forall x \in S$, then $b \leq a$.

Definition 1.33. A lattice is a partially ordered set in which every two elements have a unique supremum (also called a least upper bound or join) and a unique infimum (also called a greatest lower bound or meet) in the poset.

The set of all subgroups of a group G forms a lattice under set inclusion. The lattice is bounded by $\{1\}$ and G, and the meet and join of H, K are $H \cap K$ and $\langle H \cup K \rangle$ respectively.

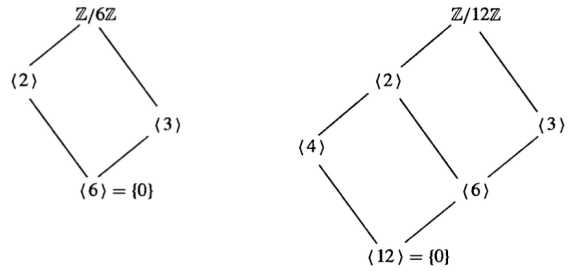


Figure 1.10: The lattice of subgroups of $\mathbb{Z}_6, \mathbb{Z}_{12}$.

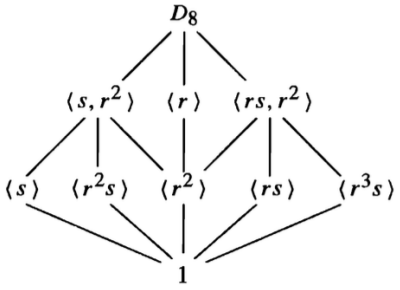


Figure 1.11: The lattice of subgroups of D_8.

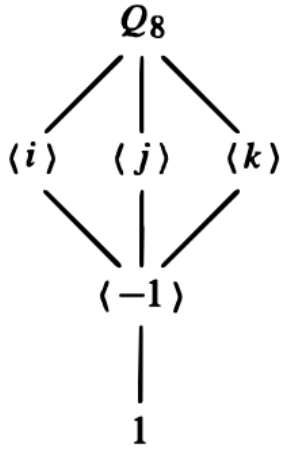


Figure 1.12: The lattice of subgroups of the Quaternion group.

Chapter 2

Quotient groups

2.1 The kernel of a homomorphism

Prototypical example. $Ax = Ay \implies x - y \in \ker A$

.

As you might remember from a linear algebra class, the kernel of a linear transformation (also a homomorphism!) is the set of vectors it sends to the identity (the zero vector). And the kernel was very useful to find the solution set to linear equations. We will see a more general picture of this here.

Definition 2.1. Let $\varphi : G \to H$ be a homomorphism. Then the kernel of φ is defined to be

$$\ker \varphi \equiv \{g \in G : \varphi(g) = 1_H\}$$

$\mathbb{E}$ The fibres of G *induced by* φ consist of the disjoint elements $f_h \equiv \{g \in G : \varphi(g) = h\}$ for $h \in \operatorname{img} \varphi$. Verify that fibres are not groups in general - it is easy to show that the fiber f_{1_H} aka the kernel is the only group among the fibres. Now an important thing: Each fibre is in one-to-one correspondence with its element h and the set of fibres partition G. The big idea: we can *treat each fibre as its element* h to end up with a group 'G *modulo* $\ker \varphi$' of the fibres isomorphic to $\operatorname{img} \varphi$. We'll get there in a bit.

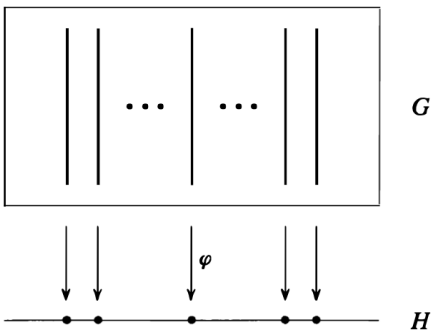


Figure 2.1: The fibres of G induced by φ

We have the following useful results:

Theorem 2.2. *Let $\varphi : G \to H$ be a homomorphism with kernel K. Let the corresponding set of fibres be F. Then we have*

1. *For each fibre $f \in F$: $|f| = |K|$. In fact, $f = xK \equiv \{xk : k \in K\}$ for every $x \in f$.*
2. *F is a group under operation $f_a \star f_b \equiv f_{ab}$.*
3. *$F \cong \operatorname{img} \varphi$.*

Proof.

1. Fix $x \in f$. For every $x' \in f$, $\varphi(x) = \varphi(x') \implies x^{-1}x' \in \ker \varphi$ so that $x' = xk$ for some $k \in K$, thus $f \subseteq xK$. Conversely, every element of the form xk satisfies $\varphi(xk) = \varphi(x) \cdot 1 = \varphi(x)$, or $xk \in f$, so that $xK \subseteq f$, yielding $xK = f$. Noting that $|xK| = |K|$ ($k \mapsto xk$ is an isomorphism) we get $|f| = |K|$, as required.
2. Exercise.
3. Consider the map $f \in F \mapsto \varphi(f) \in \operatorname{img} \varphi$, where $\varphi(f) := \varphi(x)$ for some $x \in f$ (it is well-defined, since the RHS is identical within a fibre). It is left to the reader to verify that this map is an isomorphism from $F \to \operatorname{img} \varphi$; this yields the result.

□

Notice this shows that the solution set of the linear equation system $Ax = b$ is the nullspace tranlated by a fixed element of the solution set - a result you use very often with linear systems.

We have an important corollary:

Corollary 2.3. Let $\varphi : G \to H$ be a homomorphism. Then

$$|G| = |\operatorname{img} \varphi||\ker \varphi|$$

.

As you might have realized, when you set G to a vector space, and φ to a linear transformation $V \to W$, and 'take the logarithm' (aka count the size of a basis/generator set that spans the space instead of counting the size of the space) you get the rank-nullity theorem

$$\dim V = \dim \ker A + \dim \operatorname{img} A = \operatorname{nullity} A + \operatorname{rank} A$$

Try to come up with a proof for it that matches our proof of the general result.

2.1.1 Examples

Example 5.

- The homomorphism $\varphi : \mathbb{Z} \to \mathbb{Z}_n = \{0, \ldots, n-1\}$ defined by $\varphi(z) = z \pmod n$ has kernel $n\mathbb{Z} = \{nz : z \in \mathbb{Z}\}$.
- The homomorphism $\varphi : D_{12} \to D_6$ defined on the generator set of D_{12} as $r_{12} \mapsto r_6$ and $s_{12} \mapsto s_6$ has kernel $\{1, r_{12}^3\}$.

2.2 The Quotient/modulo group

Prototypical example. $\mathbb{Z}/n\mathbb{Z}$ partitions all of $\mathbb{Z}$ into residue classes and treats all elements with residue i as i. $n\mathbb{Z}$ *divides* $\mathbb{Z}$ into classes (fibres) where a, b are in the same class iff $a - b \in n\mathbb{Z}$.

The set of fibres F is a group, formed by identifying elements of G that differ (/are translations) by an element in the kernel as identical. This group is thus given the name 'G modulo $\ker\varphi$' in accordance with the meaning of the object A modulo B - the object formed when treating elements of A as one when their difference is in B.

To keep the notations indicative, we use the notation G/K for the group G modulo K (since its cardinality is $|G|/|K|$!), and so Corollary 2.3 can be rephrased as

$$|G| = |K||G/K|$$

Definition 2.4. Let $\varphi : G \to H$ be a homomorphism with kernel K . The quotient group or factor group, G/K (read G *modulo* K or simply G mod K), is the group whose elements are the fibers of G induced by φ with group operation as defined in the proof of theorem 2.2.

$$G/K \equiv \{f_h \equiv \{g \in G : \varphi(g) = h\} : h \in \operatorname{img}\varphi\}$$

It would be nice to define quotient groups based on the structure of the subgroup $K \leq G$, independent of a particular homomorphism - but keeping with the notion that each element of the quotient group is a subset xK of G. This is our job in the next section.

2.2.1 Cosets and Normal subgroups

We first define the notion of a coset.

Definition 2.5 (coset). For $g \in G$, the left coset of H in G containing g is defined to be the set

$$gH \equiv \{gh \mid h \in H\}$$

Similarly, one defines the right coset of H in G containing g to be $gH \equiv \{gh \mid h \in H\}$.

Remark. In general we can think of the left coset, gH, of H in G as the left translate of H by g. A possible reason for the name 'coset' could because each coset xH is in $1-1$ correspondence with H, and so is a 'x-**co**(-rresponding) **set**' or 'coset' (to H).

