Group Theory Lecture Notes

Nate Annau

Table of Contents

1. Preliminaries

1.1. Relations

1.1.1. Definition: Relation

A **relation** on a set A is a subset $R \subseteq A \times A$. $a \sim b \Longleftrightarrow (a, b) \in R$. We say that R is

- reflexive if $a \sim a \forall a \in A$
- symmetric if $a \sim b \Longleftrightarrow b \sim a \forall a, b \in A$
- transitive if $a \sim b \land b \sim c \Longrightarrow a \sim c \forall a, b, c \in A$

1.1.2. Definition: Equivalence Relation

An **equivalence relation** is a relation which is reflexive, symmetric, and transitive.

1.1.3. Definition: Equivalence Class

Let R be an equivalence relation on A. The **equivalence class** of $a \in A$ is the set $\{x \in A \mid x \sim a\} = [a]_R = \overline{a}$. Any $c \in [a]_R$ is a **representative** of $[a]_R$.

The set $A/R = \{[a]_R \mid a \in A\}$ is called a **quotient set**. This is the set of equivalence classes (as defined by the equivalence relation R) on the set A.

Reference

1.1.4. Exercise

> $A = \mathbb{R}^2 \setminus \{(0, 0)\}$. Define a relation $\sim$ on A by $(x, y) \sim (z, w) \Longleftrightarrow \exists \lambda \in \mathbb{R}^x$ such that $(x, y) = \lambda(z, w)$. ($\mathbb{R}^x = \mathbb{R} \setminus \{0\}$).
>
> Is this an equivalence relation? What are the equivalence classes and the quotient set?

Solution

Check properties:

- reflexive: $(x, y) = 1(x, y) \forall (x, y) \in A)$
- symmetric: $\forall (x, y), (z, w) \in A$, suppose $(x, y) = \lambda(z, w)$ for some $\lambda \in \mathbb{R}^x$, so $(z, w) = \lambda^{-1}(x, y)$ with $\lambda \in \mathbb{R}^x$
- transitive: $\forall (x, y), (z, w), (s, t) \in A$, if $(x, y) = \lambda_1(z, w)$ and $(z, w) = \lambda_2(s, t)$ for some $\lambda_1, \lambda_2 \in \mathbb{R}^x$, then $(x, y) = \lambda_1\lambda_2(s, t)$ with $\lambda_1\lambda_2 \in \mathbb{R}^x$

Thus this is an equivalence relation on A.

Given some $(x, y) \in A$, $[(x, y)] = \{(s, t) \in A \mid (s, t) = \lambda(x, y) \text{ for some } \lambda \in \mathbb{R}^x\}$ (which is the line through (x, y) and $(0, 0)$). Then the quotient set is the set of lines through (0, 0) in $\mathbb{R}^2$ (this is the same as the projective real line $P^1(\mathbb{R})$).

1.1.5. Definition: Partition

A **partition** of a set A is a collection $\{A_i \mid i \in I\}$ of nonempty subsets of A such that

$$A = \cup_{i \in I} A_i \text{ and } A_i \cap A_j = \emptyset \text{ if } i \neq j.$$

1.1.6. Definition: Relation on Partition

Let $P = \{A_i \mid i \in I\}$ be a partition of A. The relation defined by P on A, denoted R_P, is defined by $a \sim b \iff \exists i \in I$ such that $a, b \in A_i$.

1.1.7. *Theorem*

Let A be a set.

1. If R is an equivalence relation on A, then $P = A/R$ is a partition of A and $R_P = R$.
2. If P is a partition of A, then R_P is an equivalence relation and $A/R_P = P$.

Proof:

1. Let $a \in A$ with R an equivalence relation. Recall $P = A/R = \{[a]_R \mid a \in A\}$ by definition, and since $a \in [a]_R$, we must have $\cup_{a \in A} [a] = A$. Further, since each equivalence class at least contains a, it is nonempty. Now suppose by contradiction $x \in [a], [b]$, two distinct equivalence classes. Then xRa and xRb, so by transitivity and symmetry, aRb, a contradiction. Thus, P is a partition.

   Notice $a \sim b$ in R_P if $\exists i \in I$ such that $a, b \in A_i = [a]_R = \{b \in A \mid a \sim b\} \Leftrightarrow a \sim b$ in R. Thus $R_P = R$.

2. Let P be a partition of A.
   - reflexivity: let $a \in A$ and note $\exists i \in I$ such that $a \in A_i \in P$ so $a \sim a$
   - symmetry: suppose $a \sim b$ for some $a, b \in A$. Thus $\exists i \in I$ such that $a, b \in A_i \in P$. But then $b \sim a$ because sets aren't ordered
   - transitivity: suppose $a \sim b$ and $b \sim c$ for $a, b, c \in A$. Thus exists $i, j \in I$ such that $a, b \in A_i$ and $b, c \in A_j$. Thus $b \in A_i \cap A_j$, but this is only possible if $i = j$ since otherwise it would be empty. Thus $a, c \in A_i$ and $a \sim c$.

   Now let $S \in A/R_P = \left\{[a]_{R_P} \mid a \in A\right\}$. Equivalently, $S = \{b \in A \mid a \sim b\}$ for some $a \in A$ under R_P. Note equivalence relations form partitions and vice versa, and in fact $S = \{a \mid a \in A_i \subseteq A\} \in P$. This satisfies both directions.

□

1.2. Properties of Integers

1.2.1. Definition: Divides

Let $a, b \in \mathbb{Z}$. We say that ***a* divides *b***, written $a \mid b$, if $\exists c \in \mathbb{Z}$ such that $b = ac$.

Properties

- $\forall a \in \mathbb{Z}, a \mid a$ (reflexive)
- $\forall a, b \in \mathbb{Z}$, if $a \mid b$ and $b \mid a$ then $|a| = |b|$ (symmetric)
- $\forall a, b, c \in \mathbb{Z}$, if $a \mid b$ and $b \mid c$, then $a \mid c$ (transitive)
- $\forall d, a, b, m, n \in \mathbb{Z}$ if $d \mid a$ and $d \mid b$, then $d \mid ma + nb$ (linearity)

Transitivity proof: $a \mid b \Rightarrow \exists n \in \mathbb{Z}$ such that $an = b$ and $b \mid c \Rightarrow \exists m \in \mathbb{Z}$ such that $bm = c$. Then $a(nm) = c \Rightarrow a \mid c$. Notice logically this means $a \nmid c \Rightarrow a \nmid b \lor b \nmid c$

1.2.2. Definition: GCD and LCM

Let $a, b \in \mathbb{Z}$.
1. $\exists! d \in \mathbb{Z}_{\geq 0}$ such that

- $d \mid a$ and $d \mid b$,
- $\forall e \in \mathbb{Z}$ if $e \mid a$ and $e \mid b$, then $e \mid d$

d is called the **greatest common divisor (gcd)** of a and b, denoted $d = \gcd(a, b) = (a, b)$. Note we define $\gcd(0, 0) = 0$.

2. $\exists! m \in \mathbb{Z}_{\geq 0}$ such that

- $a \mid m$ and $b \mid m$,
- $\forall n \in \mathbb{Z}$, if $a \mid m$ and $b \mid n$, then $m \mid n$.

m is the **least common multiple (lcm)** of a and b, i.e. $m = \operatorname{lcm}(a, b)$.

1.2.3. *Theorem:* Division Algorithm

Let $a, b \in \mathbb{Z}$ with $b \neq 0$. Then $\exists! q, r \in \mathbb{Z}$ such that $a = qb + r$ and $0 \leq r < |b|$

1.2.4. *Theorem:* Euclidean Algorithm

Let $a, b \in \mathbb{Z}$ with $b > 0$. Set $r_{-1} = a$ and $r_0 = b$. Apply division algorithm repeatedly: $r_{-1} = q_1 r_0 + r_1$ with $0 < r_1 < r_0$ Then $r_0 = q_2 r_1 + r_2, 0 < r_2 < r_1$ and eventually $r_{n-2} = q_n r_{n-1} + r_n$ and $r_{n-1} + q_{n+1} r_n + 0$. Note this eventually becomes zero because the sequence r_n is strictly decreasing. The theorem tells us that $r_n = \gcd(a, b)$.

1.2.5. Exercise

$a = 3132$ and $b = 936$. Find GCD.

Solution

1. $3132 = 3 \cdot 936 + 324$
2. $936 = 2 \cdot 324 + 288$
3. $324 = 1 \cdot 288 + 36$
4. $288 = 8 \cdot 36 + 0$

Ergo $\gcd(a, b) = 36$.

We can also work backwards:

$$\begin{aligned} 36 &= 324 - 1 \cdot 288 \\ &= 324 - 1 \cdot (936 - 2 \cdot 324) \\ &= 3 \cdot 324 - 1 \cdot 936 \\ &= 3 \cdot (3132 - 3 \cdot 936) - 1 \cdot 936 \\ &= 3 \cdot 3132 - 10 \cdot 936 \end{aligned}$$

and we were able to give the GCD in terms of a linear combination of our numbers.

1.2.6. *Theorem:* Bezout's Identity

Let $a, b \in \mathbb{Z}$. Then $\exists m, n \in \mathbb{Z}$ such that $(a, b) = ma + nb$.

Remark: If $a \neq 0$ or $b \neq 0$, $\gcd(a, b)$ is the smallest positive integer of the form $sa + tb$ with $s, t \in \mathbb{Z}$.

1.2.7. Definition: Prime Number

An integer $p \in \mathbb{Z}_{>1}$ is **prime** if its only positive divisors are 1 and p. An integer is **composite** if it is not prime.

So $\forall n \in \mathbb{Z}^+ \setminus \{1, p\}$, we have $n \nmid p$.

1.2.8. *Lemma:* Euclid's Lemma

Let p be prime and let $a, b \in \mathbb{Z}$. If $p \mid ab$, then $p \mid a$ or $p \mid b$.

Proof: If $p \nmid a$, then $(a, p) = 1$. This is because given $d \in \mathbb{Z}^+$ such that $d \mid a$ and $d \mid p$, by primality either $d = 1 \Leftrightarrow 1 \mid d$ or $d = p$, but the latter is impossible since d divides a but not p.

By Bezout, $\exists m, n \in \mathbb{Z}$ such that $am + np = 1$. Then $mab + nbp = b$, and since $p \mid ab$ we have $p \mid b$, but this is a contradiction.

□

1.2.9. *Proposition*

Let $a, b, c \in \mathbb{Z}$. Assume $(a, c) = 1$ (they are relatively prime) and $c \mid ab$, then $c \mid b$.

Proof: Closely related to the previous result. By Bezout, $\exists n, m \in \mathbb{Z}$ such that $ma + nc = 1$. Then $mab + ncb = b$, and since $c \mid ab$ we have $c \mid b$.

□

1.2.10. *Theorem:* Fundamental Theorem of Arithmetic

Every integer greater than 1 can be written as the product of prime numbers and the factorization is unique up to the order of the factors.

Corollary: $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}, b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r}$ where $p_1, p_2, ..., p_r$ are distinct primes and $\alpha_1, \alpha_2, ..., \alpha_r, \beta_1, \beta_2, ..., \beta_r \in \mathbb{Z}_{\geq 0}$. Then $(a, b) = p_1^{\min\{\alpha_1, \beta_1\}} \cdots p_r^{\min\{\alpha_r, \beta_r\}}$ and $\operatorname{lcm}(a, b) = p_1^{\max\{\alpha_1, \beta_1\}} \cdots p_r^{\max\{\alpha_r, \beta_r\}}$.

1.3. Modular Arithmetic

1.3.1. Definition: Modulo

Let $a, b \in \mathbb{Z}$ with $n \in \mathbb{Z}_{\geq 0}$ fixed. We say that a is **congruent to b modulo n**, i.e. $a \equiv b (\operatorname{mod} n)$ if $n \mid b - a$.

1.3.2. *Proposition*

Congruence modulo n is an equivalence relation.

1.3.3. Definition: Residue Class

The equivalence class of $a \in \mathbb{Z}$ for this relation is called the **congruence / residue class** of $a \operatorname{mod} n$.

We can also write $\overline{a} = a \operatorname{mod} n = \{a + kn : k \in \mathbb{Z}\}$

1.3.4. *Proposition*

There are exactly n different residue classes modulo n: $\overline{0}, \overline{1}, ...\overline{n-1}$ (can be proved using division algorithm). The quotient set is denoted by $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, ..., \overline{n-1}\}$.

1.3.5. ***Proposition***

Let $a, b, c, d \in \mathbb{Z}$. If $a \equiv b (\operatorname{mod} n)$ and $c \equiv d (\operatorname{mod} n)$ then $a + c \equiv b + c (\operatorname{mod} n)$ and $ac \equiv bd (\operatorname{mod} n)$.

In particular, $\overline{a} = \overline{b}$ and $\overline{c} = \overline{d}$, then $\overline{a+c} = \overline{b+d}$ and $\overline{ac} = \overline{bd}$

1.3.6. Definition: Group of Units

The **group of units** of $\mathbb{Z}/n\mathbb{Z}$, denoted by $(\mathbb{Z}/n\mathbb{Z})^\times$, is the subset of $\mathbb{Z}/n\mathbb{Z}$ consisting of the residue classes which are invertible for the multiplication operation, i.e.

$$(\mathbb{Z}/n\mathbb{Z})^\times = \left\{\overline{a} \in \mathbb{Z}/n\mathbb{Z} \mid \exists c \in \mathbb{Z}/n\mathbb{Z} \text{ such that } \overline{a} \cdot \overline{c} = \overline{1}\right\}.$$

1.3.7. ***Proposition***

$(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z} \mid (a, n) = 1\}$.

Proof: ($\subseteq$) Let $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$. Then $\exists c \in \mathbb{Z}/n\mathbb{Z}$ such that $\overline{a} \cdot \overline{c} = \overline{1}$. Therefore $ac = 1 + nk$ for some $k \in \mathbb{Z}$, which we can rewrite as $ac + n(-k) = 1$. Therefore by the remark on Bezout's Identity, we have $(a, n) = 1$.

($\supseteq$) Let $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ and suppose $(a, n) = 1$. By Bezout's Identity, $\exists x, y \in \mathbb{Z}$ such that $ax + ny = 1$. Thus $ax = 1 - ny \equiv 1 \ (\operatorname{mod} n)$, so $\overline{a} \cdot \overline{x} = \overline{1}$ and therefore $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$.

□

1.3.8. Example

$(\mathbb{Z}/9\mathbb{Z})^\times = \left\{\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{7}, \overline{8}\right\}$.

1.4. Problems

1.4.1. Exercise

(Dummit and Foote, 0.2.4) Let a, b, N be fixed integers with a and b nonzero and let $d = (a, b)$. Suppose (x_0, y_0) is a particular solution to $ax + by = N$, i.e., $ax_0 + by_0 = N$. Prove that, for any integer t, the pair of integers

$$x = x_0 + \frac{b}{d}t, \quad y = y_0 - \frac{a}{d}t$$

is also a solution to $ax + by = N$. Also try to prove that all solutions to $ax + by = N$ are of the form above.

Solution

1.4.2. Exercise

> (Dummit and Foote, 0.3.11) Let $\overline{a}, \overline{b} \in \mathbb{Z}/n\mathbb{Z}$. Prove that if $\overline{a}, \overline{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$, then $\overline{a} \cdot \overline{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$.

Solution

1.4.3. Exercise

> (Dummit and Foote, 0.3.15) For each of the following pairs of integers a and n, show that a is relatively prime to n and determine the multiplicative inverse of $\overline{a}$ in $\mathbb{Z}/n\mathbb{Z}$.

Solution

2. Groups

2.1. Groups

2.1.1. Definition: Binary Operation

A **binary operation** $\star$ on a set S is a function $\star : S \times S \to S$. For $a, b \in S$, we will write $a \star b$ for $\star (a, b)$.

A binary operation $\star$ on a set S is **associative** if, for all $a, b, c \in S$,

$$a \star (b \star c) = (a \star b) \star c.$$

A binary operation $\star$ on a set S is **commutative** if, $\forall a, b \in S$,

$$a \star b = b \star a.$$

2.1.2. Example

1. $+$ (usual addition) is an associative and commutative binary operation on $\mathbb{Z}$ and other sets
2. $\times$ (usual multiplication) is an associative and commutative binary operation for these sets as well
3. The function

$$\begin{aligned} \star : \mathbb{Z} \times \mathbb{Z} &\longrightarrow \mathbb{Z} \\ (m, n) &\mapsto m^2 + n^2 \end{aligned}$$

   is a commutative binary operation on $\mathbb{Z}$, but not associative.

2.1.3. Definition: Identity

Let $\star$ be a binary operation on a set S. An **identity** is an element $e \in S$ such that

$$e \star a = a \text{ and } a \star e = a \forall a \in S.$$

2.1.4. *Proposition*

Let $\star$ be a binary operation on a set S. Then S has at most one identity.

Proof: Suppose that $e, e' \in S$ are both identities. Then, since e is an identity, we have $e \star e' = e'$ but also, since e' is an identity, we have $e \star e' = e$. Therefore $e = e'$.

□

2.1.5. Definition: Invertible

Let $\star$ be an associative binary operation on a set S and suppose there is an identity e. We say that an element of $a \in S$ is **invertible** if $\exists b \in S$ such that

$$a \star b = e \text{ and } b \star a = e$$

and in this case, we say that b is an inverse of a.

2.1.6. *Proposition*

> Let $\star$ be an associative binary operation on a set S and suppose that there is an identity e. If $a \in S$ is invertible, then a has a unique inverse.

Proof: Suppose that $b, c \in S$ are inverses of $a \in S$. Then

$$b = b \star e = b \star (a \star c) = (b \star a) \star c = e \star c = c.$$

We denote inverses by a^{-1}.

□

2.1.7. Definition: Group

A **group** is an ordered pair $(G, \star)$, where G is a set and $\star$ is a binary operation on G satisfying

1. the operation is associative
2. G has an identity
3. every element $a \in G$ is invertible

(fourth one that G is closed under $\star$ is implicit)

2.1.8. Definition: Abelian Group

A group is **abelian** if $\star$ is commutative.

2.1.9. Definition: Group Order

The **order** of a group $(G, \star)$ is the cardinality $|G|$ of the set G. If the order is finite, then $(G, \star)$ is a finite group.

2.1.10. Definition: General and Special Linear Groups

The **general linear group** over a field F of degree n, denoted by $\mathrm{GL}_n(F)$, is the set of $n \times n$ invertible matrices together with the operation matrix multiplication. I.e., we have

$$\mathrm{GL}_n(F) = \{A \in M_n(F) : \det A \neq 0\}$$

The **special linear group** over a field F of degree n, denoted by $\mathrm{SL}_n(F)$, is the subgroup of $\mathrm{GL}_n(F)$ of matrices with determinant 1.

2.1.11. Example

1. $(\mathbb{Z}, +)$ is an abelian group.
2. $(\mathbb{Z}_{\geq 0}, +)$ is not a group since there are no inverses.
3. $(\mathbb{Z}, \times)$ is not a group since there are no inverses.

2.1.12. Definition: Direct Product of Groups

If $(G, \star)$ and $(H, \diamond)$ are groups, then we can form a new group called their **direct product**, denoted by

$$G \times H = \{(g, h) : g \in G, h \in H\}$$

and whose binary operation is defined componentwise:

$$(g_1, h_1)(g_2, h_2) = (g_1 \star g_2, h_1 \diamond h_2).$$

2.1.13. *Proposition*

Let $(G, \star)$ be a group. Let e be the identity element. Then
1. $\left(a^{-1}\right)^{-1} = a \forall a \in G$
2. $\forall a, b \in G$, if $a \star b = e$ or $b \star a = e$, then $b = a^{-1}$
3. $(a \star b)^{-1} = b^{-1} \star a^{-1} \forall a, b \in G$
4. $\forall a_1, a_2, ..., a_n \in G$, the value of $a_1 \star a_2 \star \cdots \star a_n$ is independent of how the expression is bracketed

Proof:

1. By definition, $a \star a^{-1} = e$ and $a^{-1} \star a = e$. But this also shows that a is the inverse of a^{-1}, i.e., that $a = \left(a^{-1}\right)^{-1}$.

2. Suppose that $a \star b = e$ (the case $b \star a = e$ is similar).

Then

$$a \star b = e \Rightarrow a^{-1} \star (a \star b) = a^{-1} \star e \Rightarrow \left(a^{-1} \star a\right) \star b = a^{-1} \Rightarrow e \star b = a^{-1} \Rightarrow b = a^{-1}$$

3. By (b), it suffices to show that

$$(a \star b) \star \left(b^{-1} \star a^{-1}\right) = e.$$

   To show this, observe that

   $$(a \star b) \star \left(b^{-1} \star a^{-1}\right) = a \star \left(b \star \left(b^{-1} \star a^{-1}\right)\right) = a \star \left(\left(b \star b^{-1}\right) \star a^{-1}\right) = a \star \left(e \star a^{-1}\right) = a \star a^{-1} = e.$$

4. Can be shown by induction on n – see DF section 1.1 prop 1.

□

2.1.14. *Proposition*

Let G be a group. Let e be the identity element. Let $a, b, c \in G$. We have

1. If $a \star b = a \star c$, then $b = c$
2. If $b \star a = c \star a$, then $b = c$

Proof:

1. Left multiplying by a^{-1} on both sides we get

$$a^{-1} \star (a \star b) = a^{-1} \star (a \star c) \Rightarrow (a^{-1} \star a) \star b = (a^{-1} \star a) \star c = e \star b = e \star c \Rightarrow b = c.$$

2. Similar with a right multiplication.

□

2.1.15. Remark

We will use multiplicative notation for groups:

$$a^n = \begin{cases} \underbrace{a \cdot a \cdots a}_{n \text{ times}} & \text{if } n > 0 \\ 1 & \text{if } n = 0 \\ \underbrace{a^{-1} \cdot a^{-1} \cdots a^{-1}}_{\text{n times}} & \text{if } n < 0 \end{cases}$$

Notice then $a^m a^n = a^{m+n}$, but $a^n b^n \neq (ab)^n$ in the general case.

