PMATH 347 – GROUP THEORY LECTURES

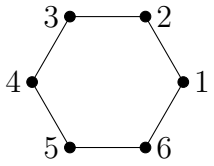
R. WILLARD

Contents

1. Dihedral Symmetries

For $n \geq 3$, let C_n denote a regular n-gon (embedded in $\mathbb{R}^3$). A **dihedral symmetry** of C_n is any "rigid motion" of $\mathbb{R}^3$ which moves C_n back to itself.

We usually label the vertices of C_n by $1, 2, \ldots, n$. For example, let $n = 6$:



Dihedral symmetries of C_6 include:

- Rotations around the center of C_6 (by multiples of 60°).
- "Flips" (called **reflections**) along an axis – either through two opposite vertices, or through the centers of two opposite sides.
- The "identity" symmetry (which does nothing).

Definition. D_{2n} = the set of all dihedral symmetries of C_n.

Note: In geometry the set is called D_n.

D_{2n} clearly includes:

- n rotations (including the identity symmetry), by multiples of $2\pi/n$ radians.
- n reflections.

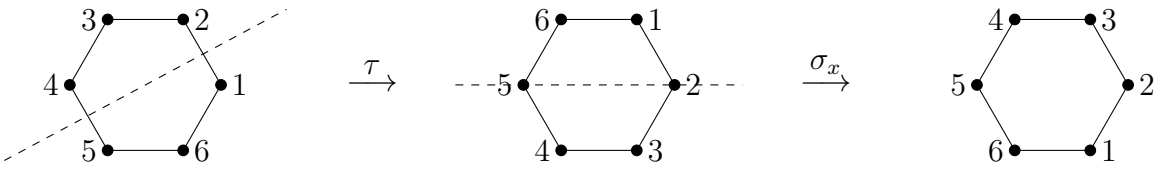
Let's prove that there are no other dihedral symmetries than these.

Lemma 1.1. $|D_{2n}| = 2n$.

Proof. We've already seen that $|D_{2n}| \geq 2n$. To prove the opposite inequality, suppose σ is an arbitrary dihedral symmetry of C_n. Then σ must send 1 to some vertex $i \in \{1, 2, \ldots, n\}$. Since σ preserves the edges of C_n, it must send 2 to either $i + 1$ or $i - 1$. Thus there are only $n \times 2$ possibilities for the pair $(\sigma(1), \sigma(2))$ of values of σ at the vertices 1,2. Since the pair $(\sigma(1), \sigma(2))$ determines σ (think about it), we have $|D_{2n}| \leq 2n$. □

We can combine or "multiply" dihedral symmetries, by applying one first and then the other. Convention: $\sigma \cdot \tau$ means "τ first, then σ."

Example 1.2. Let σ_x be the reflection through the x-axis (i.e., the line through vertices 4 and 1), and let τ be the reflection through the line through the centers of 12 and 45. Then $\sigma_x \cdot \tau$ is



Thus $\sigma_x \cdot \tau$ = rotation **clockwise (cw)** by 60° (or $\pi/3$ radians).

Exercise: check that $\tau \cdot \sigma_x$ = rotation **counter-clockwise (ccw)** by 60°.

We adopt the following convention. When n is understood, we let:

- r denote the rotation counter-clockwise by $2\pi/n$ radians.
- s denote reflection through the x-axis.
- 1 denote the identity symmetry.

Thus r^2 $(= r \cdot r)$ is rotation by $4\pi/n$ radians ccw, r^3 is rotation by $6\pi/n$ radians ccw, etc. Note that $r^n = 1$. What is r^{n-1}? We also write this symmetry as r^{-1}.

One can check that:

- sr = reflection through the line through centers of the edge $1n$ and the edge opposite to $1n$.
- sr^2 = reflection through the line through the vertex n and the vertex opposite to n.
- sr^3 = reflection through the line through the centers of the edge $n{-}1, n$ and the edge opposite to $n{-}1, n$.
- Etc.

Thus $s, sr, sr^2, \ldots, sr^{n-1}$ enumerate all n reflections. Hence we can write

$$D_{2n} = \{r^i : 0 \leq i < n\} \cup \{sr^i : 0 \leq i < n\}.$$

The expressions $1, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1}$ are called the *normal forms* for the symmetries they represent.

Here is one more useful fact:

- $rs = sr^{n-1}$ $(= sr^{-1})$.

This last fact gives us an easy way to multiply two symmetries. E.g.,

$$sr^2 \cdot sr = srrsr = (sr)(rs)r = (sr)(sr^{-1})r = s(rs) = s(sr^{-1}) = r^{-1}.$$

(Note that $s^2 = 1$.) In fact, all that we need to know to calculate products of normal forms is $\boxed{r^n = s^2 = 1 \text{ and } rs = sr^{-1}}$.

Note: The calculation displayed above used **associativity** of multiplication to permit parsing $srrsr$ as either $(sr^2)(sr)$ or $(sr)(rs)r$. This can be justified as long as multiplication of dihedral symmetries satisfies the **associative law**: $x(yz) = (xy)z$ for any choices of x, y, z. In fact, multiplication of dihedral symmetries *does* satisfy the associative law, since for any dihedral symmetries x, y, z of C_n:

- $(xy)z$ is the symmetry obtained by first applying z and then applying xy. But note that applying xy just means applying y and then applying x. Thus $(xy)z$ can be computed by first applying z, then y, and finally x.
- Similarly, $x(yz)$ is the symmetry obtained by first applying yz and then applying x. Since applying yz just means applying z and then applying y, this means $x(yz)$ can be computed by first applying z, then y, and finally x.

Hence $x(yz)$ and $(xy)z$ always compute the same dihedral symmetry.