The statement set "S partition G" means that S is a collection of disjoint sets with union exactly G. We take the following important observation about cosets:

Proposition 2.6. *The set S_H of left cosets of H in G partition G.*

Proof. Suppose that for some $a \neq b \in G$, we have $aH \cap bH \neq \varnothing$. Pick $c \in aH \cap bH$. This means $c = ah_1 = bh_2$ for some $h_1, h_2 \in H$. Consider $a' = ah \in aH$. Then $a' = bh_2h_1^{-1}h = bh' \in bH$, so $aH \subseteq bH$. Switching a and b we get $bH \subseteq aH$, so $aH = bH$. Thus the set (removing duplicates) of cosets is a collection of disjoint sets. Finally, since for every $a \in G$, $a \in aH$, S_H spans G - and hence forms a partition of G. □

Our goal is to make the set of cosets S_H a group. The operation that we would like is the same one as for quotient groups - the reason being that we can work instead with the *elements* of G instead to perform *operations in* S_H unambiguously. This is akin to working in the group $\mathbb{Z}/7\mathbb{Z}$ but writing equations like $3^3 + 4^3 = 0$ - we are working with elements of $\mathbb{Z}$ that actually *represent* their fibres ($3^3 \to \bar{6}, 4^3 \to \bar{1}, 0 \to \bar{0}$), but working with the elements themselves is simpler (people with a background in number theory can confirm!). Thus, with this motivation, the group operation we are looking for is

$$xH \star yH \equiv (xy)H$$

Will any subgroup H do? After all, we have not mentioned anything abotut H in our definition above. Indeed, we have - $\star$ should be "well-defined". Informally, this means that one should not be able to obtain two distinct values of $uH \star vH$ for any $u, v \in G$ using the rule given by $\star$ - the multiplication of the cosets is not dependent on the representative chosen for the cosets. It is easy to verify that the group operation for quotient groups (the set of cosets of the kernel) is well-defined. Basically, whatever the representatives for cosets f_a, f_b are, the underlying elements a, b in the image of φ do not change. Figure 3.2 makes this clear.

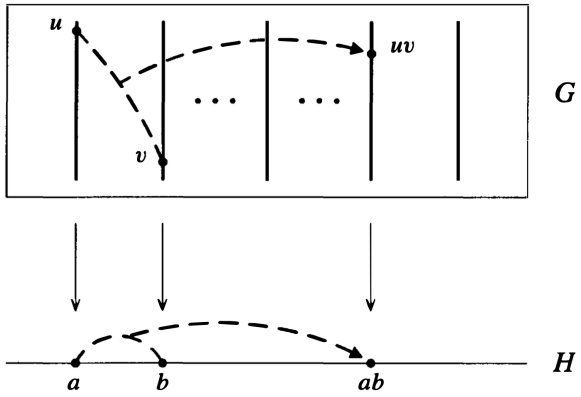


Figure 2.2: Coset multiplication is independent of the representatives u and v chosen for the two cosets.

For a general subgroup to have this property (call such a subgroup normal), notice we must have: For every $u, v, u', v' \in G$ with $uH = u'H$ and $vH = v'H$, we have $(uv)H = (u'v')H$ (that is, the product $uH \star vH$ should get the same value of the identical expression $u'H \star v'H$). Now for some pencil-pushing: Let $a \sim b \equiv aH = bH \iff ab^{-1} \in H$. Suppose that $H \leq G$ is normal. We then have that $u \sim u', v \sim v' \implies uv \sim u'v'$ for every $u, v, u', v' \in G$. That is, for every $u, v, h_1, h_2 \in H$, $uv \sim uh_1vh_2$ so $1 \sim v^{-1}h_1v$ or $v^{-1}Hv \subseteq H \iff Hv \subseteq vH$. Since $|Hv| = |vH|$, we have: for every $v \in G : vHv^{-1} = H$.

By reversing the steps above, it is easy to see that any subgroup H with the latter property has an unambiguous product and so is a group (since G is a group and a coset can be unambiguously represented by an element of G in the product).

Definition 2.7 (Normal Subgroup). A subgroup H of a group G is said to be normal if $gH = Hg$ for all $g \in G$. This is denoted by $H \trianglelefteq G$.

As we see later, gNg^{-1} is the group containing elements of N viewed from a different perspective - which is determined by $g \in G$ - and the subgroups invariant to these changes in perspective are the normal subgroups.

An alternate perspective is that the corresponding left and right cosets of a normal subgroup are always equal. The following theorem is easily established:

Theorem 2.8. *Let* H *be a subgroup of* G*. Then, the following are equivalent:*

(a) $H \trianglelefteq G$.

(b) The set of left cosets of H *in* G *form a group under the operation* $uH \star vH \equiv (uv)H$.

(c) for all $g \in G$, $gHg^{-1} \subseteq H$.

(d) for all $g \in G$, $gH = Hg$.

(e) The normalizer $N_G(H) = G$.

Thus, the subgroups that we can define quotients with (in the nice way that we wanted to) are precisely the normal subgroups. Finally, we have the neat result:

Proposition 2.9. *A subgroup* N *of the group* G *is normal if and only if it is the kernel of some homomorphism.*

The 'if' part is an easy exercise. For the 'only if' part, show that the function $\pi : G \to G/N$ defined by $\pi(g) = gN$ is a homomorphism with kernel N. In fact, the homomorphism above has a special name:

Definition 2.10. Let $N \trianglelefteq G$. The homomorphism $\pi : G \to G/N$ defined by $\pi(g) = gN$ is called the natural projection of G onto G/N. If $\bar{H} \leq G/N$, the *complete preimage* of $\bar{H}$ in G is the preimage of $\bar{H}$ under the natural projection homomorphism.

We now have an "internal" criterion which determines precisely when a subgroup N of a given group G is the kernel of some homomorphism - $N_G(N) = G$.

We may thus think of the normalizer of a subgroup N of G as being a measure of "how close" N is to being a normal subgroup (this explains the choice of name for this subgroup). Keep in mind that the property of being normal is an embedding property, that is, it depends on the relation of N to G, not on the internal structure of N itself (the same group N may be a normal subgroup of G but not be normal in a larger group containing G).

Finally, as already mentioned earlier, Computations in quotient group are typically performed by taking representatives from the various cosets involved.

Before we move on, an important thing to note: *The property "is a normal subgroup of" is not transitive*. For example, in D_8, $\langle s\rangle \trianglelefteq \langle s, r^2\rangle \trianglelefteq D_8$ but $\langle s\rangle \not\trianglelefteq D_8$ ($rsr^{-1} \notin \langle s\rangle$).

2.3 Lagrange and friends

We start with a famous but almost trivial result:

Theorem 2.11 (Lagrange). *Let* H *be a subgroup of a finite group* G*. Then,* $|H|$ *divides* $|G|$*. Further,* $|G|/|H|$ *is the number of distinct cosets of* H *in* G.

For infinite groups, the ratio $|G|/|H|$ does not make sense. To work around this:

Definition 2.12. If G is a group (possibly infinite) and $H \leq G$, the number of left cosets of H in G is called the index of H in G and is denoted $|G : H|$.

We end this section with a flurry of easy results that follow from Lagrange's theorem.

Proposition 2.13. *Let G be a finite group and $x \in G$. Then $x^{|G|} = 1_G$.*

Proof. $|\langle x \rangle|$ divides $|G|$. □

Proposition 2.14. *If G is a group of prime order p , then G is cyclic, hence $G \cong \mathbb{Z}_p$.*

Proof. Take $x \neq 1$ (so $\langle x \rangle \neq \{1\}$), then $p = |G| = |\langle x \rangle| \implies G = \langle x \rangle$. □

Is the converse to Lagrange's theorem true? That is, if integer m divides $|G|$, then does there exist subgroup H of G with $|H| = m$? Not in general. Some partial variants are true, and the full variant is true for (finite) abelian groups.

Theorem 2.15 (Cauchy). *Let G be a finite group and p a prime, such that p divides $|G|$. Then G has an element x with order p.*

Proof. Consider the set $G_p \equiv \{(x_1, \ldots, x_k) : x_i \in G \text{ and } \prod_i x_i = 1_G\}$. The relation $\sim$ on G_p defined by $\mathbf{x} \sim \mathbf{x}'$ iff $\mathbf{x}'$ can be obtained from $\mathbf{x}$ by a cyclic permutation is an equivalence. The equivalence classes under $\sim$ have size either 1 or p, since the size of each class divides p. Equivalence classes of size 1 are of the form $(x, x, \ldots, x)$ with $x^p = 1$. Thus $|G_p| = k + pk'$ where $k > 0$ - since $(1, \ldots, 1)$ is a class of size 1 - is the number of classes with size 1, and k' the number of classes with size p. Since p divides $|G_p| = |G|^{p-1}$, $p|k$ and so there exists $x \neq 1$ with $x^p = 1$. It is easy to see that the order of x must also be p, as required. □

The proof actually shows the existence of p (since $k \geq p$) distinct elements x (and thus subgroups $\langle x \rangle$) with order p.