For an abelian group, we may also use additive notation, i.e.

$$na = \begin{cases} \underbrace{a + \cdots + a}_{\text{n times}} & \text{if } n > 0 \\ 1 & \text{if } n = 0 \\ \underbrace{(-a) + (-a) + \cdots + (-a)}_{-n \text{ times}} & \text{if } n < 0 \end{cases}$$

2.1.16. Definition: Element order

Let G be a group and let $a \in G$. The **order** of a is the smallest positive integer n such that $a^n = 1$, if such an integer exists; otherwise, the order of a is defined to be infinity. We denote the order of a by $|a|$ or $\operatorname{ord}(a)$.

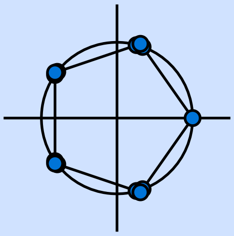
2.1.17. Example

1. An element of a group has order 1 iff it's the identity
2. In the additive group $\mathbb{Z}$, every element has infinite order
3. In the group $\mathrm{GL}_2(\mathbb{Q})$, the matrix $\begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}$ has infinite order, and $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ has order 4.
4. A matrix $A \in \mathrm{GL}_n(\mathbb{C})$ has finite order iff A is diagonalizable and all its eigenvalues are roots of unity

2.2. Dihedral Groups

2.2.1. Definition: Dihedral Group

Let $n \geq 3$ be an integer. The **dihedral group** D_{2n} is the set of isometries of the plane $\mathbb{R}^2$ that take the regular n-gon centered at $(0, 0)$ and with a vertex at $(1, 0)$ to itself. (Equivalently, it is the set of rigid motions in $\mathbb{R}^3$ taking this n-gon to itself). The binary operation on this group is composition.) Other books may denote this D_n.



It consists of

- (counterclockwise) rotation through an angle $2\pi k/n$ for $k = 0, 1, ..., n - 1$
- reflection wrt the line passing through $(0, 0)$ of slope $\tan(\pi k/n)$ for $k = 0, 1, ..., n - 1$

Let r denote the rotation by $2\pi/n$ and let s denote the reflection wrt the x-axis. Then

- r^k is the rotation by $2\pi k/n$
- $r^k s$ is the reflection wrt the line passing through $(0, 0)$ of slope $\tan(\pi k/n)$

Therefore $D_{2n} = \{1, r, ..., r^{n-1}, s, rs, ..., r^{n-1}s\}$. Writing the isometries above in terms of their matrices, we have

$$r^k = \begin{pmatrix} \cos\left(\frac{2\pi k}{n}\right) & -\sin\left(\frac{2\pi k}{n}\right) \\ \sin\left(\frac{2\pi k}{n}\right) & \cos\left(\frac{2\pi k}{n}\right) \end{pmatrix}; \quad r^k s = \begin{pmatrix} \cos\left(\frac{2\pi k}{n}\right) & \sin\left(\frac{2\pi k}{n}\right) \\ \sin\left(\frac{2\pi k}{n}\right) & -\cos\left(\frac{2\pi k}{n}\right) \end{pmatrix}$$

Since every element of D_{2n} can be expressed in terms of r and s and their inverses, we say that r and s *generate* or are *generators* of the group D_{2n}. The elements r and s satisfy the relations

$$r^n = 1, s^2 = 1, sr = r^{-1}s$$

These relations suffice to show that any product involving the elements r and s and their inverses is equal to one of the products $1, r, ..., r^{n-1}, s, rs, ..., r^{n-1}s$. These generators, together with the relations $r^n = 1$, $s^2 = 1$, $sr = r^{-1}s$ form a *presentation* of D_{2n} and we indicate this by writing

$$D_{2n} = \langle r, s : r^n = 1, s^2 = 1, sr = r^{-1}s \rangle.$$

2.3. Symmetric Groups

2.3.1. Definition: Permutation

Let Ω be a set and let $S_\Omega = \mathrm{Perm}(\Omega)$ denote the set of all permutations of Ω. A **permutation** of Ω is a bijective function $\sigma : \Omega \to \Omega$. Since bijective functions are closed under composition, if $\sigma, \tau \in S_\Omega$ then $\sigma\tau = \sigma \circ \tau \in S_\Omega$. Composition is a binary operation on S_Ω.

Notice $(S_\Omega, \circ)$ is a group:

1. Composition is associative
2. $\mathrm{id}_\Omega \in S_\Omega$ is an identity
3. Every $\sigma \in S_\Omega$ is invertible because σ is bijective and so $\sigma^{-1} \in S_\Omega$

We call $(S_\Omega, \circ)$ the symmetric group on Ω. If $\Omega = \{1, 2, ..., n\}$ then $S_\Omega = S_n$, the symmetric group of degree n. We remark that $|S_n| = n!$ (there are n permutations of a set of n elements).

2.3.2. Definition: k-cycle

A permutation $\sigma \in S_n$ is a ***k*-cycle** if $\exists$ distinct $a_1, a_2, ..., a_k \in \{1, 2, ..., n\}$ such that

- $\sigma(a_1) = a_2, ..., \sigma(a_{k-1}) = a_k, \sigma(a_k) = a_1$ and
- $\sigma(i) = i \forall i \in \{1, 2, ..., n\} \setminus \{a_1, a_2, ..., a_n\}$

2.3.3. Example

1. $\sigma \in S_5$ defined by
$$1 \mapsto 5, 2 \mapsto 1, 3 \mapsto 3, 4 \mapsto 4, 5 \mapsto 2$$
has a 3-cycle, $\sigma = (1\ 5\ 2)$
2. $\sigma \in S_4$ defined by
$$1 \mapsto 3, 2 \mapsto 4, 3 \mapsto 1, 4 \mapsto 2$$
has cycles $(1\ 3), (2\ 4)$ and can be written as the product $(1\ 3)(2\ 4)$

2.3.4. Definition: Disjoint cycle

Two cycles $(a_1\ a_2\ \cdots\ a_k)$ and $(b_1\ b_2\ \cdots\ b_l)$ are **disjoint** if $a_i \neq b_j \forall i, j$.

2.3.5. *Proposition*

1. Any k-cycle has order k
2. If $(a_1, a_2, \cdots, a_k)$ is a k-cycle in S_n, then $(a_1 a_2 \ \cdots \ a_k)^{-1} = (a_k a_{k-1} \ \cdots \ a_1)$
3. If $(a_1 a_2 \ \cdots \ a_k)$ and $(b_1 b_2 \ \cdots \ b_l)$ are disjoint then they commute

Proof:

1. We can show that $\forall n \in \mathbb{N}$ and $j \in \mathbb{Z}/k\mathbb{Z}$, we have

$$\sigma^n(a_j) = a_{j+n \pmod{k}}.$$

   This is done via induction, since trivially $\sigma\left(a_{j+n \pmod{k}}\right) = a_{j+n+1 \pmod{k}}$. Then note this implies $\sigma^k = \mathrm{Id}$ and $\forall j < k, \sigma^j \neq \mathrm{Id}$.
2. Let $\sigma = (a_1 a_2 \ \cdots \ a_k)$ and $\tau = (a_k a_{k-1} \ \cdots \ a_1)$. We want to show

$$\tau\sigma = 1 = \mathrm{Id}\,.$$

   Then for $1 \leq j < k$,
   - $\sigma(a_j) = a_{j+1}, (\tau\sigma)(a_j) = \tau(a_{j+1}) = a_j$
   - $\sigma(a_k) = a_1, (\tau\sigma)(a_k) = \tau(a_1) = a_k$

   For $j \in \{1, 2, ..., n\} \setminus \{a_1, a_2, ..., a_k\}$
   - $\sigma(j) = j, (\tau\sigma)(j) = \tau(j) = j$
3.

□

2.3.6. *Theorem:* Cycle Decomposition

Every $\sigma \in S_n$ can be written as a product of disjoint cycles. We call this factorization the cycle decomposition of v. It is unique up to the order of the cycles.

To find this factorization:

1. To start a new cycle, pick the smallest element of $\{1, 2, ..., n\}$ which has not yet appeared in a previous cycle – call it a.
2. Read off $\sigma(a)$ from the given description fo σ – call it b. If $b = a$, close the cycle with a right parenthesis; this completes a cycle – return to step 1. If $b \neq a$, write b next to a in this cycle. Repeat this step iteratively with $\sigma(b)$.

Proof: The algorithm above gives a constructive proof of existence of cycle decompositions. To prove uniqueness, we need to show that if

$$\sigma = \alpha_1 \alpha_2 \cdots \alpha_p = \beta_1 \beta_2 \cdots \beta_q$$

are two cycle decompositions of a permutation $\sigma \in S_n$, with no 1-cycles, then $p = q$, and up to rearranging the cycles, $\alpha_i = \beta_i$ for $i = 1, 2, ..., p$. We proceed by induction on $m = \max\{p, q\}$.

For $m = 0$ the result is trivial. Suppose the result holds for $m = t - 1$ for $t \geq 1$. Suppose

$$\sigma = \alpha_1 \alpha_2 \cdots \alpha_p = \beta_1 \beta_2 \cdots \beta_q$$

are two cycle decompositions of a permutation $\sigma \in S_n$, with no 1-cycles and with $\max\{p, q\} = t$. Without loss of generality assume $p = t \geq 1$. Let $\alpha_1 = (a_1 \ a_2 \ \cdots \ a_k)$. Without loss of generality, suppose that a_1 appears in β_1, and write $\beta_1 = (a_1 \ b_2 \ \cdots \ b_\ell)$. Then

$$\begin{aligned} a_2 &= \sigma(a_1) = b_2 \\ \Rightarrow a_3 &= \sigma(a_2) = \sigma(b_2) = b_3 \\ &\vdots \\ \Rightarrow a_k &= \sigma(a_{k-1}) = \sigma(b_{k-1}) = b_k \\ \Rightarrow \sigma(b_k) &= \sigma(a_k) = a_1 \end{aligned}$$

Therefore $k = \ell$ and $\alpha_1 = \beta_1$. Let $\sigma' = \alpha_1^{-1}\sigma = \beta_1^{-1}\sigma$ so $\sigma' = \alpha_2 \cdots \alpha_p = \beta_2 \cdots \beta_q$. Iterate this process and we get the desired result.

□

2.3.7. Example

i	1	2	3	4	5	6	7	8
$\sigma(i)$	4	7	2	8	5	6	3	1

Notice the cycles are $\sigma = (1\ 4\ 8)(2\ 7\ 3)(5)(6)$.

2.3.8. Example

We compute products by reading the permutations right to left. I.e. $(1\ 2)(1\ 3) = (1\ 3\ 2)$. (1 is mapped to 3 and 3 is mapped to itself, then 3 is mapped to 1 and 1 is mapped to 2, then 2 is mapped to itself and 2 is mapped to 1).

$$\begin{aligned}\sigma &= (1\ 4\ 6)(2\ 3)(5\ 7)\\ \tau &= (1\ 3\ 5\ 7)(2\ 4\ 6)\\ \tau\sigma &= (1\ 6\ 3\ 4\ 2\ 5)\\ \sigma^{-1} &= (6\ 4\ 1)(3\ 2)(7\ 5) = (1\ 6\ 4)(2\ 3)(5\ 7)\end{aligned}$$

Note that S_n is non abelian for $n \geq 3$, since $(1\ 2) \circ (1\ 3) \neq (1\ 3) \circ (1\ 2)$. Note also that since disjoint cycles permute numbers in disjoint sets, it follows that disjoint cycles commute.

2.3.9. Definition: Transpositions

2-cycles are also called **transpositions**.

2.3.10. *Proposition*

Every $\sigma \in S_n$ can be written as a product of transpositions.

Proof: Since every $\sigma \in S_n$ is a product of cycles, it suffices to prove the proposition for cycles. Observe $(a_1 \cdots a_k) = (a_1 a_2)(a_2 a_3) \cdots (a_{k-1} a_k)$, so this is true.

□

2.3.11. Definition: Inversion

A pair of integers (i, j) with $1 \leq i < j \leq n$ is said to be an **inversion** for $\sigma \in S_n$ if $\sigma(i) > \sigma(j)$. We say σ is even (resp. odd) if it has an even (resp. odd) number of inversions.

2.3.12. Definition: Permutation Sign

The **sign** of a permutation $\sigma \in S_n$ with $N(\sigma)$ inversions is

$$\varepsilon(\sigma) = (-1)^{N(\sigma)} = \begin{cases} +1 \text{ if } \sigma \text{ is even} \\ -1 \text{ if } \sigma \text{ is odd} \end{cases}$$

Notice we can write this as

$$\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j}.$$

2.3.13. Example

1. $1 \in S_n$ is even (zero inversions)
2. $(1\ 4\ 3\ 2) \in S_4$
   - $\sigma(1) = 4 > \sigma(2) = 1 \Rightarrow (1, 2)$ is an inversion
   - $\sigma(1) = 4 > \sigma(3) = 2 \Rightarrow (1, 3)$ is an inversion
   - Also $(1, 4)$ is but the rest $(2, 3), (2, 4), (3, 4)$ are not

Therefore the number of inversions for σ is $N(\sigma) = 3$ and $\varepsilon(\sigma) = (-1)^{N(\sigma)} = -1$.

2.3.14. *Lemma*

> For every $\rho \in S_n$ and for every transposition $\tau \in S_n$, $\varepsilon(\rho\tau) = -\varepsilon(\rho)$, i.e., these permutations have opposite parity.

Proof: Let $\rho \in S_n$. Let $(ij) \in S_n$ with $i < j$. Then for $a \in \{1, 2, ..., n\}$,

$$\rho\tau(a) = \begin{cases} \rho(a) \text{ if } a \neq i, j \\ \rho(j) \text{ if } a = i \\ \rho(i) \text{ if } a = j \end{cases}$$

Therefore, for any pair of integers (x, y) with $1 \leq x < y \leq n$ and $\{x, y\} \cap \{i, j\} = \emptyset$:

$$(x, y) \text{ is an inversion for } \rho\tau \Longleftrightarrow (x, y) \text{ is an inversion for } \rho.$$

- For $x \in \{1, 2, ..., n\} \setminus \{i, j\}$
  1. $x < i < j$
     - (r, i) is an inversion for $\rho\tau \Longleftrightarrow (x, j)$ is an inversion for ρ
     - (x, j) is an inversion for $\rho\tau \Longleftrightarrow (x, i)$ is an inversion for ρ
  2. $i < x < j$
     - (i, x) is an inversion for $\rho\tau \Longleftrightarrow (x, j)$ is not an inversion for ρ
     - (x, j) is an inversion for $\rho\tau \Longleftrightarrow (i, x)$ is not an inversion for ρ
  3. $i < j < x$
     - (i, x) is an inversion for $\rho\tau \Longleftrightarrow (j, x)$ is an inversion for ρ
     - (j, x) is an inversion for $\rho\tau \Longleftrightarrow (i, x)$ is an inversion for ρ
  4. (i, j) is an inversion for $\rho\tau \Longleftrightarrow (i, j)$ is not an inversion for ρ

Thus the number of inversions for $\rho\tau \not\equiv$ the number of inversions for $\rho \pmod 2$.

□

2.3.15. ***Proposition***

A *permutation* $\sigma \in S_n$ is even (resp. odd) iff it can be written as a product of an even (resp. odd) number of transpositions.

Proof: Let $\sigma \in S_n$. We know σ can be written as a product of transpositions, say $\sigma = \gamma_1 \gamma_2 \cdots \gamma_k$ so we just need to show $\varepsilon(\sigma) = (-1)^k$. We can do this from the lemma + induction.

□

2.3.16. ***Proposition***

Suppose $\sigma, \tau \in S_n$. Then

- $\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau)$
- $\varepsilon(\sigma^{-1}) = \varepsilon(\sigma)$

Proof: Suppose $\sigma = \gamma_1 \gamma_2 \cdots \gamma_k$ and $z = \gamma'_1 \gamma'_2 \cdots \gamma'_l$ where the γ'_i's are transpositions.

□

2.3.17. Definition: Alternating Group of Degree n

The group consisting of the set of all even permutations in S_n under composition. We denote it by A_n.

2.3.18. Definition: Klein 4-group

The **Klein 4-group**, denoted by V_4, is the group presentation $V_4 = (a, b : a^2 = b^2 = (ab)^2 = e)$. I.e., the group is an abelian group with 4 elements where every element is a self inverse. We can think of it as the permutation group

$$V = \{(), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}.$$

2.4. Problems

2.4.1. Exercise

(Dummit and Foote, 1.1.35) If x is an element of finite order n in a group G, use the Division Algorithm to show that *any* integral power of x equals one of the elements of the set $\{1, x, x^2, ..., x^{n-1}\}$.

Solution

2.4.2. Exercise

(Dummit and Foote, 1.2.4) If $n = 2k$ is even and $n \geq 4$, show that $z = r^k$ is an element of order 2 which commutes with all elements of D_{2n}. Show also that z is the only non-identity element of D_{2n} which commutes with all elements of D_{2n}.

Solution

2.4.3. Exercise

Prove that, for all $n \geq 2$, $|A_n| = n!/2$.

Solution

2.4.4. Exercise

(Dummit and Foote, 1.3.16) Prove that the number of k-cycles in S_n is given by

$$\frac{n(n-1)(n-2)\cdots(n-k+1)}{k}.$$

Solution

3. Subgroups

3.1. Subgroups

3.1.1. Definition: Subgroup

A subset H of a group G is a **subgroup** if it satisfies:

1. *Closure*: If a and b are in H, then $ab \in H$
2. *Identity*: $1 \in H$
3. *Inverses*: If $a \in H$, then $a^{-1} \in H$

We write $H \leq G$ to indicate that H is a subgroup of G.

3.1.2. Example

1. If G is a group, then $\{1\}$ and G are both subgroups of G. The former is the trivial subgroup and a subgroup $H \leq G$ is called proper if $H \neq G$
2. The subgroup relation is transitive
3. $A_n \leq S_n$
4. The set $\{1, (1\ 2)\}$ is a subgroup of S_3
5. Let F be a field. The *special linear group of degree n over F*, defined as
$$\mathrm{SL}_n(F) = \{A \in \mathrm{GL}_n(F) : \det(A) = 1\},$$
is a subgroup of $\mathrm{GL}_n(F)$.

3.1.3. Definition: Centralizer

Let A be a subset of a group G. The **centralizer** of A in G, defined by

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

is a subgroup of G.

Proof: Let $g, h \in C_G(A)$, so $gag^{-1} = a$ and $hah^{-1} = a \forall a \in A$. Then $gh = (aga^{-1})(aha^{-1}) = agha^{-1} \Rightarrow (gh)agh^{-1} = a$ so $gh \in H$. Thus $C_G(A)$ is closed. Notice $eae^{-1} = a \forall a \in A$, so $e \in C_G(A)$. Suppose $g \in C_G(A)$, so $gag^{-1} = a \forall a \in A$. Then $a = g^{-1}ag \forall a \in A$, so $g^{-1} \in C_G(A)$.

3.1.4. Definition: Center

The **center** of a group G, defined as

$$Z(G) = \{g \in G : gx = xg \forall x \in G\}$$

is a subgroup of G. Actually, since $Z(G) = C_G(G)$, this is just a special case of the centralizer.

3.1.5. Definition: Normalizer

Let A be a subset of a group G. For $g \in G$, define $gAg^{-1} = \{gag^{-1} : a \in A\}$. The **normalizer** of A in G, defined as

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

is a subgroup of G.

3.1.6. *Proposition*

Let A be a subset of a group G. Then $Z(G) \leq C_G(A) \leq N_G(A) \leq G$.

Proof: Notice since $A \subseteq G$, $Z(G) \subseteq C_G(A)$. Also $N_G(A) \subseteq G$, so the only nontrivial inequality is the middle one. Let $g \in C_G(A)$ so that $gag^{-1} = a \forall a \in A$. Then $gAg^{-1} = \{gag^{-1} : a \in A\} = A$ so $g \in N_G(A)$.

□

3.1.7. *Proposition*

A subset H of a group G is a subgroup if and only if

1. $H \neq \emptyset$
2. $\forall x, y \in H, xy^{-1} \in H$

Proof: $(\Longrightarrow)$ Suppose that H is a subgroup. Then $1 \in H$, so $H \neq \emptyset$. Also, if $x, y \in H$, then $y^{-1} \in H$ and $xy^{-1} \in H$.