2. Permutations

Definition. Let X be any non-empty set.

(1) A **permutation** of X is a bijection $\sigma\colon X \to X$.
(2) S_X is the set of all permutations of X.
(3) If $X = \{1, 2, 3, \ldots, n\}$ then we denote S_X by S_n.

What is $|S_n|$? (Answer: $n!$) Proof: there are n choices for $\sigma(1)$; once chosen, there are $n-1$ choices for $\sigma(2)$; etc. The total number of choices for values is $n\cdot(n-1)\ldots 2\cdot 1$.

When X is finite we use a special notation to describe permutations. Example: let $\sigma \in S_8$ be the function

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

Start with $x = 1$; where does σ send it? to 4. Then where does σ send 4? to 3. Repeat:

$$1 \mapsto 4 \mapsto 3 \mapsto 6 \mapsto 1.$$

We encode this information as (1 4 3 6). It gives the values of σ at 1, 3, 4 and 6.

We can start with 2: $2 \mapsto 8 \mapsto 7 \mapsto 2$. We record this information as (2 8 7).

All that is left is the element 5. $5 \mapsto 5$ and we record this as (5).

We put it all together and write

$$\sigma = (1\,4\,3\,6)(2\,8\,7)(5).$$

This notation completely specifies σ. Note that we could have also written

$$\begin{aligned}\sigma &= (2\,8\,7)(5)(1\,4\,3\,6)\\ &= (3\,6\,1\,4)(5)(7\,2\,8)\end{aligned}$$

etc. There is no uniqueness of notation. What is unique is the individual **cycles**. In this example we say that σ **decomposes** into one 4-cycle, one 3-cycle, and one 1-cycle. Also note that in cycle notation, **the cycles are (pairwise) disjoint.**

Convention: We usually omit 1-cycles. Thus in this example, $\sigma = (1\ 4\ 3\ 6)(2\ 8\ 7)$.

Inverses. Note that if $\sigma \in S_X$, then σ^{-1} exists and is also in S_X. The cycle notation for σ^{-1} is easy: just reverse the cycles of σ. E.g., if

$$\sigma = (1\,4\,3\,6)(2\,8\,7)$$

then

$$\sigma^{-1} = (1\,6\,3\,4)(2\,7\,8).$$

Composition. Suppose $\sigma, \tau \in S_X$. So they are both functions $X \to X$. So we can compose them to get another permutation $\sigma \circ \tau : X \to X$, which we write as $\sigma\tau$.

For example, suppose σ is as before and let $\tau = (2\ 4\ 8\ 5)(1\ 7)$. In other words, τ is the function

x	1	2	3	4	5	6	7	8
$\tau(x)$	7	4	3	8	2	6	1	5

Let's find $\sigma\tau$. We have

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

and so on. The full table is

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

Now let's find the cycle notation for $\sigma\tau$ (from the table). We see that

$$\sigma\tau = (1\,2\,3\,6)(4\,7)(5\,8).$$

Actually, we could have found this directly from the cycle notations for σ and τ, as follows:

(1) Write the cycle notation for σ followed by the notation for τ:

$$\sigma\tau = \underbrace{(1\,4\,3\,6)(2\,8\,7)}_{\sigma}\underbrace{(2\,4\,8\,5)(1\,7)}_{\tau}.$$

(Note that this expression is technically **not** cycle notation, because the cycles are not all disjoint.)

(2) Start with 1; reading the cycles from **right to left**, find the first cycle that moves 1 ($1 \mapsto 7$). Continuing to the left, find the first cycle that moves 7 ($7 \mapsto 2$); continue to the left, find the first cycle that moves 2 (there is none). So $\sigma\tau$ sends $1 \mapsto 2$. Continue in this way to find

$$\sigma\tau = (1\,2\,3\,6)(4\,7)(5\,8).$$

Let's compute $\tau\sigma$.

$$\tau\sigma = \underbrace{(2\,4\,8\,5)(1\,7)}_{\tau}\underbrace{(1\,4\,3\,6)(2\,8\,7)}_{\sigma} = (1\,8)(2\,5)(3\,6\,7\,4).$$

Note that $\sigma\tau \neq \tau\sigma$. (However $\sigma\tau$ and $\tau\sigma$ do have the same "cycle structure". Is this always true?)

Special notation, terminology.

(1) id denotes the identity permutation in S_X (so $\mathrm{id}(x) = x$ for all $x \in X$).
(2) The cycle notation for id is () or just . (Empty)
(3) Given $\sigma \in S_X$, the **support** of σ is the set

$$\mathrm{supp}(\sigma) = \{x \in X : \sigma(x) \neq x\}.$$

Equivalently, $\mathrm{supp}(\sigma)$ is the set of elements mentioned in the cycle notation of σ.

(4) σ, τ are **disjoint** if $\mathrm{supp}(\sigma) \cap \mathrm{supp}(\tau) = \varnothing$.

3. Definition of a Group

Definition. Let A be a non-empty set. A *binary operation on* A is a function $*$ whose domain is $A \times A$ (the set of all ordered pairs from A) and which maps into A.

Notational convention: we write $a*b$ for the value of $*$ at (a, b), instead of writing $*(a, b)$.

Definition. A **group** is an ordered pair $(G, *)$ where

- G is a non-empty set;
- $*$ is a binary operation on G;

which jointly satisfy the following further conditions:

(i) $*$ is **associative**: $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$;
(ii) There exists an **identity** element $e \in G$: $a * e = e * a = a$ for all $a \in G$;
(iii) Every $a \in G$ has a 2-sided **inverse**, i.e., an element $a' \in G$ which satisfies $a * a' = a' * a = e$ (where e is the identity element from (ii)).