2.3.1 The product of two subgroups

We look at subsets of the form $HK = \{hk : h \in H, k \in K\}$ where $H, K \leq G$. Clearly, if we let $H \vee K$ be the meet of subgroups H, K then $HK \subseteq H \vee K$. The containment is an equality precisely when HK is a subgroup.

Theorem 2.16.

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

Proof. The key idea is the representation of HK as a union of a collection of cosets of K:

$$HK = \cup_{h \in H} hK \tag{2.1}$$

$|HK| = |K| \times$(the number of distinct cosets in $S \equiv \{hK : h \in H\}$). The latter is the number of classes in the equivalence relation $\sim$ on H defined by $h \sim h'$ iff $hK = h'K$. One can work out that

$hK = h'K \iff hh^{-1} \in H \cap K \iff h(H \cap K) = h'(H \cap K)$, so the classes of $\sim$ are same as those of the standard equivalence relation induced by the cosets of $H \cap K$ in H and are thus $|H|/|H \cap K|$ in number. The result follows. □

When is HK a subgroup? The following (easy) proposition answers that.

Proposition 2.17. *Let* $H, K \leq G$. *Then* $HK \leq G$ *iff* $HK = KH$.

An easy *sufficient* condition for HK to be a subgroup follows from the above:

Corollary 2.18. Let $H, K \leq G$ with $H \leq N_G(K)$. Then $KH \leq G$.

2.4 The Isomorphism Theorems

Well, the fundamental theorems regarding isomorphisms between quotient groups.

2.4.1 The first theorem: the image is the quotient

We've already shown the first theorem (see Theorem 2.2):

Theorem 2.19 (The first isomorphism theorem). *If* $\varphi : G \to H$ *is a homomorphism, then*

- $\ker \varphi \trianglelefteq G$.
- $\operatorname{img} \varphi \cong G/\ker \varphi$.

We immediately get $|G : \ker \varphi| = |\operatorname{img} \varphi|$.

2.4.2 The second theorem: Diamonds in the lattice

Theorem 2.20. *Let* $H, K \leq G$ *with* $H \leq N_G(K)$ *additionally. Then*

- $H \vee K = HK \leq G$.
- $K \trianglelefteq HK$.
- $H \cap K \trianglelefteq H$.
- $HK/K \cong H/H \cap K$.

Proof.

- Follows from Corollary 2.18.
- For every element $hk \in HK$, we have $(hk)K(hk)^{-1} = hKh^{-1} = K$.
- For each $h \in H$, obviously $h(H \cap K)h^{-1} \subseteq H$. Moreover, $h(H \cap K)h^{-1} \subseteq hKh^{-1} = K$. Thus, $h(K \cap H)h^{-1} \subseteq H \cap K$ for every $h \in H$ establishing $H \cap K \trianglelefteq H$.

- Notice that the elements hkK of HK/K are exactly the cosets of K in H. The claimed statement is essantially just a rephrasing of the fact (we saw this in Theorem 2.16) that the cosets of K in H are exactly the cosets of $H \cap K$ in H. The formal proof is left as an exercise - the bijection is $\varphi : hK \in HK/K \mapsto h(H \cap K) \in H/H \cap K$.

□

An alternate (and elegant) (and I believe equivalent) proof of the last two parts is to apply the first isomorphism theorem to the (surjective) homomorphism $\varphi : H \to HK/K$ defined by $\varphi(h) = hK$.

This theorem is also called the diamond theorem because:

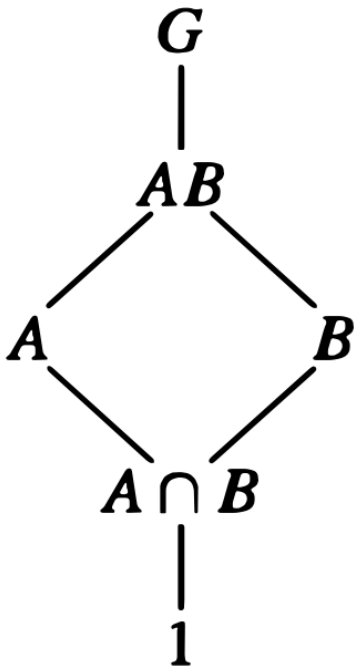


Figure 2.3: The diamond in the second theorem

2.4.3 The third theorem: ignore the modulus

We've seen that quotient groups G/H "behave like G, except that some elements are equal". The third theorem further reinforces that notion, showing that the base (modulus) of the quotient group can be "cancelled" in a quotient of quotient groups.

Theorem 2.21. *Let* $K, H \trianglelefteq G$ *and* $H \leq K$. *Then* $H \trianglelefteq K$. *Let* $\tilde{K} \equiv K/H, \tilde{G} \equiv G/H$ *Then* $\tilde{K} \trianglelefteq \tilde{G}$ *and*

$$\tilde{G}/\tilde{K} \cong G/K$$

Proof. It is an easy exercise to show the first two claims. For the third, consider the function $\varphi : \tilde{G}/\tilde{K} \mapsto G/K$ defined by $\varphi(\tilde{g}\tilde{K}) = gK$, where g is any representative for $\tilde{g}$. Is this well-defined? That is,

1. for each g, g' with $gH = g'H$, do we have $gK = g'K$? Of course, since $h \leq K$.

2. for each $\tilde{g}, \tilde{g}'$ with $\tilde{g}\tilde{K} = \tilde{g}'\tilde{K}$, and g, g' respective representatives of $\tilde{g}, \tilde{g}'$, do we have $gK = g'K$? Yes. $\tilde{g}\tilde{K} = \tilde{g}'\tilde{K} \implies \tilde{g}\tilde{g}'^{-1} = (gg'^{-1})H \in \tilde{K} = K/H \implies gg'^{-1} \in K \implies gK = g'K$.

Is it surjective? obviously. Is it injective? Yes: let gK be obtained as $\varphi(\tilde{g}\tilde{K})$ and $\varphi(\tilde{g}'\tilde{K})$. Then g is a representative of both $\tilde{g}$ and $\tilde{g}'$, so $\tilde{g} = \tilde{g}'$.

Most importantly, is it an homomorphism? $\varphi(\tilde{g}\tilde{K} \star \tilde{g}'\tilde{K}) = \varphi((\tilde{g}\tilde{g}')\tilde{K}) = \varphi(((gg')H)\tilde{K}) = gg'K = gK \star g'K = \varphi(\tilde{g}\tilde{K}) \star \varphi(\tilde{g}'\tilde{K})$, so yes. □

Again, one can prove it by appealing to the first isomorphism theorem applied to the homomorphism $\varphi : G/H \to G/K$ defined by $\varphi(gH) = gK$.

Chapter 3

Group actions

Definition 3.1. A group *action* of a group G on a set A is a map $\cdot$ from $G \times A \to A$ satisfying

- $g_1 \cdot (g_2 \cdot a) = (g_1 \star g_2) \cdot a$ for every $a \in A, g_1, g_2 \in G$.
- $1 \cdot a = a$ for every $a \in A$.

Essentially, you would like composing $\cdot$ to act like a composition of G instead (analogous to how the composition of two linear transformations is the linear transformation with matrix equal to the product of the two transformations), and ensuring that for every g, $g\cdot$ can be inverted (by none other than $g^{-1}\cdot$). One can also view the first restriction as a "multiplicativity condition" - defining $\pi : G \to (A \to A)$ by $\pi(g) = g\cdot$, we require that $\pi(g_1) \circ \pi(g_2) = \pi(g_1 \circ g_2)$.

An interesting point: note than each function $g\cdot : A \to A$ is but a permutation σ_g on A, and the function $g \mapsto \sigma_g$ is a homomorphism $G \to S_A$. The "reverse" is also true: any homomorphism $\phi : G \to S_A$ induces group action $\cdot : G \times A \to A$ defined by $g \cdot a = \phi(g)(a)$. Thus the set of homomorphisms $G \to S_A$ (called the set of permutation representations of G) and group actions of G on A are in bijection.

A few more definitions are in order.