$(\Longleftarrow)$ Suppose a and b hold for $H \subseteq G$. Since H is nonempty, let $c \in H$. By condition 2, $cc^{-1} = 1 \in H$. Let $a \in H$ and notice $1 \cdot a^{-1} \in H$ so H is closed under inverses. Let $a, b \in H$ and notice $b^{-1} \in H$ by the previous statement, so $a(b^{-1})^{-1} = ab \in H$ so H is closed under the operation.

□

3.2. Cyclic Groups and Subgroups

3.2.1. *Proposition*

Let G be a group and let $a \in G$ be an element of finite order n. Then

1. $\forall m \in \mathbb{Z}$, we have that $a^m = 1 \Longleftrightarrow n \mid m$
2. $\forall m, m' \in \mathbb{Z}$, we have that $a^m = a^{m'} \Longleftrightarrow m \equiv m' \pmod{n}$
3. $\forall m \in \mathbb{Z}$, we have that $\operatorname{ord}(a^m) = \frac{n}{(n,m)}$.

Proof:

1. If $n \mid m$, then $m = nq$ for some $q \in \mathbb{Z}$ and $a^m = a^{nq} = (a^n)^q = 1^q = 1$. Conversely, suppose $a^m = 1$. By the division algorithm, $m = nq + r$, $q, r \in \mathbb{Z}$ and $0 \leq r < n$. Then $a^r = a^{m-nq} = a^m a^{-nq} = a^m (a^n)^{-q} = 1 \cdot 1^{-q} = 1$. Since $n = \operatorname{ord}(a)$ and $0 \leq r < n$, this implies $r = 0$.
2. $a^m = a^{m'} \Leftrightarrow a^m a^{-m'} = 1 \Leftrightarrow a^{m-m'} = 1 \overset{(a)}{\Leftrightarrow} n \mid m - m' \Leftrightarrow m \equiv m' \pmod{n}$.
3. Let $k = \operatorname{ord}(a^m)$. We have that

$$(a^m)^{\frac{n}{(n,m)}} = a^{\frac{mn}{(n,m)}} = (a^n)^{\frac{m}{(n,m)}} = 1^{\frac{m}{(n,m)}} \overset{(a)}{\Rightarrow} k \mid \frac{n}{(n,m)}$$

and

$$a^{mk} = (a^m)^k = 1 \overset{(a)}{\Longrightarrow} n \mid mk \Rightarrow \frac{n}{(n,m)} \mid \frac{m}{(n,m)} k \Rightarrow \frac{n}{(n,m)} \mid k.$$

Thus $k = \frac{n}{(n,m)}$.

□

3.2.2. Definition: Cyclic Subgroup

Let G be a group. The **cyclic subgroup** of G generated by an element $a \in G$, denoted (a), is the subgroup consisting of all powers of a, i.e.,

$$(a) = \{a^k : k \in \mathbb{Z}\}.$$

The cyclic subgroup generated by a is the smallest subgroup of G containing a: any subgroup of G containing a will have (a) as a subgroup.

3.2.3. Example

1. The cyclic subgroup generated by $(1\ 2\ 3) \in S_3$ is
$$((1\ 2\ 3)) = \{1, (1\ 2\ 3), (1\ 3\ 2)\}.$$
2. The cyclic subgroup generated by π in the additive group $(\mathbb{R}, +)$ is the set of all integer multiples of π, i.e.,
$$(\pi) = \{k\pi : k \in \mathbb{Z}\}.$$

3.2.4. Definition: Cyclic Group and Group Generator

A group G is **cyclic** if it can be generated by a single element, i.e., $\exists a \in G$ such that $G = (a)$. In this case, we say that a is a **generator** of G.

3.2.5. Example

1. For $n \in \mathbb{Z}_{\geq 0}$, the additive group $\mathbb{Z}/n\mathbb{Z}$ is a cyclic group of order n: $\mathbb{Z}/n\mathbb{Z} = (\overline{1})$.
2. The additive group $\mathbb{Z}$ is a cyclic group of infinite order: $\mathbb{Z} = (1)$.

3.2.6. *Proposition*

Let $G = (a)$ be a cyclic group.

1. If $\operatorname{ord}(a) = n$, then $1, a, ..., a^{n-1}$ are the distinct elements of G (which therefore has order n).
2. If $\operatorname{ord}(a) = \infty$, then the elements a^k with $k \in \mathbb{Z}$ are all distinct (and therefore G has infinite order.)

Proof:

1. Suppose $\operatorname{ord}(x) = n$. By contradiction, suppose that that $x^a = x^b$ for some $a, b \in \{0, 1, ..., n-1\}$ with $a \neq b$. Without loss of generality, suppose $a < b$. Then $x^{-a}x^a = 1 = x^{-a}x^b = x^{b-a}$. But since $b - a \leq (n-1) - 0 < n$, we must have that x cannot be order n, a contradiction. Therefore $1, x, ..., x^{n-1}$ are all distinct. Since G is a cyclic group, these are the only elements of G, so $n = |x| = |G|$.

2. Apply the previous result in the limit as $n \to \infty$.

□

3.2.7. *Proposition*

Let $G = (a)$ be a cyclic group of finite order n.

1. For all $b \in G$, we have $\operatorname{ord}(b) \mid n$.
2. For every positive divisor d of n, we have $n_d := |\{b \in G : \operatorname{ord}(b) = d\}| = \varphi(d)$.

Proof:

1. Let $b \in G$. Then $b = a^m$ for some $m \in \mathbb{Z}$. By 3.2.1, $\operatorname{ord}(b) = \frac{n}{(n,m)} \mid n$.
2. By the previous proposition, $1, a, ..., a^{n-1}$ are the distinct elements of G. By Prop 3.2.1, $\operatorname{ord}(a^m) = \frac{n}{(n,m)}$. Thus n_d is the number of integers m with $0 \leq m < n$ such that $\frac{n}{(n,m)} = d$. We will prove that
$$\left\{m \in \mathbb{Z} : 0 \leq m < n, \frac{n}{(n,m)} = d\right\} = \left\{\frac{nk}{d} : k \in \mathbb{Z}, 0 \leq k < d, (k,d) = 1\right\}.$$
Note the cardinality of the right hand side is precisely $\varphi(d)$, so this will conclude the proof of the proposition.

   To establish the above equality of sets, let first $m \in \mathbb{Z}$ with $0 \leq m < n$ and $\frac{n}{(n,m)} = d$. Then $(n,m) = \frac{n}{d}$, so $\exists k \in \mathbb{Z}$ such that $m = \frac{nk}{d}$. Notice
$$0 \leq m < n \Longrightarrow 0 \leq \frac{nk}{d} < \frac{nd}{d} \Longrightarrow 0 \leq k < d.$$
Since $(n,m) = \frac{n}{d}$, we have $\frac{n}{d} = \left(\frac{nk}{d}, \frac{nd}{d}\right) = \frac{n}{d}(k,d)$, so $(k,d) = 1$.

   In the other direction, let $m = \frac{nk}{d}$ with $k \in \mathbb{Z}$ and $0 \leq k < d$ with $(k,d) = 1$. Then $0 \leq m < \frac{nd}{d} = n$. Also $(n,m) = \left(\frac{nd}{d}, \frac{nk}{d}\right) = \frac{n}{d}(d,k) = \frac{n}{d}$, so $\frac{n}{(n,m)} = d$.

□

3.2.8. *Corollary*

For every $n \in \mathbb{N}$,
$$\sum_{1 \leq d \mid n} \varphi(d) = n.$$

Proof: Let $G = (a)$ be a cyclic group of order n, (e.g., $\mathbb{Z}/n\mathbb{Z}$). Then
$$n = |G| = \sum_{1 \leq d \mid n} n_d = \sum_{1 \leq d \mid n} \varphi(d).$$

Example: 10 = $\varphi(1) + \varphi(2) + \varphi(5) + \varphi(10) = 1 + 1 + 4 + 4$.

Alternate proof: consider rational numbers $\frac{1}{n}, \frac{2}{n}, ..., \frac{n}{n}$. Obtain a new list by reducing each number to lowest terms, so that the denominators in the new list are exactly divisors of n. If $d \mid n$, exactly $\varphi(d)$ of the numbers will have d as their denominator, so there are $\sum\limits_{1 \leq d \mid n} \varphi(d)$ elements in the new list, but since the lists have the same number of terms, we're done.

□

4. Homomorphisms

4.1. Group Homomorphisms

4.1.1. Definition: Group Homomorphism

Let $(G_1, \star)$ and $(G_2, \diamond)$ be groups. A **homomorphism** from $(G_1, \star)$ to $(G_2, \diamond)$, is a function $\varphi : G_1 \longrightarrow G_2$ such that

$$\varphi(xy) = \varphi(x)\varphi(y) \forall x, y \in G_1.$$

4.1.2. *Proposition*

Let $\varphi : G_1 \to G_2$ be a group homomorphism.

1. If $x_1, x_2, \ldots, x_k$ are elements of G_1, then $\varphi(x_1 x_2 \cdots x_k) = \varphi(x_1)\varphi(x_2) \cdots \varphi(x_k)$.
2. $\varphi\left(1_{G_1}\right) = 1_{G_2}$.
3. $\forall x \in G_1, \varphi(a^{-1}) = \varphi(x)^{-1}$.

Proof:

□

4.1.3. *Proposition*

Let $\varphi : G_1 \to G_2$ be a group homomorphism.

1. If $H_1 \leq G_1$, then $\varphi(H_1) \leq G_2$
2. If $H_2 \leq G_2$, then $\varphi^{-1}(H_2) \leq G_1$

Recall $\varphi(H_1) = \{\varphi(x) : x \in H_1\}$ and $\varphi^{-1}(H_2) = \{x \in G : \varphi(x) \in H_2\}$.

Proof:

1. Let $H_1 \leq G_1$. Since H_1 is a subgroup, $1_{G_1} \in H_1$. Therefore $1_{G_1} = \varphi\left(1_{G_1}\right) \in \varphi(H_1)$. Let $a, b \in \varphi(H_1)$. Then $a = \varphi(x)$ and $b = \varphi(y)$ for some $x, y \in H_1$. Then $ab^{-1} = \varphi(x)\varphi(y)^{-1} = \varphi(x)\varphi(y^{-1}) = \varphi(xy^{-1})$. Since H_1 is a subgroup, $xy^{-1} \in H_1$. Then $ab^{-1} \in \varphi(H_1)$.

□

4.1.4. Definition: Image and Kernel

Let $\varphi : G_1 \to G_2$ be a group homomorphism.

- The **image** of φ is

$$\operatorname{im}\varphi = \varphi(G_1) = \{\varphi(x) : x \in G_1\}$$

- The **kernel** of φ is

$$\ker\varphi = \varphi^{-1}(\{1\}) = \{x \in G_1 : G(x) = 1\}$$

By the previous proposition, $\ker\varphi \leq G$ and $\operatorname{im}\varphi \leq G_2$.

4.1.5. *Proposition*

Let $\varphi : G_1 \to G_2$ be a group homomorphism. Then φ is injective $\Longleftrightarrow$ $\ker\varphi = \left\{1_{G_1}\right\}$.

Proof: ($\Longrightarrow$) Suppose φ is injective. Let $x \in \ker\varphi$. Then $\varphi(x) = 1_{G_1} = \varphi\left(1_{G_1}\right)$. By injectivity, $x = 1_{G_1}$.

($\Longleftarrow$) Suppose $\ker\varphi = \left\{1_{G_1}\right\}$. Let $x, y \in G_1$. Then

$$\begin{aligned} \varphi(x) = \varphi(y) &\Longleftrightarrow \varphi(x)(\varphi(y))^{-1} = 1 \\ &\Longleftrightarrow \varphi(xy^{-1}) = 1 \\ &\Longleftrightarrow xy^{-1} = 1 \\ &\Longleftrightarrow x = y \end{aligned}$$

□

4.1.6. Example

1. Recall the determinant $\det : \mathrm{GL}_n(\mathbb{Q}) \to \mathbb{Q}^x$. Then $\ker(\det) = \mathrm{SL}_n(\mathbb{Q})$ and $\operatorname{im}(\det) = \mathbb{Q}^x$.
2. For $\varepsilon : S_n \to \{\pm 1\}$ we have

$$\ker(\varepsilon) = A_n$$
$$\operatorname{im}(\varepsilon) = \begin{cases} \{1\} \text{ if } n = 1 \\ \{\pm 1\} \text{ if } n \geq 2 \end{cases}$$

3. Note $|\cdot| : \mathbb{C}^x \to \mathbb{R}^x$ has $\ker(|\cdot|) = \{z \in \mathbb{C} : |z| = 1\} = S^1$ and $\operatorname{im}(|\cdot|) = \mathbb{R}_{>0}$.
4. $\exp : (\mathbb{R}, +) \to \mathbb{R}^x$ has kernel $\ker(\exp) = \{0\}$ and $\operatorname{im}(\exp) = \mathbb{R}_{>0}$.
5. $\exp_{\mathbb{C}} : (\mathbb{C}, +) \to \mathbb{C}^x$ has $\ker(\exp_{\mathbb{C}}) = 2\pi i\mathbb{Z}$ and $\operatorname{im}(\exp_{\mathbb{C}}) = \mathbb{C}^x$. Then $\exp_{\mathbb{C}}^{-1}(S^1) = i\mathbb{R}$ and $\exp_{\mathbb{C}}(a + bi) = e^a(\cos b + i \sin b)$.
6. $\varphi : D_{2n} \to S_n$ is the map $\sigma_x(i) = j \Longleftrightarrow x \text{ takes vertex } i \text{ to vertex } = j$. Then $\ker\varphi = \{1\}$ because an isometry of $\mathbb{R}^2$ fixing 3 non collinear points is the identity. For $n = 3$, $|D_6| = |S_3| = 6$, so φ is surjective. For $n > 3$, $2n = |D_{2n}| < |S_n| = n!$.

4.1.7. *Proposition*

Let $\varphi : G_1 \to G_2$ and $\psi : G_2 \to G_3$ be group homomorphisms. Then $\psi \circ \varphi$ is a group homomorphism.

Proof: Let $x, y \in G_1$. Then

$$(\psi \circ \varphi)(xy) = \psi(\varphi(xy)) = \psi(\varphi(x)\varphi(y)) = \psi(\varphi(x))\psi(\varphi(y)) = ((\psi \circ \varphi)(x))((\psi \circ \varphi)(y)).$$

□

4.1.8. Definition: Isomorphism

An **isomorphism** from a group G_1 to a group G_2 is a bijective homomorphism from G_1 to G_2.

4.1.9. Example

1. If G is a group then $\mathrm{id}_G : G \to G$ is an isomorphism.
2. $\exp : (\mathbb{R}, +) \to \mathbb{R}_{>0}$ is an isomorphism.
3. $\log : \mathbb{R}_{>0} \to (\mathbb{R}, +)$ is an isomorphism.

We remark $\log \circ \exp = \mathrm{id}_{\mathbb{R}}$ and $\exp \circ \log = \mathrm{id}_{\mathbb{R}>0}$.

4.1.10. *Proposition*

Let $\varphi : G_1 \to G_2$ be an isomorphism. Then $\varphi^{-1} : G_2 \to G_1$ is also an isomorphism.

Proof: We know φ^{-1} is bijective since φ is bijective, so we need to check that φ^{-1} is a homomorphism. Since φ is injective, for $a, b \in G_2$ we have

$$\begin{aligned} \varphi^{-1}(ab) = \varphi^{-1}(a)\varphi^{-1}(b) &\Longleftrightarrow \varphi(\varphi^{-1}(ab)) = \varphi(\varphi^{-1}(a)\varphi^{-1}(b)) \\ &\Longleftrightarrow \varphi(\varphi^{-1}(ab)) = \varphi(\varphi^{-1}(a)) \cdot \varphi(\varphi^{-1}(b)) \\ &\Longleftrightarrow ab = ab. \end{aligned}$$

□

4.1.11. Definition: Isomorphic Groups

The groups G_1 and G_2 are **isomorphic** if $\exists$ an isomorphism $\varphi : G_1 \to G_2$. Notation: $G_1 \cong G_2$ or $G_1 \simeq G_2$.

4.1.12. Definition: Isomorphism Class

The **isomorphism class** of a group G is the class of all groups isomorphic to G.

4.1.13. Definition: Automorphism

An **automorphism** of a group G is an isomorphism from G to G. If G is a group, then $\operatorname{Aut}(G)$ denotes the set of all automorphisms of G.

Notice Aut(G) is a group under composition:
- $\varphi, \psi \in \operatorname{Aut}(G) \Longrightarrow \psi \circ \varphi \in \operatorname{Aut}(G)$
- $\mathrm{id}_G \in \operatorname{Aut}(G)$ is an identity
- $\varphi \in \operatorname{Aut}(G) \Longrightarrow \varphi^{-1} \in \operatorname{Aut}(G)$

4.1.14. Definition: Inner Automorphism

An **inner automorphism** of a group G is an automorphism of the form φ_g for some $g \in G$, where $\varphi_g : G \to G$ is defined by $\varphi_g(x) = gxg^{-1}$. I.e., it is the image of the map $G \to \operatorname{Aut}(G)$ defined by $g \mapsto \varphi_g$. We denote the group of inner automorphisms of G by $\operatorname{Inn}(G)$.

4.1.15. *Proposition*

Let $g \in G$.

1. *Conjugation by g* is the map

$$\varphi_g : \begin{aligned} G &\to G \\ x &\mapsto gxg^{-1} \end{aligned}$$

is an automorphism.

2. The map

$$\begin{aligned} G &\to \operatorname{Aut}(G) \\ g &\mapsto \varphi_g \end{aligned}$$

is a homomorphism.

Proof:

1. We show it's homomorphic: $\varphi_g(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = \varphi_g(x)\varphi_g(y)$. We show it's bijective: $\varphi_{g^{-1}}$ is an inverse of φ_g.

2. Let $g, h \in G$. Then

$$\begin{aligned} \varphi_{gh}(x) = ghx(gh)^{-1} &= g(hxh^{-1})g^{-1} \\ &= \varphi_g(hxh^{-1}) = \varphi_g(\varphi_h(x)) \\ &= (\varphi_g \circ \varphi_h)(x) \end{aligned}$$

Notice the kernel of the map is $Z(G)$ since $\varphi_g = \mathrm{id}_G$ if and only if $x = gxg^{-1} \forall x \in G$. The image is $\operatorname{Inn}(G)$. Since this is the image of a group homomorphism, we know by Proposition 4.1.3 that

$$\operatorname{Inn}(G) \leq \operatorname{Aut}(G).$$

□

4.1.16. *Proposition*

Let $G = (a)$ be a cyclic group.

1. If G has finite order n, then $G \cong \mathbb{Z}/n\mathbb{Z}$.
2. If G has infinite order, then $G \cong \mathbb{Z}$.

***Proof*:**

1. Let $G = (a)$ with $\operatorname{ord}(a) = n$. Define

$$\begin{aligned} \varphi : \mathbb{Z}/n\mathbb{Z} &\longrightarrow G \\ \overline{k} &\longmapsto a^k. \end{aligned}$$

We will show that φ is an isomorphism.

We first need to check that φ is well-defined, i.e., we need to check that, if $\overline{k_1} = \overline{k_2}$, then $a^{k_1} = a^{k_2}$. Indeed, we have

$$\overline{k_1} = \overline{k_2} \Longleftrightarrow k_1 \equiv k_2 \pmod{n} \overset{\text{Prop 3.2.1(ii)}}{\Longleftrightarrow} a^{k_1} = a^{k_2}.$$

Note that this also shows that φ is injective. It is also surjective, since any element $x \in G$ is of the form $x = a^k$ for some $k \in \mathbb{Z}$, and therefore $x = a^k = \varphi\left(\overline{k}\right)$. Thus φ is bijective.

Finally, we show that φ is a homomorphism. Let $\overline{k_1}, \overline{k_2} \in \mathbb{Z}/n\mathbb{Z}$. Then

$$\varphi\left(\overline{k_1} + \overline{k_2}\right) = \varphi\left(\overline{k_1 + k_2}\right) = a^{k_1 + k_2} = a^{k_1} a^{k_2} = \varphi\left(\overline{k_1}\right)\varphi\left(\overline{k_2}\right).$$

2. Let $G = (a)$, with $\operatorname{ord}(a) = \infty$. Define

$$\begin{aligned} \varphi : \mathbb{Z} &\longrightarrow G \\ k &\longmapsto a^k. \end{aligned}$$

We will show that φ is an isomorphism. To show it's a homomorphism, let $k_1, k_2 \in \mathbb{Z}$ and note

$$\varphi(k_1 + k_2) = a^{k_1 + k_2} = a^{k_1} a^{k_2} = \varphi(k_1)\varphi(k_2).$$

By Proposition 3.2.6(ii), the elements a^k with $k \in \mathbb{Z}$ are all distinct. Thus, for any $j \in \mathbb{Z}$,

$$\varphi(j) = 1 \Longrightarrow a^j = 1 \Longrightarrow j = 0.$$

Therefore, φ is injective. It is also surjective since any element $x \in G$ is of the form $x = a^k$ for some $k \in \mathbb{Z}$ and therefore $x = a^k = \varphi(k)$.