Example 3.1.

(1) $(\mathbb{Z}, +)$.
- $a, b \in \mathbb{Z}$ implies $a + b \in \mathbb{Z}$, so $+$ is a binary operation on $\mathbb{Z}$.
- $+$ is associative (well-known).
- $0 \in \mathbb{Z}$ satisfies $a + 0 = 0 + a = 0$ for all $a \in \mathbb{Z}$.
- Every $n \in \mathbb{Z}$ has an inverse $-n \in \mathbb{Z}$, and $n + (-n) = (-n) + n = 0$.

(2) $(D_{2n}, \cdot)$ for each $n \geq 3$. (Called the *dihedral group of order* $2n$.)
- $\sigma, \tau \in D_{2n}$ implies $\sigma \cdot \tau \in D_{2n}$, so $\cdot$ is a binary operation on D_{2n}.
- $\cdot$ is associative (see note at end of first lecture).
- 1 (the identity symmetry) satisfies $\sigma \cdot 1 = 1 \cdot \sigma = \sigma$ for all $\sigma \in D_{2n}$.
- Every $\sigma \in D_{2n}$ has an inverse symmetry $\sigma^{-1} \in D_{2n}$ (doing σ in reverse), and $\sigma \cdot \sigma^{-1} = \sigma^{-1} \cdot \sigma = 1$.

(3) $(S_n, \circ)$ for each $n \geq 2$. (Called the *symmetric group of degree* n.)
- $\sigma, \tau \in S_n$ implies $\sigma \circ \tau \in S_n$, so $\circ$ is a binary operation on S_n.
- $\circ$ is associative (because it is composition of functions).
- id (the identity permutation) satisfies $\sigma \circ \mathrm{id} = \mathrm{id} \circ \sigma = \sigma$ for all $\sigma \in S_n$.
- Every $\sigma \in S_n$ has an inverse function $\sigma^{-1} \in S_n$ and $\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = \mathrm{id}$.

(4) ($\{$all invertible $n \times n$ matrices over $\mathbb{R}\}$, matrix multiplication) is a group for each $n \geq 1$. It is called $GL_n(\mathbb{R})$.

(5) $(\mathbb{Z}_n, +\bmod n)$ is a group for each $n \geq 1$.

The groups in (2), (3) and (5) and *finite*, while those in (1) and (4) are *infinite*.

Notation: when discussing generic (or random, or arbitrary) groups,

- We often denote a group $(G, *)$ by just G. (Exception: in situations such as in Section 5 where we want a single symbol to represent the group but want to distinguish the group from its underlying set, we use different fonts, for example writing the group as $\mathbb{G}$ and its underlying set as G.)

- Write ab (or sometimes $a \cdot b$) for $a * b$ (most of the time).
- Denote the identity element e of G by 1 (most of the time).
- Denote the inverse a' of an element a by a^{-1} (most of the time).
- The **order** of a group G, denoted $|G|$, is the number of its elements.

Definition. In any group G, if $a \in G$ then define $a^0 = 1$ and $a^{n+1} = a \cdot a^n$ for $n \geq 0$. Also define $a^{-n} = (a^n)^{-1}$ for $n \geq 2$.

This notation satisfies the usual rules for exponents:

Lemma 3.2. *Let $(G, \cdot)$ be a group, $a \in G$, and $m, n \in \mathbb{Z}$.*

(1) $a^1 = a$.
(2) $a^m \cdot a^n = a^{m+n}$.
(3) $(a^m)^n = a^{mn}$.

Proof sketch. By induction and case-analysis, depending on whether $m, n > 0$, $= 0$, $= -1$, or < -1, heavily using associativity. □

Warning. In general, it is not true that $(ab)^n = a^n b^n$. E.g., $(ab)^2 = abab$ while $a^2b^2 = aabb$. In order to have $abab = aabb$ we would need $ba = ab$ (see Proposition 4.1 in Section 4), which we've already seen can fail to be true.

Warning. In groups for which the operation is addition, power notation can be alarming. E.g., in the group $(\mathbb{R}, +)$, if $a \in \mathbb{R}$ and $n \geq 2$, then $a^n = \underbrace{a + a + \ldots a}_{n}$, which seems weird. It also seems weird to denote the identity element as 1 (since it is actually 0), and to denote the inverse of a as a^{-1} (since it is actually $-a$). Because of our discomfort and inability to think flexibly, we allow the following alternative notations (called *additive notation*).

Additive Notation. When the group operation is denoted $+$ (or more generally, whenever we are thinking of the operation as a "kind of addition"), we may:

- Denote the identity element by 0 (instead of 1).
- Denote the inverse of a by $-a$ (instead of a^{-1}).
- Denote $\underbrace{a + \cdots + a}_{n}$ by na (instead of a^n), for any $n \geq 1$.

However: additive notation is almost never used when the group operation is not commutative.

Most "pure" group theorists rarely or never use additive notation, but I encourage you to learn to take any result written in the "usual" (multiplicative) notation and translate it into additive notation.

Finite groups exhibit *periodicity* in the following way. Suppose $a \in G$ and consider $a, a^2, a^3, a^4, \ldots$. If G is finite, then there must be a repeat, say $a^i = a^j$ with $i < j$. Multiply both sides by a^{-i} to get $a^0 = a^{j-i}$. This proves the existence of $n > 0$ such that $a^n = 1$. Then $a^{n+1} = a^n a^1 = 1a = a$, $a^{n+2} = a^2$, etc.

Definition. For a group G and element $a \in G$, the **order** of a (denoted $|a|$ or $\circ(a)$) is the least integer $n > 0$ such that $a^n = 1$, if it exists. If no such n exists (this requires G to be infinite), then the order of a is defined to be ∞.