Definition 3.2. Let $\cdot$ be an action of G on A, and let ϕ be the associated homomorphism $G \to S_A$. Then we say

- the kernel of $\cdot$ is the set $\{g \in G : ga = a \, \forall a \in A\} \equiv \ker \phi$.
- The orbit of $a \in A$ in G is the set $O_a \equiv \{g \cdot a : g \in G\} \subseteq A$.
- The stabilizer of $a \in A$ in G is the set $G_a \equiv \{g \in G : ga = a\}$.
- $\cdot$ is said to be faithful if its kernel is the identity.

We have the following useful lemma:

Lemma 3.3. *For each $a \in A$, we have $|O_a| = |G : G_a|$, or $|O_a||\mathrm{stab}(a)| = |G|$.*

Proof. Note that $h \in gG_a \iff g^{-1}h \in G_a \iff ha = ga$. So the elements of $G : G_a$ uniquely partition the possible images $g \cdot a$, $g \in G$ thus $|O_a| = |G : G_a|$. □

Exercise. If $G_a \trianglelefteq G$, then O_a is a group under (well-defined) operation $ga \star ha = (gh)a$ with $O_a \cong G/G_a$.

An action $\cdot$ is transitive if there is only one orbit; i.e. for every $a, b \in A$, $O_a = O_b$ or in particular there is $g \in G$ with $a = gb$. A transitive action is thus trivially surjective.

An action is faithful if its kernel is the identity. This is equivalent to the associated homomorphism $G \to S_A$ being injective.

Another way to look at orbits:

Proposition 3.4. *Consider the relation $a \sim b$ if $\exists g : ga = b$ on A. It is an equivalence. The class containing a is precisely O_a.*

This also establishes a proof of the fact that a transitive action is surjective.

We now see some examples of groups acting on action sets constructed from the group itself.

3.1 Groups acting on themselves by left multiplication

The action of G on $A = G$ by left multiplication, i.e. $g \cdot a = ga$ is a valid action. Verify that it is transitive and faithful. The kernel is trivial, and the stabilizer of a is $\{1\}$.

Theorem 3.5 (Cayley's theorem). *Every group G is isomorphic to a subgroup of S_G.*

Proof. Consider the action of G on G by left multiplication and the associated homomorphism $\phi : G \to S_G$. Since $\ker \phi = \{1\}$, $G \cong G/\ker \phi \cong \operatorname{img} \phi \leq S_G$. □

Next, we consider generalizing the action above to allow A to be the set of cosets of a subgroup H of G (what we did above was effectively the case $H = \{1\}$).

We define the action of G on A by $g \cdot (aH) = (ga)H$. This is well-defined since if $aH = bH$, then $b = ah \implies gb = (ga)h$ for some $h \in H$, so $gaH = gbH$.

The action is transitive, and the stabilizer of aH is aHa^{-1}. The kernel is thus $\cap_{g \in G} gHg^{-1}$.

Note the following remarkable fact: if H is normal, all stabilizers are identical and equal to H.

We now take another equivalent condition for normality:

Proposition 3.6. *Let $N \leq G$. Then*

$$N \trianglelefteq G \iff N = \cap_{g \in G} gNg^{-1}$$

Proof. (Hint) Note that $\cap_{g \in G} gNg^{-1} \leq N$. □

We then get the following useful result:

Proposition 3.7. *Let $H \leq G$ and $\cdot$ be the action of G on the cosets of H. Then the kernel of $\cdot$, i.e. $\cap_{g \in G} gHg^{-1}$, is the largest normal subgroup of G contained in H and is called the core of H in G.*

Proof. The kernel is obviously normal. Let $N \trianglelefteq G$, $N \leq H$. Then $N = \cap_{g \in G} gNg^{-1} \leq \cap_{g \in G} gHg^{-1}$. □

Another useful result:

Proposition 3.8. *If G is finite of order n, and p is the smallest prime dividing n, then every subgroup of index p is normal.*

Proof. Consider such a subgroup $H \leq G$. Consider the kernel K of the action of G on the cosets of H (Let associated homomorphism be ϕ). By the first isomorphism theorem, $G/K \cong \operatorname{img}\phi \leq S_{G/H}$, so by Lagrange, $|G/K|$ divides $|G/H|! = p!$, hence $|G/K|$ divides $\gcd(p!, n) = p$. Hence, $|H : K| = |G : K|/|G : H|$ divides 1, so $H = K$. □

3.2 Groups acting on themselves by conjugation

We now consider the action of G on $A = G$ by conjugation, i.e. $g \cdot a = gag^{-1}$. Verify that it is a valid action. The kernel is the center $Z(G)$, and the stabilizer of a is the centralizer $C_G(a)$.

The orbits under this action are called, for obvious reasons, the conjugacy classes of G. $a, b \in G$ are in the same conjugate class if for some $g \in G$, we have $b = gag^{-1}$, that is, if a and b are conjugate in G.

Theorem 3.9 (Class equation). *Let G be a finite group. Then*

$$|G| = |Z(G)| + \sum_{i=1}^{n} |G : C_G(a_i)|$$

where $a_1, \ldots, a_n$ are representatives of the conjugacy classes of G not in $Z(G)$.

Proof. Each element of $Z(G)$ is its own conjugacy class, while the rest of G is partitioned into conjugacy classes not contained in $Z(G)$. The size of each conjugacy class is the index of its centralizer (Lemma 3.3). Summing up the sizes of all conjugacy classes yields the result. □

Corollary 3.10. If $|G| = p^\alpha$ for some prime p, then $Z(G) \neq \{1\}$. In fact, $|Z(G)| \equiv 0 \pmod{p}$.

Proof. Since $|G : C_G(a_i)|$ divides $|G|$, it must be a power of p. Hence, from the class equation, $|Z(G)| \equiv 0 \pmod{p}$. □

One can generalize the action of G on G by conjugation to an action of G on the set of subgroups of G - $g \cdot S \equiv gSg^{-1} = \{gsg^{-1} : s \in S\}$. This is a valid action, and the stabilizer of S is the *normalizer* $N_G(S)$. The kernel is the intersection of all normalizers of subgroups of G. Since the kernel is normal and contains all normal subgroups of G, it is the union of the normal subgroups of G.

This corollary is quite important. Consider the following theorem as an application in classification:

Proposition 3.11. *Suppose $G/Z(G)$ is cyclic. Show that G is abelian.*

Theorem 3.12. *If $|G| = p^2$ for some prime p, then G is abelian. More precisely, G is isomorphic to either $\mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \times \mathbb{Z}_p$.*

Proof. $|Z(G)| \equiv 0 \pmod{p}$, so $|Z(G)| = p$ or p^2 ($|Z(G)| \mid p^2$). If $|Z(G)| = p^2$, then $G = Z(G)$, so G is abelian. If $|Z(G)| = p$, then $|G/Z(G)| = p$, so $G/Z(G)$ is cyclic (prime order implies cyclic), so G is abelian.

Next, if G has an element of order p^2, it is cyclic. Otherwise, all non-identity elements have order p. Consider such an element x and another one $y \in G - \langle x \rangle$. It is easy to see that $\langle x \rangle \cap \langle y \rangle = \{1\}$ and so $\langle x, y \rangle \cong \langle x \rangle \times \langle y \rangle$. Since $|G| = |\langle x, y \rangle|$, $G = \langle x, y \rangle \cong \langle x \rangle \times \langle y \rangle \cong \mathbb{Z}_p \times \mathbb{Z}_p$. □

One last result to conclude this section:

Proposition 3.13. *Every normal group is the union of conjugacy classes. That is, if $H \trianglelefteq G$, then for every conjugate class K of G, either $K \subseteq H$ or $K \cap H = \varnothing$.*

Proof. Suppose $h \in K \cap H$. Then since H is normal, every conjugate of h is in H. Hence, $K \subseteq H$. □

An interesting application of the above:

Corollary 3.14 (C. Jordan, 1870). The alternating group A_5 is simple.

Proof. Verify that the class equation for A_5 is $60 = 1 + 12 + 12 + 15 + 20$. Since every normal subgroup is a union of conjugacy classes - including the class $\{e\}$ - its order is a sum of 1 and some of the numbers $12, 15, 20$. It is easy to see that the only way for the order to divide 60 is when the order is 1 or 60. Hence, A_5 has no non-trivial normal subgroups. □

3.2.1 Conjugation in the permutation group S_n

Straightforward stuff - just note that if $\sigma(a) = b$, then $\tau\sigma\tau^{-1}(\tau(a)) = \tau(b)$.