□

4.2. Cosets

4.2.1. Definition: Coset

Let $H \leq G$. A left (resp. right) **coset** of H in G is a subset of G of the form

$$aH = \{ah : h \in H\} \qquad Ha = \{ha : h \in H\}$$

for some $a \in G$. Notationally we write $G/H =$ set of all left cosets of H in G and $H\backslash G$ for the converse. We remark $H = 1 \cdot H = H \cdot 1$ so H is both a left and right coset.

4.2.2. Example

1. Consider the dihedral groups D_{2n}. Notice the left cosets are $r^k H = \left(r^k, r^k s\right) = r^k s H$ for $0 \leq k < n$ and the right cosets are $H r^k = \left(r^k, s r^k\right) = \left(r^k, r^{-k} s\right)$ for $0 \leq k < n$. Thus $G/H \neq H \setminus G$.
2. Consider S_n with $n \geq 2$. If $\sigma \in S_n$ is even, then $\sigma A_n = A_n = A_n \sigma$. For n odd, we have $\sigma A_n = A_n \sigma$ is the set of all odd permutations in S_n. Then $S_n / A_n = \langle A_n, (1\ 2) A_n \rangle = \langle A_n, A_n (1\ 2) \rangle = A_n \backslash S_n$.

4.2.3. *Lemma*

Let $H \leq G$. The relation $\sim$ on G defined by $a \sim b \Longleftrightarrow a^{-1} b \in H$ for $a, b \in G$ is an equivalence relation.

Proof:

- *Reflexive:* For all $a \in G$, $a^{-1} a = 1 \in H$, so $a \sim a$.
- *Symmetric:* Let $a, b \in G$ and suppose $a \sim b$. Then $a^{-1} b \in H$. Then $\left(a^{-1} b\right)^{-1} \in H$ but thus $b^{-1} a \in H$ so $b \sim a$.
- *Transitive:* Let $a, bc \in G$. Suppose $a \sim b$ and $b \sim c$. Then $a^{-1} b, b^{-1} c \in H$. Then $\left(a^{-1} b\right)\left(b^{-1} c\right) = a^{-1} c \in H$. Thus $a \sim c$.

□

4.2.4. *Proposition*

Let $H \leq G$.

1. Let $a, b \in G$. Then
$$a^{-1}b \in H \iff b \in aH \iff aH = bH.$$
2. The left cosets of H in G form a partition of G.

Proof: Let $a, b \in G$. Then

$$\begin{aligned} a^{-1}b \in H &\iff a^{-1}b = h \text{ for some } h \in H \\ &\iff b = ah \text{ for some } h \in H \\ &\iff b \in aH \end{aligned}$$

It follows that

$$aH = \{x \in G : a^{-1}x \in H\}$$

i.e., aH is the equivalence class of a for the equivalence relation defined in the previous lemma. Since left cosets are the equivalence class for $\sim$, they form a partition of G and $b \in aH \iff aH = bH$.

□

4.2.5. *Proposition*

Let $H \leq G$. Then all the left cosets of H in G have the same cardinality.

Proof: Let $a \in G$. We have a map

$$\begin{aligned} H &\longrightarrow aH \\ h &\mapsto ah. \end{aligned}$$

It is bijective (with inverse $x \mapsto a^{-1}x$) so $|aH| = |H|$.

□

4.2.6. Definition: Index

Let $H \leq G$. The **index** of H in G is the number of left cosets of H in G. (This is the same as the number of right cosets). Notation: $[G : H]$.

4.2.7. *Proposition*

Let $K \leq H \leq G$. Then

$$[G : K] = [G : H] \cdot [H : K].$$

Proof: Let $\{a_i : i \in I\}$ be a complete set of representatives for the left cosets of H in G:

$$G = \bigcup_{i \in I} a_i H.$$

Let $\left\{b_j : j \in J\right\}$ be a complete set of representatives for the left cosets of K in H:

$$H = \bigcup_{j \in J} b_j K.$$

For any $i \in I$, left multiplication by a_i is injective. Then

$$a_i H = \bigcup_{j \in J} a_i b_j K$$

Then

$$\begin{aligned} G &= \bigcup_{i \in I} a_i H \\ &= \bigcup_{i \in I} \bigcup_{j \in J} a_i b_j K \end{aligned}$$

Thus $\left\{a_i b_j : i \in I, j \in J\right\}$ is a complete set of representatives for the left cosets of K in G. So $[G : K] = |I \times J| = |I| \cdot |J| = [G : H][H : K]$.

□

4.2.8. *Corollary:* Counting Formula

Let $H \leq G$. Then $|G| = [G : H] \cdot |H|$.

Proof: Take $K = \{1\}$ in the previous proposition.

□

4.2.9. *Corollary:* Lagrange's Theorem

Let G be a finite group. Let $H \leq G$. Then $|H|$ divides $|G|$.

Proof: Follows immediately from the counting formula.

□

4.2.10. ***Corollary***

Let G be a finite group and let $a \in G$. Then $\operatorname{ord}(a)$ divides $|G|$.

Proof: Notice $\operatorname{ord}(a) = |(a)| \mid |G|$ by Lagrange's Theorem.

□

4.2.11. ***Proposition***

Let G be a group with $H \leq G$. Then $gH = H \Longleftrightarrow g \in H$.

Proof: $(\Longrightarrow)$ First suppose $gH = H$. Then $\exists h \in H$ such that $gh \in H$. Then $\exists h' \in H$ such that $gh = h'$, so $g = h'h^{-1}$, meaning $g \in H$.

$(\Longleftarrow)$ Suppose $g \in H$.
- $(\subseteq)$ Let $h \in H$, so that $gh \in H$ clearly, meaning $gH \subseteq H$.
- $(\supseteq)$ Let $h \in H$, and define $h' = hg^{-1}$, and note $h' \in H$ since $g \in H$. Then $h = gh'$, so $h \in gH$, meaning $H \subseteq gH$.

□

4.3. Normal Subgroups

4.3.1. Remark

If S and T are subsets of a group G, we use the notation ST to refer to the set

$$ST = \{st : s \in S, t \in T\}.$$

Note that, with this notation, if S, T, and U are subsets of G, then $(ST)U = S(TU)$. If a set consists of a single element a, we may write a instead of $\{a\}$. Thus, for example, we will usually write aT instead of $\{a\}T$, with exactly the same meaning.

4.3.2. Definition: Normal Subgroup

Let G be a group. A subgroup H of G is a **normal subgroup** if $gHg^{-1} = H \forall g \in G$. We write $H \trianglelefteq G$ to indicate this.

We remark that a subgroup H of a group G is normal iff $N_G(H) = G$. We always have $H \trianglelefteq N_G(H)$ because if we let $g \in N_G(H)$, then $gHg^{-1} = H$ by definition. This also means that $N_G(H)$ is the largest subgroup of G satisfying this property.

4.3.3. Remark

Intuition behind normal subgroups on stack exchange

The reason why this seemingly arbitrary definition is so key is that it's the condition that allows taking the quotient of two groups to be a group. Suppose $H \leq G$ and suppose we use the Equivalence relation defined in Lemma 4.2.3 to create a set of cosets

$$G/H = \{[g] = gH : g \in G\}$$

The problem is that this is not a group in the general case. The natural way to induce a group structure is to make the map $G \to G/H$ a homomorphism, meaning that

$$[g_1 * g_2] = [g_1] *_{\text{new}} [g_2].$$

But this means

$$(g_1 g_2)H = [g_1 * g_2] = [g_1] *_{\text{new}} [g_2] = (g_1 H)(g_2 H) = g_1 (H g_2) H.$$

We notice that if $Hg_2 = g_2 H$, then right hand side would become $g_1 g_2 H H = g_1 g_2 H$ as desired, so this would become a well-defined operation. But this is exactly the condition for a normal subgroup.

4.3.4. *Proposition*

Let $H \leq G$. The following are equivalent:

1. $H \trianglelefteq G$
2. $gHg^{-1} \subseteq H \forall g \in G$
3. $gH = Hg \forall g \in G$
4. $gH \subseteq Hg \forall g \in G$
5. Every left coset is a right coset
6. $G/H = H \backslash G$.

Proof: $(i) \iff (iii)$: $H \trianglelefteq G \iff gHg^{-1} = H \forall g \in G \iff gH = Hg \forall g \in G$.

$(ii) \iff (iv)$: $gHg^{-1} \subseteq H \forall g \in G \iff gH \subseteq Hg \forall g \in G$.

$(i) \implies (ii)$: $H \trianglelefteq G \implies gHg^{-1} = H \forall g \in G \implies gHg^{-1} \subseteq H$.

$(ii) \implies (i)$: Suppose $gHg^{-1} \subseteq H \forall g \in G$. Replacing g by g^{-1} we get that $g^{-1}Hg \subseteq H \forall g \in G$. Thus $H \subseteq gHg^{-1} \forall g \in G$ via left and right multiplying, so $H = gHg^{-1} \forall g \in G$.

Thus the first 4 are equivalent. Now,

$(iii) \Rightarrow (vi)$ is clear.

$(vi) \Rightarrow (v)$ is clear.

$(v) \Rightarrow (iii)$: Suppose every left coset is a right coset. Let $g \in G$, then $gH = Ha$ for some $a \in G$. Since $g \in gH = Ha$, then $Ha = Hg$, so $gH = Hg$.

□

4.3.5. Example

1. If G is a group, $\{1\} \trianglelefteq G$ and $G \trianglelefteq G$. Note the first is because $g\{1\}g^{-1} = \{1\}$ is clear. Then if $h \in G$, then for $x = ghg^{-1}$ we have $h = g^{-1}xg$, so $h \in gGg^{-1}$, and thus $G \trianglelefteq G$ via (ii) in the previous proposition.
2. $(r) \trianglelefteq D_{2n}$. An arbitrary $g \in D_{2n}$ can be written $s^i r^j$. Then if $x \in s^i r^j (r) r^{-j} s^{-i}$, so $x = s^i r^k s^{-i} = r^{-k} \in (r)$, so this is true by (ii) again.
3. $A_n \trianglelefteq S_n$ To see this, let $\sigma \in S_n$ and suppose $\tau \in \sigma A_n \sigma^{-1}$, so $\tau = \sigma \prod^{2n} (a_i\ a_j) \sigma^{-1}$. But if σ is length k, then we can decompose it into k transpositions, and σ^{-1} is another k transpositions, so τ has $2n + 2k = 2(n + k)$ transpositions overall, meaning $\tau \in A_n$ and $A_n \trianglelefteq S_n$.
4. If H is a subgroup of index 2 of a group G, then $H \trianglelefteq G$. This is because $G/H = \{H, G \backslash H\} = H \backslash G$.
5. $V_r = \{1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \trianglelefteq S_4$. For all $\sigma \in S_4$, we have $\sigma \cdot 1 \sigma^{-1} \in V_4$. Any product of two disjoint transpositions will remain a product of two disjoint transpositions. Thus $\sigma(1\ 2)(3\ 4)\sigma^{-1} = (\sigma(1)\ \sigma(2))(\sigma(3)\ \sigma(4))$.

4.3.6. *Proposition*

If G is an abelian group, every subgroup is normal.

Proof: Suppose G is an abelian group and let $H \leq G$. Let $g \in G$ and let $ghg^{-1} \in gHg^{-1}$. Then since G is abelian, $ghg^{-1} = gg^{-1}h = h \in H$, so $gHg^{-1} \subseteq H$, so $H \trianglelefteq G$.

□

4.3.7. *Proposition*

If $K \leq H \leq G$ and $K \trianglelefteq G$, then $K \trianglelefteq H$.

Proof: Let $h \in H$. Since Then $hKh^{-1} = K$ since $H \leq G \Longrightarrow h \in G$, and since $K \leq H$, we have $K \trianglelefteq H$.

□

4.3.8. Remark

$K \trianglelefteq H \trianglelefteq G$ does **not** imply $K \trianglelefteq G$. For example, $\{1, (1\ 2)(3\ 4)\} \trianglelefteq V_4 \trianglelefteq A_4$, but $\{1, (1\ 2)(3\ 4)\} \ntrianglelefteq A_4$.

To see this, note $(1\ 3)((1\ 2)(3\ 4))(1\ 3) = (1\ 4)(2\ 3) \notin \{1, (1\ 2)(3\ 4)\}$.

4.3.9. *Proposition*

Let $\varphi : G_1 \to G_2$ be a group homomorphism.

1. If $H_2 \trianglelefteq G_2$, then $\varphi^{-1}(H_2) \trianglelefteq G_1$.
2. If $H_1 \trianglelefteq G_1$, then $\varphi(H_1) \trianglelefteq \operatorname{im}\varphi$.

Proof:

1. Let $H_2 \trianglelefteq G_2$. It suffices to show that $g\varphi^{-1}(H_2)g^{-1} \subseteq \varphi^{-1}(H_2) \forall g \in G_1$.

   Let $a \in G_1, h \in \varphi^{-1}(H_2)$. We want to show $aha^{-1} \in \varphi^{-1}(H_2)$. We have $\varphi(aha^{-1}) = \varphi(a)\varphi(h)\varphi(a^{-1})$. Since $h \in \varphi^{-1}(H_2)$, $\varphi(h) \in H_2$. Since $H \trianglelefteq G_2, \varphi(a)\varphi(h)\varphi(a)^{-1} \in H_2$ Then $\varphi(aha^{-1}) \in H_2 \Rightarrow aha^{-1} \in \varphi^{-1}(H_2)$.

2. Let $H_1 \trianglelefteq G_1$. It suffices to show $g\varphi(H_1)g^{-1} \subseteq \varphi(H_1) \forall g \in \operatorname{im}\varphi$.

   Let $b \in \operatorname{im}\varphi, k \in \varphi(H_1)$.T Then $b = \varphi(a)$ for some $a \in G_1$ and $k = \varphi(h)$ for some $h \in H_1$. Then $bkb^{-1} = \varphi(a)\varphi(h)\varphi(a)^{-1} = \varphi(aha^{-1})$. Since $H_1 \trianglelefteq G_1, aha^{-1} \in H_1$. Then $bkb^{-1} = \varphi(aha^{-1}) \in \varphi(H_1)$.

□

4.3.10. Remark

In general, $H_1 \trianglelefteq G_1 \nRightarrow \varphi(H_1) \trianglelefteq G_2$. For example, let H be a subgroup of a group G which is not normal. If the inclusion map $i : H \longrightarrow G$, then $H \trianglelefteq H$ but $i(H) = H \ntrianglelefteq G$.

4.3.11. *Proposition*

Let $\varphi : G_1 \to G_2$ be a group homomorphism. Then $\ker\varphi \trianglelefteq G_1$.

Proof: $\ker\varphi = \varphi^{-1}(\{1\})$ so this is a special case of previous prop.

□

4.3.12. *Proposition*

Let G be a group and H be a subgroup of G.

1. The operation on G/H defined by
$$aH \cdot bH = abH$$
is well-defined if and only if H is a normal subgroup of G.
2. If the operation in (i) is well-defined, then it makes G/H into a group.

Proof:

1. Suppose that the operation is well-defined. Therefore, for all $a, a', b, b' \in G$, if $aH = a'H$ and $bH = b'H$, then $abH = a'b'H$. We will show that $gHg^{-1} \subseteq H$ for all $g \in G$. Let $g \in G$ and let $h \in H$. Taking $a = 1, a' = h$, and $b = b' = g^{-1}$ above, we deduce that $g^{-1}H = hg^{-1}H$. By Proposition 4.2.4, this implies $ghg^{-1} \in H$. This shows that $gHg^{-1} \subseteq H \forall g \in G$ and therefore, by Proposition 4.3.3, $H \trianglelefteq G$.

   Conversely, suppose H is a normal subgroup of G and let $a, a', b, b' \in G$. Suppose $aH = a'H$ and $bH = b'H$. We want to show that $abH = a'b'H$. Since $aH = a'H$ and $bH = b'H$, $\exists h_1, h_2 \in H$ such that $a' = ah_1$ and $b' = bh_2$. Thus
$$a'b' = ah_1bh_2 = ab(b^{-1}h_1b)h_2$$
   and therefore
$$(ab)^{-1}a'b' = (b^{-1}h_1b)h_2.$$
   Since H is a normal subgroup, we have that $b^{-1}h_1b \in H$. Then $(ab)^{-1}a'b' \in H$ and therefore $abH = a'b'H$ by Proposition 4.2.4.

2. Suppose that the operation in (i) is well-defined. We will check that G/H is a group under this operation.
   - *Associativity*: Let $a, b, c \in G$. Then:
$$aH \cdot (bH \cdot cH) = aH \cdot bcH = a(bc)H = (ab)cH = abH \cdot cH = (aH \cdot bH) \cdot cH.$$
   - *Identity*: The coset $H = 1H$ is an identity.
   - *Inverses*: For all $g \in G$, the coset gH has inverse $g^{-1}H$.

□

4.3.13. Remark

Let $H \leq G$. We could have defined
$$\begin{aligned} aH \cdot bH &= aHbH \\ &= \{st : s \in aH, t \in bH\} \\ &= \{ah_1bh_2 : h_1, h_2 \in H\} \end{aligned}$$

This is always well defined. If $H \trianglelefteq G$, then $aHbH = abH$.

4.3.14. *Proposition*

Let G be a group. Let H and K be subgroups of G. Then HK is a subgroup of G if and only if $HK = KH$.

Proof: Suppose that HK is a subgroup. First we show that $KH \subseteq HK$. Note that $H \leq K$ and $K \leq HK$. Let $a \in KH$. Write $a = kh$. Write $a = kh$, with $k \in K$ and $h \in H$. Since $k, h \in HK$ and HK is a subgroup, it follows that $a = kh \in HK$. Now we show that $HK \subseteq KH$. Let $a \in HK$. Since HK is a subgroup, we have that $a^{-1} \in HK$. Therefore $a^{-1} = hk$ for some $h \in H$ and $k \in K$. Thus $a = (hk)^{-1} = k^{-1}h^{-1}$. Since $h^{-1} \in H$ and $k^{-1} \in K$, it follows that $a = k^{-1}h^{-1} \in KH$.

Conversely, suppose $HK = KH$. Clearly, $1 = 1 \cdot 1 \in HK$. Now let $a, b \in HK$. Then $a = h_1k_1$ and $b = h_2k_2$ for some $h_1, h_2 \in H$ and $k_1, k_2 \in K$. Therefore we have that $ab^{-1} = h_1k_1k_2^{-1}h_2^{-1}$. Let $k_3 = k_1k_2^{-1} \in K$ and let $h_3 = h_2^{-1} \in H$. Then $k_3h_3 \in KH$. Since $HK = KH$, we can write $k_3h_3 = h_4k_4$ for some $h_4 \in H$ and $k_4 \in K$. Therefore $ab^{-1} = h_1k_3h_3 = h_1h_4k_4$. Since $h_1h_4 \in H$ and $k_4 \in K$, we have $ab^{-1} \in HK$.

□

4.3.15. *Proposition*

If H and K are finite subgroups of a group then

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

Proof: Notice that HK is a union of left cosets of K, namely,

$$HK = \cup_{h \in H}\, hK.$$

Since each coset of K has $|K|$ elements it suffices to find the number of *distinct* left cosets of the form $hK, h \in H$. But $h_1K = h_2K$ for $h_1, h_2 \in H$ if and only if $h_2^{-1}h_1 \in K$. Thus

$$h_1K = h_2K \Leftrightarrow h_2^{-1}h_1 \in H \cap K \Leftrightarrow h_1(H \cap K) = h_2(H \cap K).$$

Thus the number of distinct cosets of the form hK, for $h \in H$, is the number of distinct cosets $h(H \cap K)$, for $h \in H$. The latter number, by Lagrange's Theorem, equals $\frac{|H|}{|H \cap K|}$. Thus HK consists of $\frac{|H|}{|H \cap K|}$ distinct cosets of K (each of which has K elements) which gives the formula above.

□

4.3.16. ***Corollary***

Let G be a group. Let H and K be subgroups of G. If $H \leq N_G(K)$, then HK is a subgroup of G.

In particular, if $K \trianglelefteq G$ then $HK \leq G$ for any $H \leq G$.

Proof: We prove that $KH = HK$. First we show that $HK \subseteq KH$. Let $a \in HK$. Then $a = hk$ for some $h \in H$ and $k \in K$. We can write $a = (hkh^{-1})h$. Since $H \leq N_G(K)$, it follows that $hkh^{-1} \in K$ and therefore $a \in KH$.

Now we show that $KH \subseteq HK$. Let $a \in KH$. Then $a = kh$ for some $k \in K$ and $h \in H$. We can write $a = h(h^{-1}kh)$. Since $H \leq N_G(K)$, it follows that $h^{-1}kh \in K$ and therefore $a \in HK$.

□

4.4. Quotient Groups

4.4.1. Definition: Quotient Group

Let $H \trianglelefteq G$. The **quotient group** G modulo H is the set G/H under the operation defined by $aH \cdot bH = abH$. Notation: We may write $\overline{a}$ instead of aH.

4.4.2. Definition: Canonical Projection

Let $H \trianglelefteq G$. The **canonical projection** of G onto G/H is the homomorphism $\pi : G \to G/H$ defined by $\pi(a) = aH$ for all $a \in G$.