Remark. Note the two uses of the word "order" defined in this section:

- of a *group* (the number of elements of the group), or
- of an *element* of a group (the least positive exponent giving the identity element).

We will see a connection between these two uses of the word "order" in Corollary 6.7.

Proposition 3.3. *Suppose G is a group, $a \in G$, and $\circ(a) = n < \infty$. Then for all $k \in \mathbb{Z}$, $a^k = 1 \iff n|k$.*

Proof. We will show the stronger claim that, for arbitrary $k, \ell \in \mathbb{Z}$, $a^k = a^\ell \iff k \equiv \ell \pmod{n}$. (The original claim follows by setting $\ell = 0$.)

($\Leftarrow$) Assume $k \equiv \ell \pmod{n}$. Then $k = \ell + nq$ for some $q \in \mathbb{Z}$. Then $a^k = a^{nq+\ell} = (a^n)^q \cdot a^\ell = 1^q \cdot a^\ell = a^\ell$.

($\Rightarrow$) Assume $a^k = a^\ell$. Then $a^{k-\ell} = 1$. Use the Division Algorithm to divide $k - \ell$ by n getting a quotient q and remainder r satisfying $k - \ell = nq + r$ and $0 \leq r < n$. Then $1 = a^{k-\ell} = a^{nq+r} = (a^n)^q \cdot a^r = 1 \cdot a^r = a^r$. Since $r < n$ and n is the smallest positive exponent of a giving value 1, it must be that r is not positive, i.e., $r = 0$, proving $k - \ell = nq$ and thus $k \equiv \ell \pmod{n}$. □

Example 3.4.

- In D_{2n}, the rotation r has order n because $r \neq 1$, $r^2 \neq 1, \ldots, r^{n-1} \neq 1$ but $r^n = 1$. [Question: what is the order of a reflection in D_{2n}?]
- In $\mathbb{Z}_4$, what is the order of 1? ($1 \neq 0$, $1 + 1 \neq 0$, $1 + 1 + 1 \neq 0$, but $1 + 1 + 1 + 1 = 0$.)
- In S_7, what is the order of $(1\ 2)(3\ 5\ 7)$?
- In $GL_2(\mathbb{R})$, what is the order of $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$? Of $\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$?

4. Elementary Properties of Groups

Proposition 4.1. *Let G be a group and $a,b,u,v \in G$.*

(1) *Left and right cancellation:*
   (a) *If $au = av$, then $u = v$.*
   (b) *If $ub = vb$, then $u = v$.*
(2) *The equations $ax = b$ and $ya = b$ have unique solutions for x, $y \in G$.*

Proof. (1) Assume $au = av$. Then $a^{-1}(au) = a^{-1}(av)$. Thus

$$u = 1u = (a^{-1}a)u = a^{-1}(au) \stackrel{*}{=} a^{-1}(av) = (a^{-1}a)v = 1v = v.$$

The proof of right cancellation is similar.

(2) Let $x := a^{-1}b$. x is one solution to $ax = b$: $a(a^{-1}b) = (aa^{-1})b = 1b = b$. Conversely, suppose u is a solution. Then $au = ax$, so $u = x$. Similarly, $y := ba^{-1}$ is the unique solution to $ya = b$. □

Corollary 4.2. *In any group G, the identity element is unique.*

Proof. Suppose d, e are both identity elements of G. Thus $xd = dx = x$ and $xe = ex = x$ for all $x \in G$. In particular, $xd = xe$. Hence $d = e$ by left cancellation. □

Similar tricks let us prove the following.

Proposition 4.3. *Suppose G is a group.*

(1) *Each $a \in G$ has a unique inverse a^{-1}.*
(2) *$(a^{-1})^{-1} = a$ for all $a \in G$.*
(3) *$(ab)^{-1} = (b^{-1})(a^{-1})$ for all a, $b \in G$.*

Proof. (1) Suppose that a has two inverses a' and a^*. That means $aa' = a'a = 1$ and $aa^* = a^*a = 1$. Find a way to use left cancellation to deduce $a' = a^*$.

(2) Let $b = a^{-1}$. We are required to show that $b^{-1} = a$. We know that $bb^{-1} = b^{-1}b = 1$ and $ab = ba = 1$. Use left cancellation.

(3) We'll use a similar trick. Let $c = ab$ and $d = b^{-1}a^{-1}$. We want to show $c^{-1} = d$, so it suffices to show $cc^{-1} = cd$. Well, $cc^{-1} = 1$, while

$$cd = (ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = a1a^{-1} = (a1)a^{-1} = aa^{-1} = 1.$$

Thus $cc^{-1} = cd$, so $c^{-1} = d$ by left cancellation. □

Definition. If $(G, *)$ is a finite group, with elements ordered $\{g_1, g_2, \ldots, g_n\}$, then the *table* for G (with respect to this ordering) is the $n \times n$ matrix whose (i, j) entry is $g_i * g_j$. It is customary to "dress up" the matrix by listing the elements $g_1, \ldots, g_n$ vertically to the left of the matrix and again horizontally above the matrix, separating these lists from the matrix by lines and finally putting the name of the group operation in the upper-left corner.

For example, the table for $\mathbb{Z}_4$ with respect to the standard ordering is

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Fact. Suppose G is a *finite* group. In the table for its operation,

(1) Each row is a permutation of G.
(2) Each column is a permutation of G.