Proposition 3.15. *Let $\sigma, \tau \in S_n$, and suppose σ has the cycle decomposition*

$$\sigma = (a_1 \dots a_{k_1})(a_{k_1+1} \dots a_{k_2}) \dots (a_{k_{r-1}+1} \dots a_{k_r})$$

Then $\tau\sigma\tau^{-1}$ has the cycle decomposition

$$\tau\sigma\tau^{-1} = (\tau(a_1) \dots \tau(a_{k_1}))(\tau(a_{k_1+1}) \dots \tau(a_{k_2})) \dots (\tau(a_{k_{r-1}+1}) \dots \tau(a_{k_r}))$$

that is, $\tau\sigma\tau^{-1}$ is obtained from σ by replacing each entry a in the cycle decomposition for σ by $\tau(a)$.

Definition 3.16. Suppose $\sigma \in S_n$ has cycles of length $n_1 \leq n_2 \cdots \leq n_r$ (including 1-cycles), the integers $n_1, \dots, n_r$ are called the cycle type of σ.

Corollary 3.17. Two permutations in S_n are conjugate iff they have the same cycle type.

Corollary 3.18. The number of conjugacy classes in S_n = the number of partitions of n.

Proof. Follows from a bijection between the set of partitions of n and the set of cycle types of permutations in S_n. □

Exercise. [The size of each conjugacy class] Let $\sigma \in S_n$. Let $m_1, \ldots, m_s$ be the distinct integers in the cycle type of σ, with m_i occurring k_i times. Then show that the size of the conjugacy class of σ is

$$\frac{n!}{\prod_{i=1}^{s}(m_i^{k_i} k_i!)}$$

3.3 Automorphisms

Definition 3.19. An automorphism of a group G is an isomorphism $G \to G$. The set of automorphisms of a group is called the automorphism group, denoted $\mathrm{Aut}(G)$.

Verify that $\mathrm{Aut}(G)$ is a group under function composition. Since an automorphism is an element of S_G, $\mathrm{Aut}(G) \leq S_G$. Automorphisms are precisely those permutations of G satisfying $\sigma(ij) = \sigma(i)\sigma(j)$ for all $i, j \in G$.

Conjugation is an example of an automorphism: $h \mapsto ghg^{-1}$ is an automorphism of G for every $g \in G$. We discuss this in a more general context below.

Proposition 3.20. *Let H be normal in G. Consider the action of G by conjugation on H - $g \cdot h = ghg^{-1}$. Then for each g, the function $g\cdot$ (i.e. $h \mapsto ghg^{-1}$) is an automorphism of H. The map $g \mapsto g\cdot$ is a homomorphism $G \to \mathrm{Aut}(H)$ with kernel $C_G(H)$.*

Proof. Trivial. □

Note that the converse, that is, if every G-conjugation is an automorphism of H, then H is normal in G, is also true.

Corollary 3.21. Let $H \leq G$. Then $N_G(H)/C_G(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$. In particular, $G/Z(G)$ is isomorphic to a subgroup of $\mathrm{Aut}(G)$.

Proof. Applying the above proposition to $G = N_G(H), H = H \trianglelefteq N_G(H)$ gives us $N_G(H)/C_{N_G(H)}(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$. But $C_{N_G(H)}(H) = C_G(H)$, so $N_G(H)/C_G(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$. The second part follows from the first by taking $H = G$. □

The set of conjugations on G is a normal subgroup of $\mathrm{Aut}(G)$, called the inner automorphism group of G, denoted $\mathrm{Inn}(G)$. One reason for this name is perhaps the fact that these automorphisms are constructed from within the group itself. Another reason is perhaps the fact that the outer automorphism group has a topological interpretation in terms of being "outer".

Exercise. Show that $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$.

The quotient $\mathrm{Aut}(G) / \mathrm{Inn}(G)$ is called the outer automorphism group of G, denoted $\mathrm{Out}(G)$.

Proposition 3.22. $G/Z(G) \cong \mathrm{Inn}(G)$.

Proof. The homomorphism $g \mapsto g\cdot$ from G to $\mathrm{Inn}(G)$ is an isomorphism. It has kernel $Z(G)$. □

One more result and application before we close this section:

Proposition 3.23. *The automorphism group of the cyclic group of order n is isomorphic to $\mathbb{Z}_n^*$.*

Proof. Consider automorphism $\psi \in \mathrm{Aut}(\mathbb{Z}_n)$ and generator x of $\mathbb{Z}_n$. $\psi(x) = x^a$ for some $0 \leq a < n$. Clearly ψ is determined by $\psi(x)$, i.e. by a (since $\psi(x^k) = (x^a)^k = (x^k)^a$ for every $x^k \in \mathbb{Z}_n$). For ψ to be an automorphism, $\operatorname{ord} x = \operatorname{ord} x^a \implies a \in \mathbb{Z}_n^*$. Further, every $a \in \mathbb{Z}_n^*$ defines an automorphism ψ_a by $\psi_a(x) = x^a$. Thus, $\mathrm{Aut}(\mathbb{Z}_n) \cong \mathbb{Z}_n^*$. □

Example 6. Suppose G is a group of order pq, where $p \leq q$ are primes. If $p \nmid q - 1$, then G is abelian.

Proof. if $Z(G) \neq \{1\}$, by Lagrange, $G/Z(G)$ is cyclic, so G is abelian. So let $Z(G) = \{1\} \implies G \cong \mathrm{Inn}(G)$. We derive a contradiction in this case.

Suppose that G has no element of order q. So every non-identity element x has order p, and since $\langle x \rangle \leq C_G(x) < G$, the index of each centralizer is q. The class equation thus gives $pq \equiv 1 \pmod{q}$, a contradiction, thus G has an element x of order q.

Let $H = \langle x \rangle$. H is normal by Proposition 3.8. We have $H \leq C_G(H) \leq G$. The latter cannot be an equality since then $H \leq Z(G)$, impossible. Thus $H = C_G(H)$. Now,

$$p = |G/H| = |N_G(H)/C_G(H)| \text{ divides } |\mathrm{Aut}(H)| = \phi(q) = q - 1,$$

a contradiction. □

3.3.1 Characteristic subgroups

Definition 3.24. A subgroup H of G is said to be characteristic if it is invariant under all automorphisms of G. That is, for every $\sigma \in \mathrm{Aut}(G)$, $\sigma(H) = H$. We denote this by $H \operatorname{char} G$.

Some simple results:

Proposition 3.25.

- *Every characteristic subgroup is normal.*
- *If H is the unique subgroup of G with a particular order, then H is characteristic in G.*
- *(The correct "transitivity" relation). If $K \operatorname{char} H$ and $H \trianglelefteq G$, then $K \trianglelefteq G$. That is, a normal subgroup of a normal subgroup need not be normal, but a characteristic subgroup of a normal subgroup is normal.*

Proof. The first two parts are trivial. For the third, note that any G-conjugation is a H-automorphism, so a K-automorphism, yielding the result. □

3.4 The Sylow theorems

The Sylow theorems are a set of very powerful results that guarantee the existence of subgroups of many orders. They are used heavily in the classification of finite groups.

Definition 3.26. Let G be a group and p a prime.

- A group of order p^k for some $k \geq 1$ is called a p-group. Subgroups of G which are p-groups are called p-subgroups.
- If G is a group of order $p^\alpha m$ where $p \nmid m$, then a subgroup of order p^α is called a Sylow p-subgroup of G. Essentially, it is a p-subgroup of maximal order.
- The set of Sylow p-subgroups of G is denoted $\mathrm{Syl}_p(G)$ and the number of Sylow p-subgroups of G is denoted $n_p(G)$ (or just n_p if G is clear from context).

Theorem 3.27 (Sylow I). *Let G be a group with*

$$|G| = p^e m$$

where $\gcd(p, m) = 1$. Then G has a subgroup H such that

$$|H| = p^e$$

Proof. We approach this using orbits and stabilizers of a well-chosen group action. Let S be the set of subsets (not necessarily groups) of G of size p^e. Then it can be seen (by computing the index of p in each factorial, for example) that

$$|S| = \binom{n}{p^e} \not\equiv 0 \pmod{p}$$

We also have from the partition into orbits:

$$|S| = \sum_i |O_i|$$

and since $p \nmid |S|$, there must be some orbit $\theta \subseteq S$ with $\gcd(p, |\theta|) = 1$.