We remark that $\ker \pi = H$. This is because

$$g \in \ker \pi \Leftrightarrow \pi(g) = 1 \cdot H \Leftrightarrow gH = H \overset{\text{Prop 4.2.11}}{\iff} g \in H.$$

4.4.3. ***Proposition***

Let $H \leq G$. Then $H \trianglelefteq G$ if and only if H is the kernel of some group homomorphism $\varphi : G \to K$.

Proof: ($\Longleftarrow$) We proved that the kernel of a group homomorphism is a normal subgroup of the domain in Proposition 4.3.10.

($\Longrightarrow$) If $H \trianglelefteq G$, then $H = \ker \pi$ by the argument in the definition above.

□

4.4.4. Example

1. Let $n \in \mathbb{Z}^+$. Then $n\mathbb{Z}$ is a normal subgroup of $\mathbb{Z}$. This is because for $m \in \mathbb{Z}$, $m + n\mathbb{Z} + (-m) = n\mathbb{Z}$ (easily follows from $\mathbb{Z}$ being abelian - this is Proposition 4.3.5).

   The quotient group $\mathbb{Z}/n\mathbb{Z}$ is the set of integers modulo n. To see this is consistent with the definition, notice if $a, b \in \mathbb{Z}/n\mathbb{Z}$ then our left cosets are $a + n\mathbb{Z}$ and $b + n\mathbb{Z}$, and our group operation is $a + b + n\mathbb{Z}$.

   The canonical projection is the map $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ defined by $a \to \overline{a} = a + n\mathbb{Z}$.

2. Consider the dihedral group D_{2n} with its usual presentation and let $H = (r)$. Then $H \trianglelefteq D_{2n}$ (proved in Example 4.3.4) and $G/H = \{H, sH\} = \underline{\{\overline{1}, \overline{s}\}}$, which is isomorphic to $\mathbb{Z}/2\mathbb{Z}$. The canonical projection $D_{2n} \to D_{2n}/H$ is defined by $r^j \mapsto \overline{r^j} = \overline{1}, r^j s \mapsto \overline{r^j s} = \overline{s}$.

4.4.5. Remark

Notice $f(f^{-1}(A)) \subseteq A$. To show this, let $x \in f(f^{-1}(A))$ so $\exists y \in f^{-1}(A)$ such that $f(y) = x$. But $f(y) \in A$, so $x \in A$.

Also, $f^{-1}(f(A)) \supseteq A$. Let $a \in A$. Then $f(a) \in f(A)$ and $a \in f^{-1}(f(a)) \subseteq f^{-1}(f(A))$.

4.4.6. *Theorem:* Correspondence Theorem

Let $H \trianglelefteq G$. Let $\pi : G \to G/H$ be the canonical projection. Then the map

$$\begin{aligned} f : \{\text{subgroups of } G \text{ containing } H\} &\longrightarrow \{\text{subgroups of } \ G/H\} \\ K &\mapsto \pi(K) = K/H. \end{aligned}$$

is well-defined and bijective. The inverse is given by $M \to \pi^{-1}(M)$.

Also:

1. If K is a subgroup of G containing H, then $K \trianglelefteq G$ if and only if $\pi(K) \trianglelefteq G/H$.
2. If K_1, K_2 are subgroups of G containing H, then $K_1 \leq K_2 \iff \pi(K_1) \leq \pi(K_2)$.

Proof: To check f is well-defined, we just need to check that if K is a subgroup of G containing H, then $\pi(K)$ is a subgroup of G/H. But π is a homomorphism, so this follows from Prop 4.1.3(i).

By Prop 4.1.3(ii), if $\mathcal{K}$ is a subgroup of G/H, then $\pi^{-1}(\mathcal{K})$ is a subgroup of G, so we have that $H = \pi^{-1}(\{\overline{1}\}) \subseteq \pi^{-1}(\mathcal{K})$ since $\{\overline{1}\} \leq M$. This shows that the function

$$\begin{gathered} \{\text{subgroups of } \ G/H\} \longrightarrow \{\text{subgroups of } G \text{ containing } H\} \\ \mathcal{K} \mapsto \pi^{-1}(\mathcal{K}) \end{gathered}$$

We want to show that f and g are inverses of each other:

1. If $K \leq G$ and $H \leq K$, then $\pi^{-1}(\pi(K)) = K$.
2. If $M \leq G/H$ then $\pi(\pi^{-1}(M)) = M$.

We show these as follows:

1. Let $K \leq G$ such that $H \leq K$. We want to show $\pi^{-1}(\pi(K)) = K$. So $K \subseteq \pi^{-1}(\pi(K))$. Now we need to show $\pi^{-1}(\pi(K)) \subseteq K$. Let $x \in \pi^{-1}(\pi(K))$. Then $\pi(x) \in \pi(K)$. Thus $\pi(x) = \pi(a)$ for some $a \in K$. Then $\pi(a^{-1}x) = \overline{1}$.
2. Notice this holds because π is surjective.

Now we show the remaining parts:

1. If $K \leq G$ such that $H \leq K$, then $K \trianglelefteq G \iff \pi(K) \trianglelefteq G/H$.

$(\Longrightarrow)$ If $K \trianglelefteq G$, then $\pi(K) \trianglelefteq \operatorname{im} \pi = G/H$. $(\Longleftarrow)$ If $\pi(K) \trianglelefteq G/H$, then $K = \pi^{-1}(\pi(K)) \trianglelefteq G$.

2. If K_1, K_2 are subgroups of G containing H, then $K_1 \leq K_2 \Longleftarrow \pi(K_1) \leq \pi(K_2)$.

$(\Longrightarrow)$ is clear

$(\Longleftarrow)$ If $\pi(K_1) \leq \pi(K_2)$, then $K_1 = \pi^{-1}(\pi(K_1)) \leq \pi^{-1}(\pi(K_2)) = K_2$.

□

4.5. Isomorphism Theorems

4.5.1. ***Theorem***

Let $\varphi : G_1 \to G_2$ be a group homomorphism. Let $H \trianglelefteq G_1$. Let $\pi : G_1 \to G_1/H$ denote the canonical projection. Suppose that $H \leq \ker\varphi$. Then, $\exists$ a unique homomorphism $\overline{\varphi} : G_1/H \to G_2$ such that $\varphi = \overline{\varphi} \circ \pi$. The homomorphism $\overline{\varphi}$ is defined by $aH \mapsto \varphi(a)$.

$$\begin{tikzcd}
G_1 \arrow[r, "\varphi"] \arrow[d, "\pi"] & G_2 \\
G_1/H \arrow[ur, dashed, "\overline{\varphi}"'] &
\end{tikzcd}$$

Proof: We first check that the map

$$\begin{aligned} \overline{\varphi} : G_1/H &\longrightarrow G_2 \\ aH &\longmapsto \varphi(a) \end{aligned}$$

is a well-defined homomorphism.

To prove this map is well-defined, observe that, for all $a, b \in G_1$,

$$\begin{aligned} aH = bH &\overset{\text{(Prop 4.2.4)}}{\Longrightarrow} a^{-1}b \in H \Rightarrow a^{-1}b \in \ker\varphi \Rightarrow \varphi(a^{-1}b) = 1 \\ &\Rightarrow \varphi(a)^{-1}\varphi(b) = 1 \Rightarrow \varphi(a) = \varphi(b) \end{aligned}$$

To prove that $\overline{\varphi}$ is a homomorphism, observe that, for all $a, b \in G_1$,

$$\overline{\varphi}(aH \cdot bH) = \overline{\varphi}(abH) = \varphi(ab) = \varphi(a)\varphi(b) = \overline{\varphi}(aH)\overline{\varphi}(bH).$$

To check that $\varphi = \overline{\varphi} \circ \pi$, observe that, for all $a \in G_1$,

$$(\overline{\varphi} \circ \pi)(a) = \overline{\varphi}(\pi(a)) = \overline{\varphi}(aH) = \varphi(a).$$

For the uniqueness claim, note that, if $\overline{\varphi'} : G_1/H \to G_2$ is a homomorphism such that $\varphi = \overline{\varphi'} \circ \pi$, then for all $aH \in G_1/H$,

$$\overline{\varphi}(aH) = \overline{\varphi'}(\pi(a)) = \left(\overline{\varphi'} \circ \pi\right)(a) = \varphi(a),$$

so $\overline{\varphi'} = \overline{\varphi}$.

□

4.5.2. *Theorem:* First Isomorphism Theorem

Let $\varphi : G_1 \to G_2$ be a group homomorphism and let $K = \ker \varphi$. Then
1. $K \trianglelefteq G_1$
2. $\operatorname{im} \varphi \leq H$
3. The map

$$\begin{aligned} \overline{\varphi} : G_1 / K &\longrightarrow \operatorname{im} \varphi \\ aK &\longmapsto \varphi(a) \end{aligned}$$

is a well-defined isomorphism.

Proof: The fact that $K \trianglelefteq G_1$ follows from Proposition 4.3.10.

The fact that $\operatorname{im} \varphi \leq H$ follows from a note in Definition 4.1.4.

The map $\overline{\varphi}$ is a well-defined homomorphism by the previous theorem (and the fact that it takes values in $\operatorname{im} \varphi$). Surjectivity is immediate. We finally prove injectivity. Let $aK \in G_1 / K$. Then via Proposition 4.1.5,

$$\overline{\varphi}(aK) = 1 \Rightarrow \varphi(a) = 1 \Rightarrow a \in K \Rightarrow aK = K.$$

□

4.5.3. Remark

The idea of the First Isomorphism Theorem is to "quotient out" some elements in the group in order to make the homomorphism injective. Obviously, any homomorphism φ with range $\operatorname{im} \varphi$ is surjective, so if we can only make the homomorphism injective, it becomes a bijection and we get an isomorphism. To do this, we group up elements of G_1 according to whether they're in $\ker \varphi$ or not–i.e., we create a coset of all elements in $\ker \varphi$ and other, mutually exclusive cosets. This means there will be only one element in the kernel of the new homomorphism $\overline{\varphi} : G_1 / \ker \varphi \longrightarrow \operatorname{im} \varphi$, so we have an isomorphism between them.

4.5.4. *Corollary*

1. If $\varphi : G_1 \to G_2$ is a surjective group homomorphism, then $G_1 / \ker \varphi \cong G_2$.
2. If $\varphi : G_1 \to G_2$ is an injective group homomorphism, then $G_1 \cong \varphi(G_1)$.

Proof:
1. Suppose that $\varphi : G_1 \to G_2$ were a surjective group homomorphism. Thus $G_2 = \operatorname{im} \varphi$, so by the previous proposition, $G_1 / \ker \varphi \cong G_2$.
2. Suppose that $\varphi : G_1 \to G_2$ were an injective group homomorphism. Thus $\ker \varphi = \{1\}$, so $G_1 / \ker \varphi = G_1$. Then by the previous theorem, $G_1 \cong \operatorname{im} \varphi$.

□

4.5.5. Example

1. The map $\det : \mathrm{GL}_n(\mathbb{Q}) \to \mathbb{Q}^\times$ is a surjective homomorphism with kernel $\mathrm{SL}_n(\mathbb{Q})$. We deduce from the First Isomorphism Theorem that $\mathrm{GL}_n(\mathbb{Q}) / \mathrm{SL}_n(\mathbb{Q}) \cong \mathbb{Q}^\times$.
2. Consider the group S_4, which we defined as the set of permutations of $\{1, 2, 3, 4\}$. Consider the following three partitions of the set:

$$\Pi_1 = \{\{1, 2\}, \{3, 4\}\}$$
$$\Pi_2 = \{\{1, 3\}, \{2, 4\}\}$$
$$\Pi_3 = \{\{1, 4\}, \{2, 3\}\}.$$

An element $\sigma \in S_4$ permutes the four indices $1, 2, 3, 4$ and thus it also permutes the three partitions Π_1, Π_2, Π_3. We denote by $\sigma(\Pi_i)$ the partition obtained by applying σ to all the indices in the partition Π_i. For example

$$\sigma(\Pi_1) = \{\{\sigma(1), \sigma(2)\}, \{\sigma(3), \sigma(4)\}\}.$$

We define a map $\varphi : S_4 \to S_3$ by defining $\varphi(\sigma)$ to be the permutation in S_3 such that $\sigma(\Pi_i) = \Pi_{\varphi(\sigma)(i)}$ for $i = 1, 2, 3$. One easily checks that this map is a homomorphism with kernel

$$V_4 = \{1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}.$$

By the First Isomorphism Theorem, we deduce that $S_4/V_4 \cong \operatorname{im} \varphi$. Moreover, since $|S_4/V_4| = 6 = |S_3|$, the homomorphism φ is surjective, so $S_4/V_4 \cong S_3$.

4.5.6. *Theorem:* Second Isomorphism Theorem

Let G be a group. Let $H \leq G$ and let $K \trianglelefteq G$ (more generally, this applies when $H \leq N_G(K)$). Then

1. $HK \leq G$
2. $K \trianglelefteq HK$
3. $H \cap K \trianglelefteq H$
4. $HK/K \cong H/H \cap K$.

$$\begin{tikzcd}
 & HK \arrow[dl] \arrow[dr, "\trianglelefteq"] & \\
H \arrow[dr, "\trianglelefteq"] & & K \arrow[dl] \\
 & H \cap K &
\end{tikzcd}$$

Proof: The fact that HK is a subgroup of G follows from Corollary 4.3.16. Since $H \leq N_G(K)$ by assumption and $K \leq N_G(K)$ trivially, it follows that $HK \leq N_G(K)$. Therefore $K \trianglelefteq HK$. Thus the quotient group is well-defined.

Consider the map

$$\begin{aligned} \varphi : H &\longrightarrow HK/K \\ a &\longmapsto aK. \end{aligned}$$

For all $a, b \in H$,

$$\varphi(ab) = abK = aK \cdot bK = \varphi(a)\varphi(b),$$

so φ is a homomorphism. Note that, for $h \in H$,

$$h \in \ker \varphi \Longleftrightarrow \varphi(h) = K \Longleftrightarrow hK = K \Longleftrightarrow h \in K \Longleftrightarrow h \in H \cap K.$$

Thus $\ker \varphi = H \cap K$. Since every element in HK/K is of the form hK for some $h \in H$, the map φ is surjective. By the First Isomorphism Theorem, $H \cap K \trianglelefteq H$ and the map

$$\begin{aligned} \overline{\varphi} : H/H \cap K &\longrightarrow HK/K \\ a(H \cap K) &\longmapsto aK \end{aligned}$$

yields an isomorphism between $H/H \cap K$ and HK/K.

□

4.5.7. *Theorem:* Third Isomorphism Theorem

Let G be a group. Let H and K be normal subgroups of G and suppose that $H \leq K$. Then $K/H \trianglelefteq G/H$ and

$$(G/H)/(K/H) \cong G/K.$$

Proof: The kernel of the canonical projection $\pi : G \to G/K$ is precisely K. Since $H \trianglelefteq G$ and $H \leq K$, it follows from Theorem 4.5.1 that the map

$$\begin{aligned} \varphi : G/H &\longrightarrow G/K \\ aH &\longmapsto aK \end{aligned}$$

is a well-defined homomorphism. It is clearly surjective. Also note that

$$\ker \varphi = \{gH \in G/H : gK = K\} \overset{\text{Prop 4.2.11}}{=} \{gH \in G/H : g \in K\} = K/H.$$

Therefore, by the First Isomorphism Theorem, it follows that $K/H \trianglelefteq G/H$ and

$$(G/H)/(K/H) \cong G/K.$$

□

4.6. Simple Groups

4.6.1. Definition: Simple Group

A group G is **simple** if $|G| > 1$ and the only normal subgroups of G are $\{1\}$ and G.

4.6.2. Example

Non-examples

1. $\{1\} \trianglelefteq (r) \trianglelefteq D_{2n}$, so D_{2n} is not simple.
2. For $n \geq 3$, $\{1\} \trianglelefteq A_n \trianglelefteq S_n$, so S_n is not simple.
3. $\{1\} \trianglelefteq V_4 \trianglelefteq A_4$ so A_4 is not simple.

4.6.3. *Theorem*

Let G be an abelian group. Then G is simple if and only if G is cyclic of finite prime order.

Proof: ($\Longleftarrow$) Suppose $G = (a)$ is cyclic of prime order p. G has only two subgroups: $\{1\}, G$. So G is simple.

($\Longrightarrow$) Suppose G is simple. Then $G \neq \{1\}$, so $\exists a \in G$ with $a \neq 1$. Then

$$\{1\} \neq (a) \trianglelefteq G$$

(since G is abelian, every subgroup of G is normal). Then $G = (a)$. If $\operatorname{ord}(a) = \infty$, then $\{1\} \neq \left(a^d\right) \ntrianglelefteq (a)$, so G would not be simple ($d \geq 2$). Then $\operatorname{ord}(a) = n$ for some $n \in \mathbb{Z}_{>1}$. Recall (normal) subgroups of (a) are in bijection with the positive divisors of n. Since G is simple, n must be prime.

□

4.6.4. *Lemma:* 1

For $n \geq 3$, A_n is generated by the 3-cycles in S_n.

Proof: Note: this proof is currently incorrect because it does not include all cases in the second part.

Recall that the alternating group A_n is the set of all even permutations of S_n under composition. Then recall that permutations of S_n are even if and only if they can be written as a product of an even number of transpositions.

We begin by showing a permutation that is the product of 3-cycles is a member of A_n. Let $\sigma \in S_n$ be given by

$$\sigma = \prod_{t=1}^{m} (a_i\ a_j\ a_k)$$

for some number $m \in \mathbb{N}$ of (i, j, k) triplets where no two of i, j, k are equal. Notice since $n \geq 3$, we must have $m \geq 1$. Then observe $(a_i\ a_j\ a_k) = (a_i\ a_k)(a_i\ a_j)$. Thus

$$\sigma = \prod_{t=1}^{2m} (a_i\ a_k)(a_i\ a_j),$$

i.e., we can write σ as a product of $2m$ transpositions, so $\sigma \in A_n$.

In the other direction, let $\sigma \in A_n$, so that

$$\sigma = \prod_{t=1}^{2m} (a_i\ a_j)$$

where $m \in \mathbb{N}$ and $i \neq j$ for each (i, j) pair. Consider two consecutive terms, $(a_i\ a_j)$ and $(a_k\ a_l)$. Notice $(a_i\ a_j)(a_k\ a_l) = (a_i\ a_j\ a_k)(a_k\ a_l\ a_j)$. Thus

$$\sigma = \prod_{t=1}^{m} (a_i\ a_j\ a_k)(a_k\ a_l\ a_j)$$

so any $\sigma \in A_n$ can be written as a product of 3-cycles.

Thus, we have shown that the alternating group A_n is generated by the set of all 3-cycles in S_n.

□

4.6.5. ***Lemma:*** **2**

For $n \geq 5$, every two 3-cycles in A_n are conjugate. I.e., if $\gamma_1, \gamma_2 \in A_n$ are 3-cycles, $\exists \sigma \in A_n$ such that $\sigma \gamma \sigma^{-1} = \gamma_2$.

Proof: Let $(a_1\ a_2\ a_3), (b_1, b_2, b_3) \in A_n$. Choose $\sigma \in S_n$ such that $\sigma(a_1) = b_1, \sigma(a_2) = b_2$ and $\sigma(a_3) = b_3$. Then

$$\sigma(a_1\ a_2\ a_3)\sigma^{-1} = (\sigma(a_1)\ \sigma(a_2)\ \sigma(a_3)) = (b_1\ b_2\ b_3).$$

If $\sigma \in A_n$, we are done. Thus suppose $\sigma \notin A_n$. Choose two different numbers $a_4, a_5 \in \{1, 2, ..., n\} \setminus \{a_1, a_2, a_3\}$ (which is possible because $n \geq 5$).

Let $\tau = \sigma(a_4\ a_5)$. Then $\tau \in A_n$ and

$$\begin{aligned} \tau(a_1\ a_2\ a_3)\tau^{-1} &= \sigma(a_4\ a_5)(a_1\ a_2\ a_3)(a_4\ a_5)\sigma^{-1} \\ &= \sigma(a_1\ a_2\ a_3)\sigma^{-1} \\ &= (b_1\ b_2\ b_3). \end{aligned}$$

□

4.6.6. *Lemma:* 3

For $n \geq 5$, if H is a non-trivial normal subgroup of A_n, then H contains a 3-cycle.

Proof: Let $\{1\} \neq H \trianglelefteq A_n$. Notice that if $\sigma \in H$, $\tau \in A_n$, so $\tau\sigma\tau^{-1}\sigma^{-1} \in H$. Let $1 \neq \sigma \in H$. Let

$$\sigma = \gamma_1\gamma_2 \cdots \gamma_r$$

be the cycle decomposition of σ.