To see why, suppose that some element u occurs twice in row a, so

$\cdot$	1	$\cdots$	b	$\cdots$	c	$\cdots$
1	1	$\cdots$	b	$\cdots$	c	$\cdots$
$\vdots$						
a	a		u		u	
$\vdots$						

This means $ab = ac$, but $b \neq c$, contradicting left cancellation. Hence no element occurs more than once in the row labeled by a. Thus the function $f : G \to G$ given by $f : x \mapsto ax$ is injective. Since G is finite, it follows that f is a bijection, i.e., a permutation of G.

The same thing works for any row, and a similar argument works for any column.

Some jargon:

(1) G is **abelian** (named for Niels Henrik Abel, 1802-1829) if $ab = ba$ for all $a, b \in G$.
(2) If $a \in G$ then $\langle a \rangle$ denotes the set $\{a^n : n \in \mathbb{Z}\}$. Thus $\langle a \rangle \subseteq G$.
(3) G is **cyclic** if there exists $a \in G$ such that $G = \langle a \rangle$.
    - In this case we call a a **generator** of G.

    Note: a cyclic group can have more than one generator.

Example 4.4.

(1) $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$, and $(\mathbb{Z}_n, +\pmod n)$ $(n \geq 1)$ are all abelian.
(2) Given $n \geq 2$, let $\mathbb{Z}_n^\times = \{a \in \mathbb{Z}_n : \gcd(a, n) = 1\}$. It can be shown that $(\mathbb{Z}_n^\times, \cdot \pmod n)$ is a group (exercise). It is abelian for any $n \geq 2$.
(3) D_{2n}, S_n are not abelian $(n \geq 3)$.
(4) Suppose $\mathbb{F}$ is a field (e.g., $\mathbb{F}$ could be $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$, or $\mathbb{Z}_p$ (p prime)). $GL_n(\mathbb{F})$ denotes the set of all invertible $n \times n$ matrices with entries from $\mathbb{F}$. $GL_n(\mathbb{F})$ with matrix multiplication is a group (exercise). It is nonabelian if n ≥ 2.
(5) $(\mathbb{Z}, +)$ is cyclic, generated by 1. This is because $\langle 1 \rangle = \{n1 : n \in \mathbb{Z}\} = \mathbb{Z}$. -1 is another generator.
(6) $(\mathbb{Z}_n, +)$ is cyclic for every $n \geq 1$. How many generators does $(\mathbb{Z}_n, +)$ have?
(7) $(\mathbb{R}, +)$ is not cyclic. Are D_{2n}, S_n cyclic? No: every cyclic group is abelian and countable (exercise).
(8) Is $(\mathbb{Z}_n^\times, \cdot)$ cyclic?

5. Isomorphisms

The most fundamental relation between groups is that of *isomorphism*.

Definition. Let $\mathbb{G} = (G, \star)$ and $\mathbb{H} = (H, \diamond)$ be groups. A function $\varphi : G \to H$ is an **isomorphism from $\mathbb{G}$ to $\mathbb{H}$** if φ is a bijection and

$$\varphi(x \star y) = \varphi(x) \diamond \varphi(y) \qquad \text{for all } x, y \in G.$$

Example 5.1. Suppose $\mathbb{G} = (\mathbb{Z}_4, +)$ and $\mathbb{H} = (\mathbb{Z}_5^\times, \cdot)$.

(1) The map $\varphi : G \to H$ given by $\varphi(i) = i + 1$ is <u>not</u> an isomorphism. It is a bijection, but when $x = y = 3$, the requirement $\varphi(x + y) = \varphi(x) \cdot \varphi(y)$ fails because

$$\varphi(3 + 3) = \varphi(2) = 3 \qquad \text{while} \qquad \varphi(3) \cdot \varphi(3) = 4 \cdot 4 = 1.$$

(2) The map $\psi : G \to H$ given by $\psi(i) = 2^i \pmod 5$ <u>is</u> an isomorphism.

(a)

i	0	1	2	3
$\psi(i)$	1	2	4	3

, so ψ is a bijection.

(b) Regarding the condition $\psi(x + y) = \psi(x) \cdot \psi(y)$, note first that for all $a, b \in \mathbb{Z}$, if $a \equiv b \pmod 4$ then $2^a \equiv 2^b \pmod 5$. Now suppose $i, j, k \in \mathbb{Z}_4$ with $i + j = k$ (in $\mathbb{Z}_4$, meaning $i + j \equiv k \pmod 4$). Then $2^{i+j} \equiv 2^k \pmod 5$, so

$$\psi(i + j) = \psi(k) = 2^k \pmod 5 = 2^{i+j} \pmod 5 = 2^i \cdot 2^j \pmod 5 = \psi(i) \cdot \psi(j).$$

Exploring the last example, consider the tables for $(\mathbb{Z}_4, +)$ and for $(\mathbb{Z}_5^\times, \cdot)$. If we order $\mathbb{Z}_4$ as (0, 1, 2, 3) and order $\mathbb{Z}_5^\times$ as (1, 2, 4, 3), then the tables are

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	1	2	4	3
1	1	2	4	3
2	2	4	3	1
4	4	3	1	2
3	3	1	2	4

The tables are "the same" modulo identifying $0 \mapsto 1$, $1 \mapsto 2$, $2 \mapsto 4$, and $3 \mapsto 3$; i.e., $x \mapsto \psi(x)$.

Theology:

(1) If φ is an isomorphism from $\mathbb{G}$ to $\mathbb{H}$, then the operation tables for $\mathbb{G}$ and $\mathbb{H}$ are "the same" (modulo the translation given by φ).
(2) If the operation tables for $\mathbb{G}$ and $\mathbb{H}$ are "the same" in this sense, then $\mathbb{G}$ and $\mathbb{H}$ are "essentially the same group."