Let H be the stabilizer of some $x \in \theta$. We have $|H||\theta| = |G| = p^e m$, and since $\gcd(p^e, |\theta|) = 1$, $p^e \mid |H|$. To show the reverse, we use the following lemma:

Lemma 3.28. *Suppose subgroup H is in the stabilizer of subset U. Then $|H|$ divides $|U|$.*

Proof. We have for every $h \in H$: $hU = U$. So, for every $u \in U$ we have $Hu \subseteq U$. Hence these sets Hu, namely the right cosets of H in U, partition U. Since each coset has size $|H|$, we have $|H|$ divides $|U|$. □

Applying the above lemma to the case of $H = H$ and $U = x$, we have $|H|$ divides $|x| = p^e$. Thus $|H| = p^e$, and since H is a stabilizer, $H \leq G$, as needed. □

Theorem 3.29 (Sylow II). *Given any subgroup* $K \leq G$ *with* $|K| = p^d, 0 \leq d \leq e$, *and any Sylow subgroup* H *of* G, *there is* $g \in G$ *such that* $K \leq gHg^{-1}$.

Proof. The proof is of similar flavour - we use orbits and stabilizers. We run a quick calculation: we want g such that for each $k \in K$, we have $g^{-1}kg \in H$, or $kgH = gH$. That is, we are looking for an orbit of size one in the action of K on the cosets of H in G by left multiplication - this is the action we look at.

As usual, we have the decomposition into orbits:

$$|G : H| = \sum_i |O_i|$$

and since $\gcd(p, |G : H| = m) = 1$, there must be some orbit θ with $\gcd(p, |\theta|) = 1$. Also, we have $|\theta|$ divides $|K| = p^d$, so $|\theta| = 1$ - the orbit of size one that we were looking for. The result follows. □

Corollary 3.30. Any two Sylow p-subgroups of G are conjugate.

Proof. Exercise. □

Theorem 3.31 (Sylow III). *Let* G *be a group with* $|G| = p^e m$ *where* $\gcd(p, m) = 1$. *Let* t *be the number of Sylow* p*-subgroups of* G. *Then*

1. $t \mid m$.
2. $t \equiv 1 \pmod{p}$.

Proof.

1. Again, we must look at an action. What better action set to choose than the set Y of Sylow subgroups itself - we have to get the size of this set in somehow. The group can be G. And from Corollary 3.30, conjugation is an obvious choice for the type of action - there is only one orbit. The orbit decomposition is simply $|Y| = |O_1|$, with $|O_1||\text{stab}(y)| = p^e m$ for some $y \in Y$. Here's the cool part: $\text{stab}(y) = \{g \in G : gyg^{-1} = y\}$ is the normalizer of $y \leq G$. And so $y \leq N(y) = \text{stab}(y) \rightarrow p^e = |y| \mid \text{stab}(y)$. So $p^e m = |Y|p^e \cdot$ hence $|Y|$ divides m.

2. You know the drill. The action space, since we care about $|Y|$, is of course, Y. The group, however, is different - we use a Sylow p-subgroup H. The action is conjugation again. The orbit decomposition is

$$|Y| = \sum_i |O_i|$$

Since the size of each orbit divides $|H| = p^e$, each orbit is a power of p (possibly 1) and so

$$|Y| \equiv \text{number of size-one orbits} \pmod{p}$$

Consider a size-one orbit, say of $H' \in Y$. The corresponding stabilizer is, of course, contained in the normalizer $N(H')$ of H'. We shall next require the following lemma:

Lemma 3.32. *Let H' be a Sylow p-subgroup. Then the only Sylow p-subgroup of G contained in $N(H')$ is H' itself.*

Proof. Suppose H is a Sylow p-subgroup of G contained in $N(H')$. Since $N(H')$ is a subgroup of G and $p^e \mid |N(H')|$ since $H' \leq N(H')$, the exponent of p in $|N(H')|$ is exactly e. So, H, H' are Sylow p-subgroups of $N(H')$.

By Corollary 3.30,

$$\exists n \in N(H') \text{ with } H = nH'n^{-1}.$$

But by definition, $nH'n^{-1} = H'$, so $H = H'$. □

Since the stabilizer of H' is H itself, we have $H \leq \text{stab}(H') \leq N(H')$, so by the lemma $H' = H$. Hence, there is only one size-one orbit (precisely the orbit of $H \in Y$), and so $|Y| \equiv 1 \pmod{p}$.

□

Proposition 3.33. *Let P be a Sylow p-subgroup of G. Then the following statements are equivalent:*

1. *P is the unique Sylow p-subgroup of G.*
2. *$P \trianglelefteq G$.*
3. *P char G.*
4. *All subgroups generated by elements of p-power order are p-groups, i.e. if $X \subseteq G$ with $|x|$ a power of p for each $x \in X$, then $\langle X \rangle$ is a p-group.*

Proof. The nontrivial proof is $(1) \iff (4)$.

- $(1) \implies (4)$: Take $x \in X$. Then $\langle x \rangle$ has order $|x|$, so by Sylow II there exists $g \in G$ with $x \in gPg^{-1} = P$. So $X \subseteq P$, hence $\langle X \rangle \leq P$. Thus $\langle X \rangle$ is a p-group.
- $(4) \implies (1)$: Consider X to be the union of all Sylow p-groups of G. Since every $x \in X$ has order a power of p, by (4), $\langle X \rangle$ is a p-subgroup. By Sylow II and Corollary 3.30, there is a Sylow p-subgroup P with $\langle X \rangle \leq P$. But by definition, $P \subseteq X \subseteq \langle X \rangle$ so $P \leq \langle X \rangle$. Equality is forced, yielding (1).

□

Exercise. Let G be an abelian group.

- G has a unique Sylow p-subgroup P for each p.
- This unique p-subgroup consists of precisely the elements x with order a power of p.

Chapter 4

A few odds and ends

We touch upon some interesting results in group theory, to finish.

4.1 The direct product

Definition 4.1. Let $G_1, G_2, \ldots, G_n$ be groups with group operations $\star_1, \star_2, \ldots, \star_n$. The **direct product** of these groups is the set

$$G_1 \times G_2 \times \cdots \times G_n = \{(g_1, g_2, \ldots, g_n) \mid g_i \in G_i\}$$

with the operation

$$(g_1, g_2, \ldots, g_n) \star (h_1, h_2, \ldots, h_n) = (g_1 h_1, g_2 h_2, \ldots, g_n h_n)$$

Similarly, the direct product of groups $G_1, G_2, \ldots$ with group operations $\star_1, \star_2, \ldots$ is the set of all sequences $(g_1, g_2, \ldots)$ with $g_i \in G_i$ with the operation

$$(g_1, g_2, \ldots) \star (h_1, h_2, \ldots) = (g_1 \star_1 h_1, g_2 \star_2 h_2, \ldots)$$

Example 7.

- $\mathbb{R} \times \mathbb{R} \times \cdots \times \mathbb{R} \equiv \mathbb{R}^n$ is the familiar euclidean n-space with usual vector addition:
$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n)$$
- $\mathbb{Z} \times \mathbb{Z}$ is the group of lattice points in the plane with co-ordinate wise addition as the operation.

Exercise. Prove that the direct product of groups is a group of order $|G_1||G_2|\ldots|G_n|$. (if any G_i is infinite, so is their direct product)

Exercise. Show that if the factors of a direct product are rearranged, the resulting group is isomorphic to the original group.

The next proposition shows that a direct product contains an *isomorphic* copy of each factor:

Proposition 4.2.

1. *Let* $G_1, G_2, \ldots, G_n$ *be groups and* $G = G_1 \times G_2 \times \cdots \times G_n$ *be their direct product. Then*

$$G_i \cong \{(1, \ldots, 1, g_i, 1, \ldots, 1) : g_i \in G_i\} \leq G.$$

Further, if we identify G_i *with* $\{(1, \ldots, 1, g_i, 1, \ldots, 1) : g_i \in G_i\}$*, then* $G_i \trianglelefteq G$ *and*

$$G/G_i \cong G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n.$$

2. ***Projection homomorphisms****. The map* $\pi_i : G \to G_i$ *defined by* $\pi_i(g_1, g_2, \ldots, g_n) = g_i$ *is a surjective homomorphism with*

$$\ker \pi_i = G_1 \times \cdots \times G_{i-1} \times \{1\} \times G_{i+1} \times \cdots \times G_n \cong G/G_i$$

.

3. *With the identification as in part* 1*, if* $x \in G_i$ *and* $y \in G_j$ *with* $i \neq j$*, then*

$$xy = yx$$

.

Proof. We prove the first part. The rest are left as exercises.