Case 1: Suppose at least one of the γ_i's has length ≥ 4. Without loss of generality, say γ_1 has length ≥ 4. Write $\gamma_1 = (a_1\ a_2\ \ldots\ a_k)$. Let $\tau = (a_1\ a_2\ a_3)$. Then

$$\begin{aligned}
\tau\sigma\tau^{-1}\sigma^{-1} &= \tau\gamma_1\tau^{-1}\tau\gamma_2\tau^{-1}\cdots\tau\gamma_r)\tau^{-1}\gamma_r^{-1}\cdots\gamma_2^{-1}\gamma_1^{-1} \\
&= \tau\sigma\tau^{-1}\cdots\gamma_r\gamma_r^{-1}\cdots\gamma_2^{-1}\gamma_1^{-1} \\
&= (a_1\ a_2\ a_3)(a_1\ a_2\ \ \cdots\ \ a_k)(a_3\ a_2\ a_1)(a_k\ \ \cdots\ \ a_2\ a_1) \\
&= (a_1\ a_2\ a_3\ a_1\ a_4\ \ \cdots\ \ a_k)(a_k\ \ \cdots\ \ a_4\ a_3\ a_2\ a_1) \\
&= (a_1\ a_2\ a_4) \in H.
\end{aligned}$$

Case 2: Suppose there are at least two 3-cycles, among $\gamma_1, \cdots, \gamma_r$. Without loss of generality γ_1, γ_2 are 3-cycles. Write $\gamma_1 = (a_1\ a_2\ a_3)$ and $\gamma_2 = (a_4\ a_5\ a_6)$. Let $\tau = (a_1\ a_2\ a_4) \in A_n$. Then

$$\begin{aligned}
\tau\sigma\tau^{-1}\sigma^{-1} &= \tau\gamma_1\tau^{-1}\tau\gamma_2\tau^{-1}\gamma_2\tau^{-1}\gamma_2^{-1}\gamma_1^{-1} \\
&= (a_2\ a_4\ a_3)(a_1\ a_5\ a_6)(a_6\ a_5\ a_4)(a_3\ a_2\ a_1) \\
&= (a_1\ a_2\ a_5\ a_3\ a_4) \in H.
\end{aligned}$$

Then we are in case 1.

Case 3: Suppose one of the γ_i's is a 3-cycle and all the others are transpositions. Without loss of generality γ_1 is the 3-cycle. Then

$$\sigma^2 = \gamma_1^2\gamma_2^2 \cdots \gamma_r^2 = \gamma_1^2$$

is a 3-cycle in H.

Case 4: Suppose σ is the product of two disjoint transpositions. Write $\sigma = (a_1\ a_2)(a_3\ a_4)$. Choose $a_5 \in \{1, 2, \ldots, n\} \setminus \{a_1, a_2, a_3, a_4\}$ (possible because $n \geq 5$). Let $\tau = (a_1\ a_2\ a_5)$. Then

$$\begin{aligned}
\tau\sigma\tau^{-1}\sigma^{-1} &= \tau(a_1\ a_2)\tau^{-1}(a_1\ a_2) \\
&= (a_2\ a_5)(a_1\ a_2) \\
&= (a_1\ a_5\ a_2) \in H.
\end{aligned}$$

Case 5: Suppose there are at least two transpositions among the γ_i's. Without loss of generality γ_1, γ_2 are transpositions. Write $\gamma_1 = (a_1\ a_2), \gamma_2 = (a_3\ a_4)$. Then $\tau = (a_1\ a_2\ a_3) \in A_n$. Then

$$\begin{aligned}
\tau\sigma\tau^{-1}\sigma^{-1} &= \tau\gamma_1\tau^{-1}\tau\sigma_2\tau^{-1}\gamma_2^{-1}\gamma_1^{-1} \\
&= (a_2\ a_3)(a_1\ a_4)(a_3\ a_4)(a_1\ a_2) \\
&= (a_1\ a_3)(a_2\ a_4) \in H.
\end{aligned}$$

So we are in case 4.

□

4.6.7. *Theorem*

For $n \geq 5$, A_n is simple.

Proof: Let $\{1\} \neq H \trianglelefteq A_n$. We want to show $H = A_n$. By Lemma 3, H contains a 3-cycle. By Lemma 2, since $H \trianglelefteq A_n$ and H contains a 3-cycle, H contains all the 3-cycles. By Lemma 1, this implies $H = A_n$.

□

4.7. Normal Towers

4.7.1. Definition: Normal Tower and Factor Group

Let G be a group. A **normal tower** of G is a sequence

$$\{1\} = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_k = G.$$

The quotients H_i/H_{i-1} are called the **factor groups** of this normal tower.

4.7.2. Definition: Composition Series

Let G be a group. A **composition series** of G is a normal tower of G in which all the factor groups are simple. In this case, the factor groups are called the **composition factors** of G.

4.7.3. Remark

Let G be a group and let H be a normal subgroup of G. Then H is a maximal proper subgroup of G if and only if G/H is a simple group.

Therefore, a composition series of G is a normal tower in which each subgroups is a maximal proper normal subgroup of the next one.

4.7.4. Example

For example,

$$\{1\} \trianglelefteq ((1\ 2)(3\ 4)) \trianglelefteq V_4 \trianglelefteq A_4 \trianglelefteq S_4$$

This is a composition series of S_4. Another example of a composition series is

$$\{1\} \trianglelefteq (r^3)) \trianglelefteq (r) \trianglelefteq D_{30}.$$

Also for $n \geq 5$, we have

$$\{1\} \trianglelefteq A_n \trianglelefteq S_n$$

4.7.5. *Theorem*

Every finite group G has a composition series.

Proof: We proceed by strong induction on $|G|$. If $|G| = 1$, then $|G = \{1\}$ and $\{1\}$ is a composition series of length zero. Let $n \geq 2$ and suppose that every group of order $< n$ has a composition series.

Let G be a group with $|G| = n$. Let $H \trianglelefteq G$ be a maximal proper normal subgroup of G. Then G/H is simple and $|H| < n$. By the induction hypothesis H has a composition series:

$$\{1\} = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_k = H$$

Then

$$\{1\} = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_k \trianglelefteq N_{k+1} = G$$

is a composition series of G.

□

4.7.6. *Theorem:* Jordan-Hölder Theorem

Let G be a finite group with $|G| > 1$. If

$$\{1\} = M_0 \trianglelefteq M_1 \trianglelefteq \cdots \trianglelefteq M_r = G$$
$$\{1\} = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_s = G$$

are composition series of G, then $r = s$ and $\exists \sigma \in S_r$ such that

$$M_{\sigma(i)}/M_{\sigma(i)-1} \cong N_i/N_{i-1} \text{ for } 1 \leq i \leq r.$$

Proof: We proceed by strong induction on $|G|$. If $|G| = 2$, then G is simple, so G has a unique composition series:

$$\{1\} \trianglelefteq G.$$

Then we are done.

Let $n \geq 3$. Suppose the statement is true for all groups G with $1 < |G| < n$. Let G be a group with $|G| = n$. If G is simple, $\{1\} \trianglelefteq G$ is the unique composition series and we are done, so suppose that G is not simple.

Let

$$\{1\} = M_0 \trianglelefteq M_1 \trianglelefteq \cdots \trianglelefteq M_r = G$$
$$\{1\} = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_s = G$$

be composition series of G.

Case 1: Suppose $M_{r-1} = N_{s-1}$. Then

$$\{1\} = M_0 \trianglelefteq M_1 \trianglelefteq \cdots \trianglelefteq M_{r-1}$$
$$\{1\} = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_{s-1} = M_{r-1}$$

are composition series of M_{r-1}. Also $1 < |M_{r-1}| < |G| = n$, where the first inequality follows from G not being simple.

By the inductive hypothesis, $r-1 = s-1$ and $\exists \tau \in S_{r-1}$ such that

$$M_{\tau(i)}/M_{\tau(i)-1} \cong N_i/N_{i-1} \text{ for } 1 \leq i \leq r-1.$$

Then $r = s$ and defining $\sigma \in S_r$ by

$$\sigma(i) = \begin{cases} \tau(i) \text{ if } 1 \leq i \leq r-1 \\ r \text{ if } i = r \end{cases}$$

so $M_{\sigma(i)}/M_{\sigma(i)-1} \cong N_i/N_{i-1}$.

Case 2: Suppose $M_{r-1} \neq N_{s-1}$. Then $M_{r-1} \ntrianglelefteq M_{r-1}N_{s-1} \trianglelefteq G$ (the latter relation is an exercise). Since M_{r-1} is a maximal proper normal subgroup of G, $M_{r-1}N_{s-1} = G$.

Let $K = M_{r-1} \cap N_{s-1}$. By the Second Isomorphism Theorem, $K \trianglelefteq M_{r-1}$, $K \trianglelefteq N_{s-1}$ and

$$M_{r-1}/K \cong M_{r-1}N_{s-1}/N_{s-1} = G/N_{s-1} \text{ and } N_{s-1}/K \cong G/M_{r-1}.$$

In particular, M_{r-1}/K and N_{s-1}/K are simple. Let $\{1\} = H_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq H_t = K$ be a composition series for K. Then

$$\begin{gathered} \{1\} = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_t \trianglelefteq M_{r-1} \\ \{1\} = M_0 \trianglelefteq M_1 \trianglelefteq \cdots \trianglelefteq M_{r-1} \end{gathered}$$

are composition series of M_{r-1} and

$$\begin{gathered} \{1\} = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_t \trianglelefteq N_{s-1} \\ \{1\} = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_{s-1} \end{gathered}$$

are composition series of N_{s-1}. Since $1 < |M_{r-1}| < n$ and $1 < |N_{s-1}| < n$, we can apply the induction hypothesis. Then $r = 1 = t+1 = s-1$ and $\exists \tau_1, \tau_2 \in S_{t+1}$ such that

$$M_{\tau_1(i)}/M_{\tau_1(i)-1} \cong H_i/(H_{i-1}) \text{ for } 1 \leq i \leq t$$

so

$$M_{\tau_1(t+1)}/M_{\tau_1(t+1)-1} \cong M_{r-1}/K$$

and

$$\begin{gathered} N_{\tau_2(i)}/N_{\tau_2(i)-1} \cong H_i/H_{i-1} \text{ for } 1 \leq i \leq t \\ N_{\tau_2(t+1)}/N_{\tau_2(t+1)-1} \cong N_{s-1}/K. \end{gathered}$$

Thus

$$\begin{gathered} M_{\tau_1(i)}/M_{\tau_1(i)-1} \cong N_{\tau_2(i)}/N_{\tau_2(i)-1} \\ M_{\tau_1(t+1)}/M_{\tau_1(t+1)-1} \cong M_{\tau-1}/K \cong N_s/(N_{s-1}) \\ M_r/M_{r-1} \cong N_{s-1}/K \cong N_{\tau_2(t+1)}/N_{\tau_2(t+1)-1} \end{gathered}$$

Then $r = s$ and defining $\tau \in S_r$ by

$$\sigma(i) = \begin{cases} \tau_1 \tau_2^{-1}(i) \text{ if } i \in \{\tau_1(1), ..., \tau_1(t)\} \\ \tau_1(t+1) \text{ if } i = r \\ r \text{ if } i = \tau_2(t+1) \end{cases}$$

so $M_{\sigma(i)}/M_{\sigma(i)-1} \cong N_i/N_{i-1}$ for $1 \leq i \leq r$.

□

4.7.7. Definition: Abelian Tower

A normal tower of a group G is called an **abelian tower** if all the factor groups are abelian.

4.7.8. Definition: Solvable Group

A group G is **solvable** if it has an abelian tower. This is equivalent to all the composition factors of G being cyclic of prime order (exercise).

4.7.9. Example

1. $\{1\} \trianglelefteq (r) \trianglelefteq D_{2n}$ is an abelian tower, so D_{2n} is solvable.
2. $S_3 \cong D_6$ is solvable.
3. $\{1\} \trianglelefteq V_4 \trianglelefteq A_4 \trianglelefteq S_4$ is an abelian tower, so S_4 is solvable.
4. For $n \geq 5$, S_n is not solvable. Because A_n is a composition factor of S_n and A_n is a non-abelian simple group. (Note: this is the fundamental reason why we can't deterministically find roots of 5th degree and higher polynomials, but the reason will be further expanded on in Galois theory).

4.7.10. *Theorem*

Let $H \leq G$.
1. If G is solvable, then H is solvable.
2. If $H \trianglelefteq G$ and G is solvable, then G/H is solvable.
3. If $H \trianglelefteq G$ and H is solvable, and G/H is solvable, then G is solvable.

Proof:

1. Assume G is solvable. Let

$$\{1\} = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_t = G$$

be an abelian tower of G. Let $K_i = N_i \cap H$ for $i = 0, 1, ...t$. Let $\varphi_i : K_i \hookrightarrow N_i \xrightarrow{\pi_i} N_i/(N_{i-1})$. Then $\ker \varphi_i = K_i \cap N_{i-1} = H \cap N_i \cap N_{i-1} = H \cap N_{i-1} = K_{i-1}$. By the First Isomorphism Theorem, $K_{i-1} \trianglelefteq K_i$ and $K_i/(K_{i-1}) \cong \operatorname{im} \varphi_i \leq N_i/N_{i-1}$. Therefore K_i/K_{i-1} is abelian. Then

$$\{1\} = K_0 \trianglelefteq K_1 \trianglelefteq \cdots \trianglelefteq K_t = H$$

is an abelian tower of H.

2. Suppose $H \trianglelefteq G$ and G is solvable. Let $\{1\} = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_t = G$ be an abelian tower of G. Let $\pi_H : G \longrightarrow G/H$ be the canonical projection. Let $M_i = \pi_H(N_i)$ for $i = 0, 1, \ldots, t$. Notice since $N_{i-1} \trianglelefteq N_i$, we have $M_{i-1} = \pi_H(N_{i-1}) \trianglelefteq \pi_H(N_i) = M_i$. Let

$$\varphi_i : N_i \xrightarrow{\pi_H \mid N_i} \xrightarrow{\pi_i} M_i/M_{i-1}$$

By definition of M_i, we have $\pi_H(N_i) = M_i$ and π_i is surjective. Thus φ_i is a surjective homomorphism. Notice $\ker \varphi_i = \{a \in N_i : \pi_H(a) \in M_{i-1}\} \supseteq N_{i-1}$. Then φ_i induces a homomorphism

$$\begin{aligned} \overline{\varphi_i} : N_i/N_{i-1} &\longrightarrow M_i/M_{i-1} \\ aN_{i-1} &\longmapsto \varphi_i(a) \end{aligned}$$

Since N_i/N_{i-1} is abelian, $M_i/M_{i-1} = \overline{\varphi_i}(N_i/N_{i-1})$ is also abelian. Thus

$$\{1\} = M_0 \trianglelefteq M_1 \trianglelefteq \cdots \trianglelefteq M_t = G/H.$$

3. Suppose that $H \trianglelefteq G$, G/H is solvable, and H is solvable. Let $\pi_H : G \to G/H$ denote the canonical projection. Let

$$\{\overline{1}\} = M_0 \trianglelefteq M_1 \trianglelefteq \cdots \trianglelefteq M_r = G/H$$

be an abelian tower of G/H and let

$$\{1\} = K_0 \trianglelefteq K_1 \trianglelefteq \cdots \trianglelefteq K_s = H$$

be an abelian tower of H.

For each $i \in \{0, 1, \ldots, r\}$, let $Q_i = \pi_H^{-1}(M_i)$. Let $\pi_i : M_i \to M_i/M_{i-1}$ denote the canonical projection. Let $\varphi_i = \pi_i \circ \pi_{H \mid Q_i}$:

$$\varphi_i : Q_i \xrightarrow{\pi_H} M_i \xrightarrow{\pi_i} M_i/M_{i-1}.$$

Since π_H is surjective, $\pi_H(Q_i) = \pi_H(\pi_H^{-1}(M_i)) = M_i$. Combining this observation with the fact that π_i is also surjective, we deduce that φ_i is a surjective homomorphism. Note that

$$\ker \varphi_i = \{a \in Q_i : \pi_H(a) \in M_{i-1}\} = Q_{i-1}.$$

Therefore, by the First Isomorphism Theorem, we know that $Q_{i-1} \trianglelefteq Q_i$ and $Q_i/Q_{i-1} \cong M_I/M_{i-1}$. In particular, Q_i/Q_{i-1} is abelian. Therefore,

$$\{1\} = K_0 \trianglelefteq K_s = H = Q_0 \trianglelefteq Q_1 \trianglelefteq \cdots \trianglelefteq Q_r = G$$

is an abelian tower of G.

□

4.7.11. *Theorem:* Feit-Thompson Theorem

Every finite group of odd order is solvable.

Proof:

□

4.8. Problems

4.8.1. Exercise

Suppose we have a group G with $H \leq G$ and $N \trianglelefteq G$. Prove $N \cap H \trianglelefteq H$.

Solution

Let $g \in h(N \cap H)h^{-1}$ for some $h \in H$. Then $g = hah^{-1}$ for some $a \in N \cap H$. Since $a \in H$, $g \in H$. Since $N \trianglelefteq G$, $xNx^{-1} = N \forall x \in G$. Since $a \in N$ and $h \in G$, we have $g \in xNx^{-1} = N$, so $g \in N$. Thus $h(N \cap H)h^{-1} \subseteq N \cap H \Longrightarrow N \cap H \trianglelefteq H$.

4.8.2. Exercise

Let G be a group and let N be a finite subgroup of G. Let $g \in G$. Then show g normalizes N if and only if $gNg^{-1} \subseteq N$.

Is this true if N is not finite?

Solution

$(\Longrightarrow)$ clear since by definition $gNg^{-1} = N$.

$(\Longleftarrow)$ Notice $|gNg^{-1}| = |N|$ since the map

$$\begin{aligned} N &\longrightarrow gNg^{-1} \\ n &\mapsto gng^{-1} \end{aligned}$$

is a bijection.

A counterexample to show that it is not true if N is infinite is

$$N = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} : a \in \mathbb{Z} \right\}$$

where $N \leq \mathrm{GL}_2(\mathbb{Q})$. Take $g = \left(\begin{smallmatrix} 2 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Then $gNg^{-1} = \left\{ \left(\begin{smallmatrix} 1 & 2a \\ 0 & 1 \end{smallmatrix}\right) : a \in \mathbb{Z} \right\} \nsubseteq N$.

4.8.3. Exercise

Let G be a group. Prove that $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$, where the set of inner automorphisms $\mathrm{Inn}(G) = \left\{ \varphi_g : g \in G \right\}$ where $\varphi_g : G \to G$ is defined by $x \mapsto gxg^{-1}$.

Solution

Let $g \in G$ and let $\sigma \in \mathrm{Aut}(G)$. For $\varphi \in \mathrm{Inn}(G)$, we want to show that $\sigma\varphi\sigma^{-1} \in \mathrm{Inn}(G)$. Let $x \in G$ and note

$$(\sigma\varphi_g\sigma^{-1})(x) = \sigma\left(\varphi_g\left(\sigma^{-1}(x)\right)\right) = \sigma\left(g\sigma^{-1}(x)g^{-1}\right) = \sigma(g)x\sigma(g)^{-1} = \varphi_{\sigma(g)} \in \mathrm{Inn}(G).$$

4.8.4. Exercise

Prove that $D_{24} \ncong S_4$.

Solution

(Could check elements of order 12 - D has them but not S_4).

Check elements of order 2 - there aer 12 reflections and r^6 so there are 13 such elements in D_{24}. In S_4 there are $\binom{4}{2} = 6$ transpositions with the others staying in place, and there are an additional 3 given by products of two cycles: https://math.stackexchange.com/questions/311680/finding-the-number-of-elements-of-order-two-in-the-symmetric-group-s-4

4.8.5. Exercise

Prove that for $n \geq 3$, the homomorphism $S_n \to \operatorname{Aut}(S_n)$ defined by $g \mapsto \varphi_g$ (where φ_g is conjugation by g) is injective.

Solution

Notice that it is sufficient to prove $\ker = \{1\}$. Take $\sigma \in S_n$, so that its image is the automorphism $\varphi_\sigma(g) = \sigma g \sigma^{-1}$. This must be the identity automorphism, so $\sigma g \sigma^{-1} = g \Rightarrow \sigma g = g \sigma$, so $g \in Z(S_n)$. The only element that commutes with all others in the symmetric group for $n \geq 3$ is e, so we must have $\ker = \{1\}$ as desired.

4.8.6. Exercise

Suppose that H and K are subgroup of finite index in the (possibly infinite) group G with $[G : H] = m$ and $[G : K] = n$. Prove that $\operatorname{lcm}(m, n) \leq [G : H \cap K] \leq mn$. Deduce that if m and n are relatively prime then $[G : H \cap K] = [G : H] \cdot [G : K]$.

Solution

We need to show $[H : H \cap K] \leq [G : K] = n$. We want to find an injective function $H / H \cap K \longrightarrow G / K$ and $aH \cap K \mapsto aK$. First we show it's well defined: for $a, b \in H$

$$\begin{aligned} aH \cap K = bH \cap K &\iff a^{-1}b \in H \cap K \\ &\iff a^{-1}b \in K \\ &\iff aK = bK. \end{aligned}$$

This also shows it's injective.

Then $|H / H \cap K| \leq |G / K|$. Since $[G : H \cap K] = m[H : H \cap K]$, we have $m \mid [G : H \cap K]$. Since $[G : H \cap K] = [G : K][K : H \cap K]$. Then $n \mid [G : H \cap K]$.

4.8.7. Exercise

Prove that if G is a group of prime order p, then G is cyclic.