Definition. We say that groups $\mathbb{G}$ and $\mathbb{H}$ are **isomorphic** and write $\mathbb{G} \cong \mathbb{H}$ if there exists an isomorphism $\varphi : G \to H$.

Example 5.2. $(\mathbb{Z}_5^\times, \cdot) \cong (\mathbb{Z}_4, +)$.

6. Subgroups

Definition. Let $\mathbb{G} = (G, \cdot)$ be a group. A **subgroup** of $\mathbb{G}$ is a subset $H \subseteq G$ satisfying

(1) $H \neq \varnothing$.
(2) H is closed under products; i.e., $a, b \in H$ implies $ab \in H$.
(3) H is closed under inverses; i.e., $a \in H$ implies $a^{-1} \in H$.

Example 6.1. Suppose $\mathbb{G} = (\mathbb{Z}, +)$.

(1) Let $E = \{\dots, -4, -2, 0, 2, 4, \dots\}$. Obviously nonempty. If $a, b \in E$ then a, b are even, so $a + b$ is even, so $a + b \in E$. Similarly, if a is even then so is $-a$, so E is closed under inverses. Thus H is a subgroup of $(\mathbb{Z}, +)$.
(2) The set of odd integers is *not* a subgroup of $(\mathbb{Z}, +)$.

Proposition 6.2. *If $\mathbb{G} = (G, \cdot)$ is a group and H is a subgroup of $\mathbb{G}$, then $\mathbb{H} = (H, \cdot\restriction_H)$ is a group in its own right. ($\cdot\restriction_H$ is the restriction of the operation $\cdot$ to pairs from H.)*

Proof sketch. We must check that all of the conditions in the definition of "group" are satisfied. Clearly $H \neq \varnothing$. Because H is closed under $\cdot$, the restriction $\cdot\restriction_H$ is a binary operation on H. The restriction $\cdot\restriction_H$ inherits the associative property from the operation $\cdot$ of G. Showing that $(H, \cdot\restriction_H)$ has an identity element amounts to showing that the identity element of G is in H. We can prove this as follows: pick any $a \in H$ (can do, $H \neq \varnothing$). Then $a^{-1} \in H$, so $1 = a \cdot a^{-1} \in H$ since H is closed under taking products and inverses in G. Finally, showing that $(H, \cdot\restriction_H)$ has inverses follows from the fact that H is closed under taking inverses in G. □

Conventions.

(1) In light of Proposition 6.2, we will return to being sloppy by not distinguishing between $\mathbb{H}$ and H (just as we usually don't distinguish between $\mathbb{G}$ and G).
(2) We will no longer write $(H, \cdot\restriction_H)$ and instead will just write $(H, \cdot)$.
(3) We write $H \leq G$ or $\mathbb{H} \leq \mathbb{G}$ to mean H is a subgroup of $\mathbb{G}$.

Example 6.3. Let $E = \{\dots, -4, -2, 0, 2, 4, \dots\}$. We saw in Example 6.1 that E is a subgroup of $(\mathbb{Z}, +)$. Hence $(E, +)$ is also a group (where now $+$ denotes addition restricted to even integers). This group is isomorphic to $(\mathbb{Z}, +)$ via the isomorphism $\varphi : \mathbb{Z} \to E$ given by $\varphi(n) = 2n$. (Exercise: verify that φ is an isomorphism.)

Example 6.4. Let G be a group and $a \in G$. Recall that $\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$.

Claim: $\langle a \rangle \leq G$.

Proof. Clearly $\langle a \rangle \subseteq G$ and $\langle a \rangle \neq \varnothing$. We check closure under the operation and under inverses.

(1) Given $a^n, a^m \in \langle a \rangle$, we have $a^n \cdot a^m = a^{n+m} \in \langle a \rangle$. ✓
(2) Given $a^n \in \langle a \rangle$, its inverse (in G) is $(a^n)^{-1} = a^{-n}$, which is in $\langle a \rangle$. ✓ □

Definition. If G is a group and $a \in G$, then $\langle a \rangle$ is called the **cyclic subgroup** of G **generated by** a.

Example 6.5. Let E be the subgroup of $(\mathbb{Z}, +)$ given in Example 6.3. Then E is cyclic; in fact, $E = \langle 2 \rangle$, since (using additive notation)

$$\langle 2 \rangle = \{n2 : n \in \mathbb{Z}\} = \{\ldots, -4, -2, 0, 2, 4, \ldots\}.$$

Cyclic subgroups are very important and are the easiest subgroups to find. Note that if G is a group and $a \in G$, then $\langle a \rangle$ is the *smallest* subgroup of G containing a. Furthermore, any subgroup which contains a must also contain $\langle a \rangle$.

Cyclic subgroups are also very easy to characterize *up to isomorphism*, as the next Proposition shows.

Proposition 6.6. *Let G be a group and $a \in G$.*

(1) *If $\circ(a) = \infty$, then $a^i \neq a^j$ for all $i \neq j$ and $\langle a \rangle \cong (\mathbb{Z}, +)$.*
(2) *If $\circ(a) = n$, then $\langle a \rangle = \{a^0, a^1, a^2, \ldots, a^{n-1}\}$ and $\langle a \rangle \cong (\mathbb{Z}_n, +)$.*

Proof sketch. (1) Suppose $\circ(a) = \infty$. Define $\varphi : \mathbb{Z} \to \langle a \rangle$ by $\varphi(k) = a^k$. Clearly φ is surjective. Suppose there exist $i, j \in \mathbb{Z}$ with $i < j$ and $\varphi(i) = \varphi(j)$. Then $a^i = a^j$. Multiplying both side by a^{-i} gives $1 = a^{j-i}$, contradicting the assumption that $\circ(a) = \infty$. This proves that φ is injective. Finally, $\varphi(m+n) = a^{m+n} = a^m \cdot a^n = \varphi(m) \cdot \varphi(n)$ using Lemma 3.2(2), which proves that φ is an isomorphism.