The first claim in part 1 follows from the function $\phi : G_i \to G$ defined by

$$\phi(g_i) \equiv (1, \ldots, 1, g_i, 1, \ldots, 1)$$

that can be verified to be an isomorphism. The second claim follows from the first isomorphism theorem applied to the function $\phi : G \to G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n$ defined by

$$\phi((g_1, \ldots, g_n)) \equiv (g_1, \ldots, g_{i-1}, 1, g_{i+1}, \ldots, g_n)$$

which can be verified to be a surjective homomorphism with kernel G_i (under the identification for G_i mentioned in the statement of part 1). □

4.2 The fundamental theorem of finitely generated abelian groups

Definition 4.3. A group G is **finitely generated** if there exists a finite set $S \subset G$ such that every element of G can be written as a finite product of elements of S and their inverses.

Example 8.

- $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ is finitely generated by $\{(1, 0), (0, 1)\}$.
- Any finite group is finitely generated ($G = \langle G \rangle$ if G is finite).

Definition 4.4 (The free abelian group of rank r). For $r \in \mathbb{Z}_{\geq 0}$, define $\mathbb{Z}^r \equiv \mathbb{Z} \times \cdots \times \mathbb{Z}$ (r times) with $\mathbb{Z}^0 \equiv \{1\}$.

Theorem 4.5. *[The fundamental theorem of finitely generated abelian groups] Let G be a finitely generated abelian group. Then*

- $$G \cong \mathbb{Z}^r \times \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_s}$$

  for some integers $r, n_1, \ldots, n_s$ with

  1. *$r \geq 0$ and $n_i \geq 2$ for each i.*
  2. *$n_i \mid n_{i+1}$ for each $1 \leq i \leq s-1$.*

- *The expression above is unique: if*

  $$G \cong \mathbb{Z}^{r'} \times \mathbb{Z}_{n'_1} \times \cdots \times \mathbb{Z}_{n'_s}$$

  for some integers $r', n'_1, \ldots, n'_s$ satisfying (1) and (2) above, then $r' = r, s' = s$ and $n'_i = n_i$ for each i.

Definition 4.6. The integer r in Theorem 4.5 is called the free rank or Betti number of G and the numbers $n_1, \ldots, n_s$ are called the invariant factors of G. The representation in Theorem 4.5 is called the invariant factor decomposition of G.

This theorem has a fundamental significance: The study of finitely generated abelian groups is reduced to the study of abelian groups $\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$ - that is, the study of the cyclic groups. These are very well-studied, and thus, one can say a lot about finitely generated abelian groups.

A finitely generated abelian group is finite iff its rank is 0. The order of a finite abelian group is thus simply the product of its invariant factors.

Theorem 4.5 gives us a way of listing all finite abelian groups of a given order n. The classes are in bijection with the set of tuples $(n_1, \ldots, n_s)$ satisfying

1. $n_i \geq 2$ for each i.
2. $n_{i+1} \mid n_i$ for each $1 \leq i \leq s-1$.
3. $n_1 n_2 \ldots n_s = n$.

Consider a finite abelian group with order n, and take prime $p \mid n$. Then $\exists i : p \mid n_i$ and since for every i, $n_i \mid n_1$, $p \mid n_1$. For an application of this observation, suppose that n is a product of distinct primes. Then $n \mid n_1$ and so $s = 1, n_1 = n$ and hence G is cyclic!

4.3 Burnside's lemma

Consider a group G acting on set A. How many orbits are induced? Burnside's lemma provides an exceedingly elegant answer.

In what follows, let i range over the orbits of A. The number of orbits is

$$n_o = \sum_i 1$$

which, at first glance, does not seem to be useful. By the way, writing what you want as a summation of 1s and indicators is very useful. Infact, along with swapping the order of summation, it captures the boilerplate of many double counting arguments.

But consider now the modified representation of 1:

$$1 = \frac{1}{|O_i|} \sum_{a \in O_i} 1 = \sum_{a \in O_i} \frac{1}{|O_a|}$$

where O_a is the orbit of element a (which is O_i). This is exceptionally useful! It gives us

$$n_o = \sum_i \sum_{a \in O_i} \frac{1}{|O_a|} = \sum_{a \in A} \frac{1}{|O_a|}.$$

This is an expression purely dependent on the orbits of each element a! We can rewrite it (using Lemma 3.3) as

$$n_o = \frac{1}{|G|} \sum_{a \in A} |\operatorname{stab}(a)|.$$

Cool, but can we do better? That is, can we express n_o in terms of the group G? Indicators come to our rescue (aka double counting). An indicator for predicate $P(x)$ is a function $\mathbb{1}_P : \mathcal{X} \to \{0, 1\}$ defined by $\mathbb{1}_P(x) = 1$ if $P(x)$ is true and 0 otherwise.

We have

$$|\operatorname{stab}(a)| = \sum_{g \in G} \mathbb{1}_{[ga=a]}.$$

So

$$n_o = \frac{1}{|G|} \sum_{g \in G} \sum_{a \in A} \mathbb{1}_{[ga=a]} = \frac{1}{|G|} \sum_{g \in G} |A^g|,$$

where $A^g \equiv \{a \in A : ga = a\}$ is the set of elements of A fixed by $g \in G$. This is Burnside's lemma.

Theorem 4.7 (Burnside's lemma). *Let G be a finite group acting on a finite set A. Then the number of orbits of A under G is equal to*

$$\frac{1}{|G|} \sum_{g \in G} |A^g|$$

Is the number of orbits of a group action useful? Indeed! The orbit of a is the equivalence class of A identifying elements of A as identical upto an application of a group element to a - and since many groups indicate the set of symmetries of an object, the number of distinct orbits is the number of *distinct* constructable objects (from a set of possibilities A) under the symmetries of the group. Let's see an example.

Definition 4.8 (Necklace). A k-ary necklace of length n is an equivalence class of n-character strings over an alphabet of size k, taking all rotations as equivalent. Less formally, it is the number of distinct necklaces containing n beads that can be made from beads of k different colors, with the constraint that two necklaces are equivalent if one can be rotated to become the other.

The necklace counting problem, then, is to evaluate for given n and k the number of k-ary necklaces of length n.

Exercise. Solve the necklace problem by hand for

- $n = 3, k = 2$.
- $n = 6, k = 2$.
- $n = 6, k = 3$.

As you can see, it gets very tedious to compute by exhaustive case analysis requiring a lot of examination of necklaces to check for equality.

Abstracting the symmetry of the problem into the cyclic group $G = \langle r | r^n = 1 \rangle$ (also the rotation part of the Dihedral group D_{2n}), the problem reduces (convince yourself!) to the number of orbits under the action of G on the set $A = S_n^k$ of n-character strings over an alphabet of size k. It remains, by Burnside's lemma, to evaluate the size of the sets A^g.

Consider $g = r^t$ and let $a = a_1 a_2 \dots a_n$ be an action fixed by g. We have $g \cdot a = a_{t+1} a_{t+2} \dots a_{t+n}$ (where indices are reduced modulo n). Since $g \cdot a = a$, we must have $a_i = a_{t+i}$ for each i. The set of such actions a is precisely the set of n-length string over a k-sized alphabet invariant under cyclic shifts of length t - which is the same as the set of n-length strings over a k-sized alphabet invariant under cyclic shifts of length $\gcd(n, t)$ (why?), where we take $\gcd(n, 0) = n$. Thus,

$$|A^{r^t}| = k^{\gcd(n,t)},$$

and by Burnside's lemma, we have the general solution to the necklace problem:

$$N_k(n) = \frac{1}{n} \sum_{t=0}^{n-1} k^{\gcd(n,t)}.$$

A double counting argument gives us an alternate form of the solution:

$$N_k(n) = \frac{1}{n} \sum_{d|n} \varphi(d) k^{n/d}$$

where φ is the Euler totient function ($\varphi(n) \equiv |\mathbb{Z}_n^*|$).

Definition 4.9 (Bracelet). A k-ary bracelet of length n is an equivalence class of n-character strings over an alphabet of size k, taking all rotations and reflections as equivalent. Less formally, it is the number of distinct bracelets containing n beads that can be made from beads of k different colors, with the constraint that two bracelets are equivalent if one can be rotated or reflected to become the other.

The bracelet problem is to compute the number of k-ary bracelets of length n.

Exercise. Show that the solution to the bracelet problem is

$$B_k(n) = \begin{cases} \frac{1}{2}N_k(n) + \frac{1}{4}(k+1)k^{n/2} & \text{if } n \text{ is even} \\ \frac{1}{2}N_k(n) + \frac{1}{2}k^{(n+1)/2} & \text{if } n \text{ is odd} \end{cases}$$

Can we reduce the 'number of fixed points' in Burnside's lemma to something even simpler to count? The unweighted case of Pólya's enumeration theorem does exactly that.