Solution

By the above corollary, for some $a \in G$, we must have that $\operatorname{ord}(a) \mid p$. But then $\operatorname{ord}(a) = 1$ or $\operatorname{ord}(a) = p$ since p is prime. If the order of the element is 1, we have the identity, and we can just pick another element since $|G| = p > 1$. Thus we can always pick an element with order p. Then note G at least contains the cyclic group (a), but this has $\operatorname{ord}(a) = p$ elements, so G also cannot contain anything else. Therefore we must have $(a) = G$.

4.8.8. Exercise

Find all the normal subgroups of S_n for $n \geq 5$.

Solution

Notice $\{1\}, A_n, S_n$ are all normal subgroups of S_n. To show that these are the only normal subgroups, let $H \trianglelefteq S_n$. Then notice $H \cap A_n \trianglelefteq A_n$, so $H \cap A_n = \{1\}$ or A_n by Theorem 4.6.7.

- *Case 1*: First suppose $H \cap A_n = A_n$. Then $A_n \leq H \leq S_n$. Then $|A_n| \mid |H| \mid |S_n| = 2\,|A_n|$. Thus $|H| = |A_n| \Rightarrow H = A_n$ or $|H| = |S_n| \Rightarrow H = S_n$.
- *Case 2*: Suppose $H \cap A_n = \{1\}$. Thus any non-identity element in H is odd. Suppose $H \neq \{1\}$. Then $\exists x \in H, x \neq 1$. Then x is odd. If y is any other non-identity element in H, then y is odd and xy is even so $xy = 1$. In particular, $x^2 = 1$ and any other nonidentity element $y \in H$ satisfies $y = x^{-1} = x$. Then $H = \{1, x\}$. Since $H \trianglelefteq S_n$, for all $\sigma \in S_n$, we have $\sigma H \sigma^{-1} = H$, so $\sigma x \sigma^{-1} = x \forall \sigma \in S_n$. Then $x \in Z(S_n) = \{1\}$, a contradiction.

5. Group Actions

5.1. Group Actions

5.1.1. Remark

Let X be an arbitrary set. Let $\mathcal{F}$ be the collection of functions that map X to itself. Notice that $\mathcal{G} \subseteq \mathcal{F}$, the bijections, form a group under composition.

We want to relate a given group G to $\mathcal{G}$ to better understand the structure of $\mathcal{G}$. Particularly, is there a homomorphism $\varphi : G \to \mathcal{G}$? We want φ to have the property that the image of the identity is the trivial bijection, i.e., $\varphi(e)(x) = x \forall x \in X$. Since we want φ to be a homomorphism, we also define

$$\varphi(g_1 g_2)(x) = \varphi(g_1) \circ \varphi(g_2)(x).$$

This gives rise to the idea of a *group action*, which we define below.

5.1.2. Definition: Group Action

Let G be a group and let X be a set. A **(left) group action** of G on X is a map $\mu : G \times X \to X$ such that

1. $\mu(gh, x) = \mu(g, \mu(h, x))$ for all $g, h \in G$ and for all $x \in X$
2. $\mu(1, x) = x$ for all $x \in X$

Alternately, a more intuitive definition is:

Let G be a group and let X be a set. Let S_X be the group of all permutations of X, i.e., the symmetric group on X. An **action** of G on X is a homomorphism $G \to S(X)$.

5.1.3. Remark

From now on, given a group action $\mu : G \times X \to X$, we will usually write $g \cdot x$ (or simply gx) instead of $\mu(g, x)$. With this notation, conditions (i) and (ii) can be written

1. $(gh) \cdot x = g(h \cdot x)$ for all $g, h \in G$ and for all $x \in X$
2. $1 \cdot x = x$ for all $x \in X$

Because of condition (i), if $g, h \in G$ and $x \in X$, we can write ghx without any risk of ambiguity.

5.1.4. Remark

We can also define a **right group action** of a group G on a set X as a map $\mu : X \times G \to X$ such that

1. $\mu(x, gh) = \mu(\mu(x, g), h)$ for all $g, h \in G$ and for all $x \in X$
2. $\mu(x, 1) = x$ for all $x \in X$

We focus on left actions, but all results have analogous results for right actions.

5.1.5. Remark

We want to show the equivalence of the two definitions given above.

Suppose that we are given a group action $\mu : G \times X \to X$. For each $g \in G$, we can define a map $\sigma_g : X \to X$ by $\sigma_g(x) = g \cdot x$. Then we claim that $\sigma_g \in S_X$ for all $g \in G$ and that the map

$$\begin{aligned} \varphi : G &\longrightarrow S_X \\ g &\longmapsto \sigma_g \end{aligned}$$

is a group homomorphism.

Let us first show that $\sigma_g \in S_X$ for all $g \in G$. To show that σ_g is injective, note that for all $x, y \in X$,

$$\begin{aligned} \sigma_g(x) = \sigma_g(y) \Longrightarrow g \cdot x = g \cdot y \Longrightarrow g^{-1} \cdot (g \cdot x) = g^{-1} \cdot (g \cdot y) \\ \Longrightarrow (g^{-1}g) \cdot x = (g^{-1}g) \cdot y \Longrightarrow 1 \cdot x = 1 \cdot y \Longrightarrow x = y. \end{aligned}$$

To show that σ_g is surjective, note that, given $x \in X$, we have

$$\sigma_g(g^{-1} \cdot x) = g \cdot (g^{-1} \cdot x) = (gg^{-1}) \cdot x = 1 \cdot x = x.$$

Now we show that σ is a homomorphism. Let $g, h \in G$. We need to check that $\sigma_{gh} = \sigma_g \circ \sigma_h$. For that, note that, for all $x \in X$,

$$\sigma_{gh}(x) = (gh) \cdot x = g \cdot (h \cdot x) = \sigma_g(h \cdot x) = \sigma_g(\sigma_h(x)) = (\sigma_g \circ \sigma_h)(x).$$

Conversely, suppose that we are given a homomorphism $\varphi : G \to S_X$. Then, we can define an action of G on X by

$$\begin{aligned} G \times X &\longrightarrow X \\ (g, x) &\longmapsto \varphi(g)(x). \end{aligned}$$

To check that this is indeed a group action, note that

1. For all $g, h \in G$ and for all $x \in X$,

$$(gh) \cdot x = \varphi(gh)(x) = (\varphi(g) \circ \varphi(h))(x) = \varphi(g)(\varphi(h)(x)) = g \cdot (h \cdot x);$$

2. For all $x, \in X$,

$$1 \cdot x = \varphi(1)(x) = \mathrm{id}_X(x) = x.$$

I should check that the map

$$\{\text{actions of } G \text{ on } X\} \longrightarrow \{\text{homomorphisms } \varphi : G \to S_X\}$$

and the map

$$\{\text{homomorphisms } \varphi : G \to S_X\} \longrightarrow \{\text{actions of } G \text{ on } X\}$$

that we have just constructed are inverses of each other, thus providing a bijection between these two sets.

5.1.6. Definition: Action Kernel and Faithful Action

1. The **kernel** of the action is the set of elements of G that act trivially on X:
$$\{g \in G : g \cdot x = x \text{ for all } x \in X\}.$$
2. The action is said to be **faithful** if the kernel is the trivial subgroup of G. More intuitively, an action is faithful if different elements of the group correspond to different transformations.

5.1.7. *Proposition*

1. The kernel of the action is the kernel of the associated homomorphism $\varphi : G \to S_X$ (and is therefore a normal subgroup of G).
2. The action is faithful if the associated homomorphism $\varphi : G \to S_X$ is injective.

Proof:

1. Notice that
$$\begin{aligned}\{g \in G : g \cdot x = x \forall x \in X\} &= \{g \in G : \varphi(g)(x) = x \forall x \in X\} \\ &= \left\{g \in G : \varphi(g) = 1_{S_X}\right\} \\ &= \ker \varphi.\end{aligned}$$

Thus by Proposition 4.4.3, the kernel of the action is a normal subgroup of G.

2. By the above, if the kernel of the action is just $\{1_G\}$, then $\ker \varphi = \{1_G\}$ and by Proposition 4.1.5, φ is injective.

□

5.1.8. Definition: Trivial Action

Let G be a group and let X be a set. The **trivial action** of G on X is the action defined by
$$g \cdot x = x \text{ for all } g \in G \text{ and for all } x \in X.$$

The corresponding homomorphism from G to S_X is the trivial homomorphism $g \to \mathrm{id}_X$. The kernel of the trivial action is G. In particular, the trivial action is not faithful unless $G = \{1\}$.

5.1.9. Example

1. Let X be a set. Then we can define an action of S_X on X by
$$\sigma \cdot x = \sigma(x) \text{ for all } \sigma \in S_X \text{ and for all } x \in X.$$
The corresponding homomorphism from S_X to S_X is the identity map. This action is faithful.
2. Let G be a group acting on a set X. Let $H \leq G$. The action of G on X induces an action of H on X via restriction of the map $G \times X \to X$ to a map $H \times X \to X$. Let $\varphi : G \to S_X$ be the homomorphism corresponding to the action of G on X. Then the homomorphism corresponding to the action of H on X is the restriction of φ to H. Note that $\ker\left(\varphi_{|H}\right) = \ker\varphi \cap H$, so the action of H on X is faithful if and only if $H \cap \ker\varphi = \{1\}$.
3. Consider the additive group $\mathbb{R}$. We can define an action of $\mathbb{R}$ on $\mathbb{C}$ by
$$\alpha \cdot z = e^{i\alpha} z \text{ for all } \alpha \in \mathbb{R} \text{ and for all } z \in \mathbb{C}.$$
To show that this is actually an action, note that:
   - for all $\alpha, \beta \in \mathbb{R}$ and for all $z \in \mathbb{C}$,
$$(\alpha + \beta) \cdot z = e^{i(\alpha+\beta)} z = e^{i\alpha}\left(e^{i\beta} z\right) = \alpha \cdot (\beta \cdot z)$$
   - for all $z \in \mathbb{C}$, we have $0 \cdot z = e^{i0} z = z$.

   To find the kernel of this action, we want $\alpha \cdot z = z \forall z \in \mathbb{C}$. This is $e^{i\alpha} z = z$ so $e^{i\alpha} = 1 \Longrightarrow \ker\varphi = 2\pi\mathbb{Z}$. In particular, this action is not faithful. (What if $z = 0$?)
4. Let $n \geq 3$. The dihedral group D_{2n} acts naturally on the set of vertices of a regular n-gon. If we label the vertices of a regular n-gon with the integers $1, 2, ..., n$, the corresponding homomorphism $\varphi : D_{2n} \to S_n$ is given by
$$\varphi(x)(j) = k \Longleftrightarrow x \text{ sends the vertex } j \text{ to the vertex } k$$
This homomorphism was discussed in Example 4.1.6, and is injective, so the action is faithful.
5. Let G be a group. We can define an action of G on itself by conjugation:
$$\begin{aligned} G \times G &\longrightarrow G \\ (g, a) &\longmapsto gag^{-1}. \end{aligned}$$
To show that this is indeed an action, note that:
   - for all $g, h, a \in G$,
$$(gh) \cdot a = (gh)a(gh)^{-1} = g(hah^{-1})g^{-1} = g \cdot (hah^{-1}) = g \cdot (h \cdot a)$$
   - for all $a \in G$, we have that $1 \cdot a = 1a1^{-1} = a$.

   The corresponding homomorphism is the map
$$\begin{aligned} G &\longrightarrow \operatorname{Aut}(G) \leq S_G \\ g &\longmapsto \varphi_g \end{aligned}$$
which has kernel $Z(G)$ (this was shown in Proposition 4.1.15), so the action is faithful iff $Z(G) = \{1\}$.

5.1.10. Definition: Regular Action

Let G be a group. We can define an action of G on itself by

$$g \cdot a = ga \text{ for all } g \in G \text{ and for all } a \in G,$$

where on the right hand side ga is the product of g and a using the group operation on G. This action is called the **left regular action** of G on itself. It is faithful: if $g \in G$ acts trivially on G, then in particular $g \cdot 1 = 1$ and therefore $g = 1$. Further, the stabilizer of any point is the identity subgroup.

5.1.11. Remark

We can generalize regular actions in the following way: let H be any subgroup of G and let A be the set of all left cosets of H in G. Define an action of G on A by

$$g \cdot aH = gaH \text{ for all } g \in G, aH \in A$$

where gaH is the left coset with representative ga. One easily checks that this satisfies the two axioms for a group action. In the special case when H is the identity subgroup of G, the coset aH is just $\{a\}$ and if we identify the element a with the set $\{a\}$, this action by left multiplication on left cosets of the identity subgroup is the same as the action of G on itself by left multiplication.

5.1.12. *Theorem:* Cayley's Theorem

> Every group is isomorphic to a subgroup of a symmetric group. A group of finite order n is isomorphic to a subgroup of S_n.

Proof: Let G be a group. As we saw in the previous example, the left regular action of G on itself is faithful. Therefore, this action provides an injective homomorphism $\varphi : G \to S_G$. By the First Isomorphism Theorem, it follows that $G \cong \varphi(G)$, so G is isomorphic to a subgroup of a permutation group. If G is finite of order n, then we can define an isomorphism between S_G and S_n by choosing a bijection between G and $\{1, 2, ..., n\}$. Thus G is isomorphic to a subgroup of S_n.

□

5.2. Orbits and Stabilizers

5.2.1. Definition: Stabilizer

The stabilizer of x is $G_x = \{g \in G : g \cdot x = x\}$. Intuitively, the stabilizer of x is "the set of all elements of G which don't move x when they act on x."

5.2.2. *Lemma*

Let G act on X. Define a relation $\sim$ on X by

$$x \sim y \Longleftrightarrow \exists g \in G \text{ such that } x = gy.$$

Then $\sim$ is an equivalence relation

Proof: *Reflexive*: For all $x \in X$, $1 \cdot x = x$, so $x \sim x$. *Symmetric*: Let $x, y \in X$. Suppose $x \sim y$. Then $x = g \cdot y$ for some $g \in G$. Then $g^{-1}x = g^{-1} \cdot (g \cdot y) = (g^{-1}g) \cdot y = 1 \cdot y = y$. Then $y \sim x$. *Transitive*: Let $x, y, z \in X$. Suppose $x \sim y$ and $y \sim z$. Then $x = g_1 \cdot y$ and $y = g_2 \cdot z$. Then $x = g_1 \cdot (g_2 \cdot z) = (g_1 g_2) \cdot z$. Thus $x \sim z$.

□

5.2.3. Definition: Orbit, Transitive Action

Let G act on X. The **orbit** of $x \in X$ is $G \cdot x = \{g \cdot x : g \in G\}$, an equivalence class of x for $\sim$. Intuitively, the orbit of x is "everything that can be reached from x by an action of G."

The action is **transitive** if there is only one orbit, i.e., $\forall x, y \in X, \exists g \in G$ such that $x = g \cdot y$.

5.2.4. Example

1. Let G be the circle group $G = \{z \in \mathbb{C} : |z| = 1\}$. This is a group under multiplication, and in the group action sense, we think of G acting on $\mathbb{C}$ by multiplication. Algebraically we multiply by $z = e^{i\theta}$, and geometrically we rotate by some angle θ. If we fix some $x \in \mathbb{C}$, the orbit through x is exactly the circle of radius $|x|$ centered at the origin, unless $x = 0$.

   The stabilizer of x in the case that $x \neq 0$ is just the set of points $z \in \mathbb{C}$ such that $z \cdot x = x$, implying $z = 1$, so the stabilizer is just $\{1\}$. If $x = 0$, then $zx = x \forall z \in G$, so the stabilizer is G.

2. Now consider the dihedral group of order 8, i.e., the symmetries of the square. Here we consider the set $X = \{1, 2, 3, 4\}$ of the vertices. What is the orbit of vertex 1? Note that it can be sent to any of the other vertices by a rotation, so its orbit is X – this applies for all vertices. What are their stabilizers? None of the rotations fix any vertices, and only two reflections do, so each vertex has a stabilizer with cardinality 2. For example, for vertex 3, the stabilizer is $\{e, s\}$ if we consider s to be reflection through the line joining 1 and 3.

5.2.5. *Theorem:* Orbit-Stabilizer Theorem

Let G act on X. Let $x \in X$. The map

$$\begin{aligned} G/G_x &\longrightarrow G \cdot x \\ aG_x &\longmapsto a \cdot x \end{aligned}$$

is well-defined and bijective, and therefore $|G \cdot x| = [G : G_x]$.

Proof: Let $a, b \in G$.

$$\begin{aligned} aG_x = bG_x &\Longleftrightarrow b^{-1}a \in G_x \\ &\Longleftrightarrow b^{-1}a \cdot x = x \\ &\Longleftrightarrow a \cdot x = b \cdot x. \end{aligned}$$

The map is well-defined by $(\Longrightarrow)$ and injective by $(\Longleftarrow)$.

Surjectivity: Let $a \in G$. Then $a \cdot x$ is the image of aG_x.

□

5.2.6. *Corollary*

Let G act on X. Suppose G is finite. The cardinality of every orbit divides $|G|$.

Proof: Let $G \cdot x$ be an orbit. Then $|G \cdot x| = [G : G_x]$, which divides $|G|$ by the Counting Formula.

□

5.2.7. *Corollary:* Orbits Formula

Let G act on X. Suppose X is finite. Let $x_1, x_2, ..., x_r$ be a complete set of representatives for the orbits. Then

$$|X| = \sum_{i=1}^{r} |G \cdot x_i| = \sum_{i=1}^{r} \left[G : G_{x_i}\right].$$

Proof: The orbits are the equivalence classes for the equivalence relations defined by Lemma 5.2.2. Therefore, they form a partition of X, giving us hte first equality. The second equality follows from the orbit stabilizer theorem.

□

5.2.8. Example

Consider a Rubik's cube, where G represents the possible orientations of the cube and X represents the faces, labeled 1-6. If we hold it such that we are facing the yellow side, the stabilizer of the yellow side consists of the four rotations we can make while keeping the yellow side in front. The other 5 sides are similar. The orbits of every face consist of every other side, since we can always rotate any face towards us. Then the orbit stabilizer theorem tells us that the number of equivalence classes created by the stabilizer partition (6 classes consisting of 4 elements each) is the same as the number of orbits for every element (6 each). We could for example use this to find the total number of orientations of Rubik's cube:

$$|G| = |G : G_x| \cdot |G_x| = |G \cdot x| \cdot |G_x| = 6 \cdot 4 = 24.$$

5.2.9. *Proposition*

Let G act on X. Suppose x and y are elements in the same orbit. Then G_x is conjugate to G_y in G.

Proof: Since x and y are in the same orbit, $\exists g \in G$ such that $y = g \cdot x$. For all $a \in G$,

$$a \in G_y \Longleftrightarrow ay = y \Longleftrightarrow agx = gx \Longleftrightarrow g^{-1}agx = x \Longleftrightarrow g^{-1}ag \in G_x \Longleftrightarrow a \in gG_xg^{-1}.$$

Thus $G_y = gG_xg^{-1}$.

□

5.2.10. Definition: Fixed Point

Let G act on X. An element $x \in X$ is a **fixed point** if $g \cdot x = x \forall g \in G$. In other words, $G_x = G \Longleftrightarrow G \cdot x = \{x\}$.

5.2.11. Example

1. For $n \geq 3$, D_{2n}. Label the vertices of the n-gon by $\overline{0}, \overline{1}, ...\overline{n-1} \in \mathbb{Z}/n\mathbb{Z}$. Then D_{2n} acts on $\mathbb{Z}/n\mathbb{Z}$. It is transitive because given $\overline{i}, \overline{j} \in \mathbb{Z}/n\mathbb{Z}$, $r^{j-i} \cdot \overline{i} = \overline{j}$. The stabilizer of $\overline{k}$ is $r^k\{1, s\}r^{-k} = \{1, r^ksr^{-k}\} = \{1, r^{2k}s\}$.

   The kernel of the action is thus $\cap_{\overline{k}\in\mathbb{Z}/n\mathbb{Z}} \{1, r^{2k}s\} = \{1\}$, so the action is faithful.

   Applying the orbit formula in this case, we get $|\mathbb{Z}/n\mathbb{Z}| = [D_{2n} : (r^ks)]$.

2. Left regular action of G. I.e.,

   $$\begin{aligned} G \times G &\longrightarrow G \\ (g, a) &\longmapsto ga \end{aligned}$$

   This is transitive since given $a, b \in G$, $b = (ba^{-1})a$. There are no fixed points unless G is trivial. The stabilizer of a is $\{1\}$. From the orbit formula we get $|G| = [G : \{1\}]$ (obvious).

3. Let $H \leq G$. Restrict left regular actions of G to H:

   $$\begin{aligned} H \times G &\longrightarrow G \\ (h, a) &\longmapsto ha \end{aligned}$$

   The orbit of a is the right coset Ha. This is not transitive unless $H = G$. The stabilizer of a is $\{1\}$. Let $x_1, ..., x_r$ be a complete set of representative for the orbits of H in G. By the orbits formula,

$$\begin{aligned} |G| &= \sum_{i=1}^{r} \left[H : H_{x_i}\right] = \sum_{i=1}^{r} [H : \{1\}] \\ &= r\ |H| = [G : H] \cdot |H| \end{aligned}$$

which is the Counting Formula.