(2) Let $\circ(a) = n$. The proof of Proposition 3.3 shows that $\langle a \rangle = \{a^0, a^1, a^2, \ldots, a^{n-1}\}$ and the elements $a^0, a^1, a^2, \ldots, a^{n-1}$ are distinct. Define $\varphi : \mathbb{Z}_n \to \langle a \rangle$ by $\varphi(k) = a^k$. It follows that φ is a bijection. Lemma 3.2 and the proof of Proposition 3.3 can be used to show that $\varphi(i + j) = \varphi(i) \cdot \varphi(j)$ for all $i, j \in \mathbb{Z}_n$, so φ is an isomorphism. □

As an immediate consequence we get

Corollary 6.7. *If G is a group and $a \in G$, then $\circ(a) = |\langle a \rangle|$. That is, the orders of an element and the cyclic subgroup generated by that element are the same.*

7. Cosets and Lagrance's Theorem

Definition. Suppose G is a group, $H \leq G$, and $a \in G$. The **left coset of H determined by a** is the set

$$aH := \{ah : h \in H\}.$$

E.g., $1H = H$. **Caution**: aH is generally *not* a subgroup of G. (Can you characterize which elements $a \in G$ are such that $aH \leq G$?)

Notation: When using additive notation for G, we write $a + H$ instead of aH.

Example 7.1. Consider the group $G = D_6$ of dihedral symmetries of the triangle. Thus

$$D_6 = \{1, r, r^2\} \cup \{s, sr, sr^2\} \quad \text{where } r^3 = s^2 = 1 \text{ and } rs = sr^2.$$

Let $H = \langle s \rangle = \{1, s\}$, which is a subgroup of G. Here are all of the left cosets of H.

$$1H = \{1\cdot 1, 1\cdot s\} = \{1, s\} \qquad sH = \{s\cdot 1, s\cdot s\} = \{s, 1\}$$
$$rH = \{r\cdot 1, r\cdot s\} = \{r, sr^2\} \qquad (sr)H = \{sr\cdot 1, sr\cdot s\} = \{sr, r^2\}$$
$$r^2H = \{r^2\cdot 1, r^2\cdot s\} = \{r^2, sr\} \qquad (sr^2)H = \{sr^2\cdot 1, sr^2\cdot s\} = \{sr^2, r\}$$

Note that in this example there are just three distinct left cosets of H because $1H = sH$, $rH = (sr^2)H$, and $r^2H = (sr)H$. Furthermore, each left coset has the same number of elements as H, and the left cosets partition G into subsets of equal size.

The observations in the previous example hold generally.

Lemma 7.2. *For all $a \in G, |aH| = |H|$. Hence all left cosets of H have the same size as H.*

Proof. We define a bijection from H to aH in the only reasonable way. Define $f : H \to aH$ by $f(h) = ah$. f is surjective by definition. Suppose $f(h_1) = f(h_2)$. I.e., $ah_1 = ah_2$. Then $h_1 = h_2$ by left cancellation, so f is injective. Thus f is a bijection from H to aH. Hence $|H| = |aH|$. □

Caution: As we saw in the example, it can happen that $aH = bH$ even if $a \neq b$.

Proposition 7.3. *Suppose $H \leq G$. The set of left cosets of H partition G; that is,*

1. $\cup\{aH : a \in G\} = G$
2. *If $aH \neq bH$ then $aH \cap bH = \varnothing$.*

Proof. (1) Every $a \in G$ is an element of aH (since $1 \in H$), so clearly $G \subseteq \bigcup\{aH : a \in G\}$. The other inclusion is obvious.

(2) I'll show you the contrapositive: $aH \cap bH \neq \varnothing$ implies $aH = bH$. Suppose $x \in aH \cap bH$. Thus $x = ah = bh'$ for some $h, h' \in H$. Then $a = xh^{-1} = (bh')h^{-1} = bh_1$ where $h_1 = h'h^{-1}$. Observe that $h \in H$ implies $h^{-1} \in H$, and with $h' \in H$ implies $h_1 = h'h^{-1} \in H$. As $a = bh_1$, this proves $a \in bH$.

Now let ah_2 be an arbitrary element of aH. Then $ah_2 = (bh_1)h2 = bh_3 \in bH$. This proves $aH \subseteq bH$. A symmetric argument proves $bH \subseteq aH$. □

Theorem 7.4 (Lagrange's Theorem)**.** *Suppose G is a finite group and $H \leq G$. Then $|H|$ divides $|G|$.*

Proof. Let $|G| = n$ and $|H| = k$. H has only finitely many distinct left cosets; list them as $H, a_2H, \ldots, a_mH$. They partition G and all have the same size, namely k. Hence $n = mk$. □

Corollary 7.5. *Suppose G is a finite group and $a \in G$. Then $\circ(a)$ divides $|G|$.*

Proof. Recall from Corollary 6.7 that $\circ(a) = |\langle a \rangle|$. Since $\langle a \rangle$ is a subgroup of G (see Example 6.4), we get the desired result by applying Lagrange's Theorem. □

Here are two nice applications.