The idea is the following. Suppose that X and Y are two sets with Y^X denoting the set of functions $f : X \to Y$. Consider G acting on Y^X. What kind of G? Well, for this to work for our necklace case (where A was of the form Y^X - X was the set of character indices $\{1, \ldots, n\}$ and Y the set of k colors), we had a rotation/cyclic group for G with $g \cdot (a_1 \ldots a_n) = (a_{t+1} \ldots a_{t+n})$. Here the function is a taking $i \mapsto a_i$. That is, $(g \cdot a)(i) = a(g(i))$, where g is now treated as a permutation of X taking $i \mapsto i + t$ (that is, we looked at G acting on X and took g's permutation representation). Could we abstract away G and just ask for permutation representations? That would save some trouble for different groups whose permutation representations coincided, because that's all we care about - how they move the indices of the set.

TL;DR: Let G be a subgroup of the symmetric group S_X acting on Y^X.

What is the size of set $|A^g|$? - This was what we wanted to simplify!

Proposition 4.10.

$$|A^g| = |Y|^{c(g)}$$

where $c(g)$ is the number of cycles in the permutation representation of g.

Proof. $|A^g| = \#a : \forall x \in X : a(g(x)) = a(x)$. For each such a, the cycle in g containing x must map to the same value $y \in Y$, and there is no other constraint. □

We thus get the unweighted case of Pólya's enumeration theorem:

Theorem 4.11 (Pólya's enumeration theorem, unweighted case). *Let G be a subgroup of the symmetric group S_X acting on Y^X. Then the number of orbits of Y^X under G is equal to*

$$\frac{1}{|G|}\sum_{g \in G} k^{c(g)}$$

where $c(g)$ is the number of cycles in the permutation representation of g and $k = |Y|$.

Exercise. In the necklace problem, show that $c(r^t) = \gcd(n, t)$. Of course, $c(r^t)$ stands for $c(\tilde{g})$ where $\tilde{g}$ is the permutation representation of r^t.

4.4 The Pólya Enumeration Theorem

Consider setting up weights $w \in \mathbb{N} \cup \{0\}$ for each color (we shall informally call the elements of X beads and the elements of Y colors, in view of the necklace problem) - suppose that the generating function for the number of colors of each weight $w \geq 0$ is

$$f(t) = f_0 + f_1 t + f_2 t^2 + \ldots$$

Suppose we define the weight of an element $\phi \in Y^X$ to be

$$w(\phi) = \sum_{x \in X} w(\phi(x))$$

Essentially, if ϕ represents a possible necklace, its weight is the sum of the weights of each bead's color. Notice that the weight of any element in an orbit is the same (as you might expect with our example of necklaces - rotating doesn't change the total weight of the necklace). We thus define the weight of an orbit to be the weight of any element in it.

The question then is, how many necklaces of weight w are there? (one can think of weight as literal weight, in which case we want the necklaces to be of the same total weight, for example). That is, how many orbits have weight w?

Proposition 4.12 (Weighted Burnside's Lemma). *The answer is*

$$\#_w = \frac{1}{|G|} \sum_{g \in G} |A_{w,g}|$$

where $A_{w,g} = \{\phi \in Y^X : w(\phi) = w, g \cdot \phi = \phi\}$ *is the number of fixed points of* g *in* Y^X *of weight* w.

Proof. This is simple. Start with

$$\#_w = \sum_{a \in A} \mathbb{1}_{[w(a)=w]} \frac{1}{|O_a|}$$

and repeat the proof of Burnside's Lemma. The indicator tags along till the end, when it merges with the indicator for fixed points giving $|A_{w,g}|$. □

We want, again, to cast this in terms of the cycles of G. Let's analyse an element $a \in A$ of $A_{w,g}$ as we did before. As before, the value of a is identical (say y_c) on each cycle c of G. So a satisfies the following conditions:

$$y_c \in Y \ \forall \text{ cycles } c \in C$$
$$\sum_{c \in C} w(y_c)|c| = w$$

where C is the set of cycles of G and $|c|$ is the length of cycle c. The latter condition can be re-written as

$$w = \sum_{i=1}^{n} i \sum_{c \in C_i(g)} w(y_c)$$

where $C_i(g)$ is the set of cycles of length i of G and $n = |X|$. Enumerating the number of such functions a is a standard problem in generating functions, and the answer is given by

$$\#a = [x^w] \left(\prod_{i=1}^{n} f(x^i)^{c_i(g)} \right).$$

Whew. That is a lot to unpack. First the notation. $[x^w]f(x)$ is the coefficient of x^w in the power series $f(x)$ and $c_i(g) = |C_i(g)|$. Why does this work? Well, consider any occurrence of x^w, and let the individual powers of x in the $\sum_i c_i(g)$ generating functions multiplied be

$w_{11}, \dots, w_{1c_1(g)}, w_{21}, \dots, w_{2c_2(g)}, \dots, w_{n1}, w_{nc_n(g)}$ (some of these could be zero, of course). The exponent w_{ij} corresponds to choosing colors of weight w_{ij} for the jth cycle of length i - and together, they account for $i \cdot w_{ij}$ of the weight in a. Thus, we choose $c_i(g)$ weights $\{w_{ij}\}_{j=1}^{c_i(g)}$ for each i, use the power series $f(x^i)$ to count the number of ways to do so - x^i since we must multiply by i to get the weight of the cycle, and multiply them all together to get the total number of ways to choose the weights for a.

So, finally, this emphis $|A_{w,g}|$, albeit much more complicated than the unweighted case (in which $f(t) \equiv k = |Y|$ and $w = 0$). Plugging this value into the weighted Burnside's lemma gives the general Pólya enumeration theorem.

But one more thing: let's isolate the computation within the group and computation with regards to the colors. Consider the cycle index polynomial of G:

Definition 4.13 (Cycle index polynomial). The **cycle index polynomial** of permutation subgroup $G \leq S_X$ is the polynomial

$$Z(G)(t_1, \dots, t_n) = \frac{1}{|G|} \sum_{g \in G} t_1^{c_1(g)} t_2^{c_2(g)} \dots t_n^{c_n(g)}$$

where $n = |X|$ and $c_i(g)$ is the number of cycles of length i in the permutation representation of g.

So the Pólya theorem becomes

$$\#_w = \frac{1}{|G|} \sum_{g \in G} [x^w] \left(\prod_{i=1}^{n} f(x^i)^{c_i(g)} \right) = [x^w] Z(G)(f(x), f(x^2), \dots, f(x^n)).$$

We can actually string all these into the generating function F for the number of orbits of each weight w:

$$F(x) = \sum_{w=0}^{\infty} \#_w x^w = Z(G)(f(x), f(x^2), \dots, f(x^n))$$

This is how the Pólya enumeration theorem is typically written:

Theorem 4.14 (Pólya enumeration theorem). *Let G be a subgroup of the symmetric group S_X acting on Y^X. Then the generating function for the number of orbits of each weight w is given by*

$$F(x) = Z(G)(f(x), \dots, f(x^n))$$

where $f(t)$ is the generating function for the number of colors of each weight w.

The power of the theorem is in the following: once one puts down the cycle polynomial $Z(G)$, one has the answer to the number of orbits for *any* choice of $f(t)$!

Exercise.

- Let C_n be the cyclic group of order n. Show that $Z(C_n)(t_1, \dots, t_n) = \frac{1}{n} \sum_{d|n} \varphi(d) t_d^{n/d}$.

Symbolic Combinatorics is an emerging field that uses the Pólya enumeration theorem to build constructs that can solve enumeration problems almost straight from the definitions of the objects involved.

Bibliography

[1] David S. Dummit, and Richard M. Foote. *Abstract Algebra*. 3rd ed., John Wiley & Sons, 2004.

[2] Nathan Carter. *Visual Group Theory*. The Mathematical Association of America, 2009.

[3] Chen, Evan. *An Infinitely Large Napkin*. 2016. https://web.evanchen.cc/napkin.html.

[4] Joseph A. Gallian. *Contemporary Abstract Algebra*. 9th ed., Cengage Learning, 2017.

[5] MIT Open Courseware: Lecture 23, Student Notes, Algebra I, Fall'21. https://ocw.mit.edu/courses/res-18-011-algebra-i-student-notes-fall-2021/mit18_701f21_lec23.pdf

[6] Burnside's lemma: https://en.wikipedia.org/wiki/Burnside%27s_lemma

[7] Pólya enumeration theorem: https://en.wikipedia.org/wiki/P%C3%B3lya_enumeration_theorem