4. Let $H \leq G$. Define the action of G on G/H by

$$\begin{aligned} G \times G/H &\longrightarrow G/H \\ (g, aH) &\longmapsto gaH \end{aligned}$$

This is transitive since given $aH, bH \in G/H$, we have $ba^{-1} \cdot aH = bH$. The stabilizer of H is H, and the stabilizer of aH is aHa^{-1}. The kernel is

$$\cap_{a \in G}\ aHa^{-1}$$

which is the largest normal subgroup of G contained in H. By the orbit formula, $|G/H| = \left[G : aHa^{-1}\right]$. To find the fixed points, note that

$$\begin{aligned} aH \text{ fixed point} &\Longleftrightarrow \text{stabilizer of } a = G \\ &\Longleftrightarrow aHa^{-1} = G \Longleftrightarrow H = G. \end{aligned}$$

There will be no fixed points unless $H = G$.

5. G acting on itself by conjugation.

$$\begin{aligned} G \times G &\longrightarrow G \\ (g, a) &\longmapsto g \cdot a = gag^{-1} \end{aligned}$$

The orbit of a is $G \cdot a = \left\{gag^{-1} : g \in G\right\}$ which is called the **conjugacy class** of a in G.

Note $G \cdot 1 = \{1\}$. The action is not transitive unless $G = \{1\}$. The stabilizer of a is $C_G(a)$, the centralizer of a. The kernel is $Z(G)$. The fixed points are the elements of $Z(G)$.

Let $z_1, \ldots, z_k$ be the elements of $Z(G)$. Then $\{z_1\}, \ldots, \{z_k\}$ are the trivial conjugacy classes (each has only one element).

Let $x_1, \ldots, x_r$ be a complete set of representatives for the nontrivial conjugacy classes. The orbits formula gives

$$|G| = \sum_{i=1}^{k} |\{z_i\}| = \sum_{i=1}^{r} |G \cdot x_i| = |Z(G)| + \sum_{i=1}^{r} [G : C_G(x_i)].$$

This is known as the **class equation** for the group G.

5.2.12. *Lemma:* Burnside's Lemma

Let G be a finite group acting on a finite set X. For each $g \in G$, we denote by X^g the set of elements in X that are fixed by g, i.e., $X^g = \{x \in X : g \cdot x = x\}$.

Then

$$|G \backslash X| = \frac{1}{|G|} \sum_{g \in G} |X^g|.$$

5.2.13. *Theorem*

Let G be a group, let $H \leq G$ and let G act by left multiplication on the set A of left cosets of H in G. Let π_H be the associated permutation representation afforded by this action. Then

1. G acts transitively on A
2. The stabilizer in G of the point $1H \in A$ is the subgroup H
3. The kernel of the action is $\cap_{x \in G} xHx^{-1}$, and $\ker \pi_H$ is the largest normal subgroup of G contained in H

5.2.14. *Theorem:* Cauchy's Theorem

Let G be a finite group. Let p be a prime dividing $|G|$. Then G contains an element of order p.

Proof:

We proceed by strong induction on $|G|$. If $|G| = p$, any nonidentity element has order p. Let $n > p$ be a multiple of p. Suppose every finite abelian group G with $|G| < n$ and $p \mid |G|$ contains an element of order p.

First assume that G is abelian. Let $a \in G$ be a nonidentity element. Let $k = \operatorname{ord}(a)$. If $p \mid k$, then $a^{\frac{k}{p}}$ has order p. Now suppose $p \nmid k$. We know $n = [G : (a)] \cdot k$. Then $p \mid [G : (a)]$.

Since G is abelian, $(a) \trianglelefteq G$ (Prop 4.3.5). Note $G/(a)$ is a group of order divisible by p, and $|G| < n$ because $k > 1$. By the induction hypothesis, $G/(a)$ contains an element b of order p.

Now let $\pi : G \to G/(a)$ be the canonical projection. π is surjective, so $\exists c \in G$ such that $\pi(c) = b$. Let $t = \operatorname{ord}(c)$. Then $b^t = \pi(c)^t = \pi(c^t) = \pi(1) = \overline{1}$, so $p = \operatorname{ord}(b) \mid t$. Thus $c^{\frac{t}{p}} \in G$ and this element has order p.

Note this result can be considered a partial converse to Lagrange's theorem.

□

5.2.15. Definition: p-group

Let p be a prime number. A ***p*-group** is a finite group of order p^k for some integer $k \geq 0$. In other words, the order of every element is a power of p (by Lagrange's Theorem).

5.2.16. *Theorem*

Every nontrivial p-group has a nontrivial center.

Proof: The Class Equation for G reads

$$|G| = |Z(G)| + \sum_{i=1}^{r} [G : C_G(x_i)]$$

Note that $|G|$ and all the terms $[G : C_G(x_i)]$ are divisible by p. It follows that p divides $|Z(G)|$ and therefore $Z(G)$ is nontrivial.

□

5.2.17. *Corollary*

Every p-group is solvable.

Proof: We proceed by strong induction on $|G|$. If $|G| = 1$, then G is trivial and is clearly solvable. Let $n > 1$ be a power of p and suppose that every p-group of order smaller than n is solvable. Let G be a group of order n. By the previous theorem, we know that $Z(G)$ is a nontrivial normal subgroup of G. Therefore, the quotient group $G/Z(G)$ is a p-group of order smaller than n. By the induction hypothesis, $G/Z(G)$ is solvable. Also $Z(G)$ is abelian and therefore solvable. Finally, since $Z(G)$ and $Z/Z(G)$ are solvable, it follows by Proposition 4.7.10(iii) that G is solvable.

□

5.3. Exercises

5.3.1. Exercise

Let G be a finite group. Let $g_1, …, g_r$ be a complete set of representatives of the conjugacy classes in G. Suppose $g_1, …, g_r$ commute with each other. Prove that G is abelian.

Solution

So $g_1, …, g_r \in C_G(g_i) \Rightarrow r \leq \sum_i |C_G(g_i)| \Rightarrow |\text{Conj}(g_i)| \leq \frac{n}{r}$. Then $n = |G| = \sum_{i=1}^{r} |\text{Conj}(g_i)| \leq \sum_{i=1}^{r} \frac{n}{r} = n$. Thus $|\text{Conj}(g_i)| = \frac{n}{r} \forall i$. But we know $|\text{Conj}(1)| = 1$, so $\frac{n}{r} = 1$. All conjugacy classes have size 1, so G is abelian.

5.3.2. Exercise

Let G be a finite group of order $n = p^k m$, where p is a prime, $k > 0$ and $p \nmid m$.

Let P be a subgroup of G with order p^k (a p-Sylow subgroup). Let $H \leq N_G(P)$ with $|H| = p^a$ for some $a \geq 0$. Prove $H \leq P$.

Solution

By the Second Isomorphism Theorem,

$$(HP)/P \cong H/H \cap P.$$

Note $|H/H \cap P| \mid |H|$, so $|H/H \cap P|$ is a power of p. Thus $|HP/P|$ is a power of p. Notice $|HP| = |HP/P| \cdot |P|$ is a power of p.

Also, $|HP| \mid p^k m$, so $|HP| \mid p^k$. Since $P \leq HP$ and $|P| = p^k$, $|HP| = p^k$ and $P = HP$. Therefore $H \leq P$.

6. Classification of Finitely Generated Abelian Groups

6.1. Direct Products

6.1.1. Definition: Direct Product

Let $G_1, \ldots, G_n$ be groups. The **direct product** $G_1 \times G_2 \times \cdots \times G_n$ is the set of n-tuples $(g_1, \ldots, g_n)$ with $g_i \in G_i$ for all $i \in \{1, 2, \ldots, n\}$ and binary operation defined componentwise:

$$(g_1, \ldots, g_n) \cdot (h_1, \ldots, h_n) = (g_1 h_1, \ldots, g_n h_n).$$

With this operation $G_1 \times G_2 \times \cdots \times G_n$ is a group.

We remark that this group is abelian if and only if each G_i is abelian.

6.1.2. *Proposition*

Let $G_1, \ldots, G_n$ be groups. Let $G = G_1 \times \cdots \times G_n$.

1. For each $i \in \{1, 2, \ldots, n\}$, the map

$$\begin{aligned} \iota_i : G_i &\longrightarrow G = G_1 \times \cdots G_{i-1} \times G_i \times G_{i+1} \times \cdots \times G_n \\ g_i &\longmapsto (1, \ldots, 1, g_i, 1, \ldots, 1) \end{aligned}$$

defines an isomorphism between G_i and the subgroup

$$\{1\} \times \cdots \times \{1\} \times G_i \times \{1\} \times \cdots \times \{1\} \leq G.$$

Identifying G_i with this subgroup, $G_i \trianglelefteq G$ and

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

2. For each $i \in \{1, 2, \ldots, n\}$, the map

$$\begin{aligned} \pi_i : G_1 \times \cdots \times G_n &\longrightarrow G_i \\ (g_1, \ldots, g_n) &\longmapsto g_i \end{aligned}$$

is a surjective homomorphism with

$$\begin{aligned} \ker \pi_i &= G_1 \times \cdots \times G_{i-1} \times \{1\} \times G_{i+1} \times \cdots \times G_n \\ &\cong G_1 \times \cdots G_{i-1} \cdots G_{i+1} \times \cdots \times G_n. \end{aligned}$$

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

Proof:

□

6.1.3. *Proposition*

Let H and K be subgroups of a group G and let $f : H \times K \to G$ be the multiplication map, defined by $f(h, k) = hk$.

1. f is injective iff $H \cap K = \{1\}$
2. f is a homomorphism iff elements of H commute with elements of K, i.e., $hk = kh$ for all $h \in H, k \in K$
3. f is an isomorphism iff $H \cap K = \{1\}$, $HK = G$, and both H and K are normal subgroups of G

Proof:

1. Suppose that $H \cap K \neq \{1\}$. Then $H \cap K$ contains a nonidentity element x. Then $x^{-1} \in H$ and $f(x^{-1}, x) = 1 = f(1, 1)$, which shows that f is not injective.

   Now suppose that $H \cap K = \{1\}$. Let $(h_1, k_1), (h_2, k_2) \in H \times K$ and suppose that $f(h_1, k_1) = f(h_2, k_2)$. Then $h_1 k_1 = h_2 k_2$. Left multiplying both sides by h_1^{-1} and right multiplying by k_2^{-1}, we find $k_1 k_2^{-1} = h_1^{-1} h_2$. This element is in $H \cap K$, so $k_1 k_2^{-1} = 1 = h_1^{-1} h_2$, meaning $h_1 = h_2$ and $k_1 = k_2$. Therefore $(h_1, k_1) = (h_2, k_2)$.

2. $$\begin{aligned} f \text{ is a homomorphism} &\iff f((h_1, k_1)(h_2, k_2)) = f(h_1, k_1) f(h_2, k_2) \forall (h_1, k_1), (h_2, k_2) \in H \times K \\ &\iff f(h_1, h_2, k_1, k_2) = f(h_1, k_1) f(h_2, k_2) \forall h_1, h_2 \in H, k_1, k_2 \in K \\ &\iff h_1 h_2 k_1 k_2 = h_1 k_1 h_2 k_2 \forall h_1, h_2 \in H, k_1, k_2 \in K \\ &\iff h_2 k_1 = k_1 h_2 \forall h_2 \in H, k_1 \in K. \end{aligned}$$

3. Suppose that $H \cap K = \{1\}$, $HK = G$ and both H and K are normal subgroups of G. Then f is injective by (i), and it is surjective since its image is clearly HK. By (ii), in order to conclude that f is an isomorphism, it suffices to show that $hk = kh$ for all $h \in H, k \in K$. Consider the product $(hkh^{-1})k^{-1} = h(kh^{-1}k^{-1})$. Since K is normal, the left side is in K, and since H is normal, the right side is in H. Since $H \cap K = \{1\}$, we deduce that $hkh^{-1}k^{-1} = 1$ and therefore $hk = kh$.

   Conversely, suppose f is an isomorphism. Note that $H = f(H \times \{1\})$ and $K = f(\{1\} \times K)$. Since f is an isomorphism, it suffices to show that
   - $(H \times \{1\}) \cap (\{1\} \times K) = \{(1, 1)\}$
   - $(H \times \{1\})(\{1\} \times K) = H \times K$
   - $H \times \{1\} \trianglelefteq H \times K$ and $\{1\} \times K \trianglelefteq H \times K$

   The first two conditions are clear, whereas the third one follows from Proposition 6.1.2(i).

□

6.1.4. *Proposition*

Let G be a group. Let $H_1, ..., H_n$ be normal subgroups of G such that

- $H_1 H_2 \cdots H_n = G$,
- for all $i \in \{1, 2, ..., n\}$,

  $$H_i \cap (H_1 \cdots H_{i-1} H_{i+1} \cdots H_n) = \{1\}.$$

Then $G \cong H_1 \times H_2 \cdots \times H_n$.

Proof:

□

6.1.5. *Proposition*

Let $m, n \in \mathbb{Z}_{>0}$. Then $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ if and only if $(m, n) = 1$.

Proof: Let $l = \operatorname{lcm}(m, n)$. Let $([a]_m, [b]_m) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Then (using additive notation)

$$l([a]_m, [b]_n) = ([la]_m, [lb]_n) = ([0]_m, [0]_n).$$

Therefore, the order of every element in $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ divides l.

Suppose that $(m, n) > 1$. Since $l = mn/(m, n)$, it follows that $l < mn$. Since the element $[1]_{mn} \in \mathbb{Z}/mn\mathbb{Z}$ has order mn, whereas every element in $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ has order a divisor of l, we deduce that $\mathbb{Z}/mn\mathbb{Z} \ncong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

Now suppose that $(m, n) = 1$. In this case, one can show easily (exercise) that the map

$$\begin{aligned} \mathbb{Z}/mn\mathbb{Z} &\longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ [a]_{mn} &\longmapsto ([a]_m, [a]_n) \end{aligned}$$

is a well defined isomorphism.

□

6.1.6. *Corollary*

Let $n \in \mathbb{Z}_{>0}$. If $n = p_1^{a_1} \cdots p_r^{a_k}$, where $p_1, ..., p_k$ are distinct primes, then

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p^{a_1}\mathbb{Z} \times \mathbb{Z}/p^{a_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{a_k}\mathbb{Z}.$$

Proof: The result follows easily from the proposition by induction on k.

□

6.2. Fundamental Theorem of Finitely Generated Abelian Groups

6.2.1. *Theorem:* Fundamental Theorem of Finitely Generated Abelian Groups

Let G be a finitely generated abelian group.

1. There exist unique integers $r \geq 0$ and $n_1, ..., n_s \geq 2$, with $n_{i+1} \mid n_i$ for all $1 \leq i \leq s - 1$ such that

$$G \cong \mathbb{Z}^r \times \mathbb{Z}/n_1\mathbb{Z} \times \cdots \mathbb{Z}/n_s\mathbb{Z}.$$

The integer r is called the **free rank** of G, the integers $n_1, ..., n_s$ are called the **invariant factors** of G, and the isomorphism above is called the **invariant factor decomposition** of G.

2. With r as in (i), there exist integers $q_1, ..., q_t$ which are powers of (not necessarily distinct) primes such that

$$G \cong \mathbb{Z}^r \times \mathbb{Z}/q_1\mathbb{Z} \times \cdots \times \mathbb{Z}/q_s\mathbb{Z}.$$

The powers of the primes $q_1, ..., q_t$ are unique up to order. They are called the **elementary divisors** of G and the isomorphism above is called the **elementary divisor decomposition** of G.

Proof: A more general version of this theorem is shown in 111B, so we omit the proof here.

□

6.2.2. Remark

Two finitely generated abelian groups are isomorphic if and only if they have the same free rank and the same invariant factors if and only if they have the same free rank and same elementary divisors. Therefore, the isomorphism class of a finitely generated abelian group is determined by the free rank and the invariant factors, and also by the free rank and the elementary divisors.

Note a finitely generated abelian group is finite if and only if its free rank is zero. In this case the order of the group is equal to the product of its invariant factors, and also to the product of its elementary divisors.

6.2.3. Definition: Torsion Subgroup and Free Abelian Group

Let G be a finitely generated abelian group with invariant factor decomposition

$$G \cong \mathbb{Z}^r \times \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_s\mathbb{Z}.$$

The subgroup of G corresponding via this isomorphism to

$$\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_s\mathbb{Z}$$

is called the **torsion subgroup** of G. If the torsion subgroup of G is trivial, we say that G is a **free abelian group** of rank r.

6.2.4. Remark

Let G be a finitely generated abelian group. The torsion subgroup of G is uniquely characterized as

$$G_{\text{tors}} = \{x \in G : nx = 0 \text{ for some } n \in \mathbb{Z}_{>}0\}.$$

6.2.5. Example

1. Let $G = \mathbb{Z}/9\mathbb{Z}$ and $H = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. They are both written in their invariant factor decomposition, which in this case is also their elementary divisor decomposition. Therefore $G \ncong H$.
2. Let $G = \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$. Note that $\mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ and $\mathbb{Z}/18\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$. Therefore, the elementary divisor decomposition of G is given by

   $$G \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.$$

   To obtain the invariant factor decomposition of G, note that

   $$G \cong (\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) \cong \mathbb{Z}/36\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}.$$

3. Let G be a group of finite order n. Let $n = p_1^{a_1} \cdots p_k^{a_k}$ be the prime factorization of n, where $p_1, ..., p_k$ are distinct primes. Then, the elementary divisor decomposition of G is of the form

   $$G \cong \left(\mathbb{Z}/p_1^{b_{11}}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_1^{b_{1t_1}}\right) \times \cdots \times \left(\mathbb{Z}/p_k^{b_{k1}}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{b_{kt_k}}\mathbb{Z}\right)$$

   with

   $$\begin{gathered} b_{11} + \cdots + b_{1t_1} = a_1, \\ \vdots \\ b_{k1} + \cdots + b_{kt_k} = a_k. \end{gathered}$$

   Therefore, there is a one-to-one correspondence between the set of isomorphism classes of finite abelian groups of order n and the set

   $$\{\text{partitions of } a_1\} \times \cdots \times \{\text{partitions of } a_k\}.$$

6.3. Exercises

6.3.1. Exercise

Let G be a finite abelian group with invariant factors $n_1, n_2, ..., n_s$. Prove that G contains an element of order m if and only if $m \mid n$.

Solution

Take the isomorphism

$$G \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_s\mathbb{Z}$$

where $n_{i+1} \mid n_i$ for $i = 1, ..., s - 1$. Let $x \in \mathbb{Z}/n_1\mathbb{Z} \times \cdots \mathbb{Z}/n_s\mathbb{Z}$. Then $x = \left([a_1]_{n_1}, ..., [a_s]_{n_s}\right)$ and

$$n_1 x = \left([n_1 a_1]_{n_1}, ..., [n_1 a_s]_{n_s} = \left([0]_{n_1}, ..., [0]_{n_s}\right)\right)$$

so $\operatorname{ord}(x) \mid n_1$. Then if $\exists x \in G$ with $\operatorname{ord}(x) = m$, then $m \mid n_1$. If $m \mid n_1$, take

$$\left(\left[\frac{n_1}{m}\right]_{n_1}, [0]_{n_2}, ..., [0]_{n_s}\right)$$

has order m.

6.3.2. Exercise

Let $G = (x_1) \times (x_2) \times \cdots \times (x_k)$ where $\operatorname{ord}(x_i) = p^{a_i}$ for some $a_i > 0$. Define

$$\begin{aligned} \varphi : G &\longrightarrow G \\ a &\longmapsto a^p \end{aligned}$$

1. Show that φ is a homomorphism.
2. Find $\ker \varphi$ and $\operatorname{im} \varphi$.

Solution

1. Since G is abelian, $\varphi(ab) = (ab)^p = a^p b^p = \varphi(a)\varphi(b)$.
2. We have $\ker \varphi = \left(x_1^{p^{a_1-1}}\right) \times \cdots \times \left(x_k^{p^{a_k-1}}\right)$. Also $\operatorname{im} \varphi = (x_1^p) \times \cdots \times (x_k^p)$. Thus $\ker \varphi \cong \underbrace{\mathbb{Z}/p\mathbb{Z} \times \cdots \times \mathbb{Z}/p\mathbb{Z}}_{k \text{ times}}$.

   Thus

   $$((x_1) \times \cdots \times (x_k))/((x_1^p) \times \cdots \times (x_k^p)) \cong (x_1)/(x_1^p) \times (x_2)/(x_2^p) \times \cdots \times (x_k)/(x_k^p).$$

   So if we define

   $$\begin{aligned} \psi : \mathbb{Z} &\longrightarrow (x_i)/(x_i^p) \\ a &\longmapsto x_i^a(x_1^p) \end{aligned}$$

   with

   $$\begin{aligned} \ker \psi &= \{a \in \mathbb{Z} : x_i^a \in (x_i^p)\} \\ &= \left\{a \in \mathbb{Z} : x_i^a = x_i^{k_p} \text{ for some } k \in \mathbb{Z}\right\} \\ &= \{a \in \mathbb{Z} : a \equiv kp \pmod{p_i^{a_i}} \text{ for some } k \in \mathbb{Z}\} \\ &= p\mathbb{Z} \end{aligned}$$

   Then by the First Isomorphism Theorem,

   $$\mathbb{Z}/p\mathbb{Z} \cong (x_i)/(x_i^p).$$