Corollary 7.6. *If G is a finite group and $|G| = n$, then $x^n = 1$ for all $x \in G$.*

Proof. Given $x \in G$, let $k = \circ(x)$. Then $x^k = 1$. We have $k|n$ by the Corollary 7.5, say $n = km$. Then $x^n = x^{km} = (x^k)^m = 1^m = 1$. □

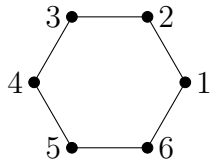
Corollary 7.7. *If G is a finite group and $|G| = p$ is prime, then G is cyclic.*

Proof. Pick any $a \in G$ satisfying $a \neq 1$. Then $\circ(a)|p$ by Corollary 7.5, so $\circ(a) = 1$ or p. If $\circ(a) = 1$ then $a^1 = 1$, contradicting $a \neq 1$. So $\circ(a) = p$. Hence $|\langle a \rangle| = p$. But $\langle a \rangle \subseteq G$ and $|G| = p$, which forces $\langle a \rangle = G$. So G is cyclic. □

Note: the previous proof shows that if $|G|$ is prime then *every* non-identity element of G is a generator.

8. Cosets (continued), Normal subgroups

Consider the dihedral group D_{12} of symmetries of the regular hexagon C_6.



Also recall that $D_{12} = \{r^i : 0 \leq i \leq 6\} \cup \{sr^i : 0 \leq i \leq 6\}$ where

- r = rotation ccw by $\pi/3$ radians = (1 2 3 4 5 6).
- s = reflection through the x-axis = (2 6)(3 5).
- $r^6 = s^2 = 1$ and $rs = sr^{-1}$.

What are some subgroups of D_{12}? For starters, we know that $|D_{12}| = 12$, so by Lagrange's theorem, a subgroup can only have order 1, 2, 3, 4, 6 or 12.

Looking at some cyclic subgroups, we find

$$\begin{aligned}
\langle 1 \rangle &= \{1\} \\
\langle r \rangle &= \{1, r, r^2, r^3, r^4, r^5\} \\
\langle s \rangle &= \{1, s\} \\
\langle sr \rangle &= \{1, sr\}, \quad \text{etc. for any reflection}
\end{aligned}$$

Can we find a subgroup of order 3? (Yes: $\langle r^2 \rangle$.)
Can we find a subgroup of order 4? (Yes: $\langle r^3, s \rangle$. This subgroup is not cyclic.)

Each subgroup has left cosets. For example:

- The left cosets of $\langle r \rangle$ are $\langle r \rangle = \{1, r, r^2, r^3, r^4, r^5\}$ and $s\langle r \rangle = \{s, sr, sr^2, sr^3, sr^4, sr^5\}$.
- Let $H = \langle s \rangle$. $|H| = 2$, so there are 6 left cosets of H. They are:

$$\begin{aligned}
H &= \{1, s\} \\
rH &= \{r, rs\} = \{r, sr^5\}, \\
r^2H &= \{r^2, r^2s\} = \{r^2, sr^4\}, \\
r^3H &= \{r^3, r^3s\} = \{r^3, sr^3\}, \\
r^4H &= \{r^4, r^4s\} = \{r^4, sr^2\}, \\
r^5H &= \{r^5, r^5s\} = \{r^5, sr\}.
\end{aligned}$$

Subgroups also have *right* cosets. For example, the right cosets of $H = \langle s \rangle$ are

$$\begin{aligned} H &= \{1, s\} \\ Hr &= \{r, sr\}, \\ Hr^2 &= \{r^2, sr^2\}, \\ Hr^3 &= \{r^3, sr^3\}, \\ Hr^4 &= \{r^4, sr^4\}, \\ Hr^5 &= \{r^5, sr^5\}. \end{aligned}$$

Note that H has the same **number** of right and left cosets, but they aren't the same sets. This is true in general: whenever H is a subgroup of a group G, there is a bijection between the collection of left cosets of H and the collection of right cosets of H. (Can you find a proof of this?) This justifies the next definition.

Definition. If G is a group and $H \leq G$, the **index** of H in G, denoted $[G : H]$, is the number of distinct left (or right) cosets of H.

Of course, if G is finite than $[G : H] = \dfrac{|G|}{|H|}$.

Definition. Suppose $H \leq G$. We say that H is **normal**, or is a **normal subgroup**, and write $H \lhd G$, if $aH = Ha$ for all $a \in G$.

Of course if G is a abelian then every subgroup is normal. In the example above, $\langle r \rangle \lhd D_{12}$ but $\langle s \rangle \not\lhd D_{12}$. In general, it can be tedious to determine whether or not a subgroup of a group is normal.

Notation. Generalizing the notation used for cosets: if A, B are nonempty subsets of a group G and $g \in G$ then

$$\begin{aligned} gA &:= \{ga \,:\, a \in A\} \\ Ag &:= \{ag \,:\, a \in A\} \\ AB &:= \{ab \,:\, a \in A \text{ and } b \in B\} \\ A^{-1} &:= \{a^{-1} \,:\, a \in A\}. \end{aligned}$$

This notation allows us to "multiply" and "invert" nonempty sets as well as elements of G. It can be shown that this multiplication is associative, so for example $(Ag)B = A(gB)$, and so we can just write AgB. The following law for inverses also holds: $(AB)^{-1} = B^{-1}A^{-1}$ and $(gA)^{-1} = A^{-1}g^{-1}$ (exercise). Note however that you can't use the cancellation laws in this context. For example, for any $a, b \in G$ it is true that $aG = bG$, but this does not imply $a = b$. Similarly, it is not true that $AA^{-1} = 1$ (or $\{1\}$). So inverses of sets are not true inverses.

This notation is particularly useful for shortening the definition of a being a subgroup. Using this notation, if $H \subseteq G$ then H is a subgroup of G iff $H \neq \varnothing$, $HH \subseteq H$, and $H^{-1} \subseteq H$. (In fact, if H is a subgroup then $HH = H^{-1} = H$; exercise.)

9. Applications of normality

The following is a useful characterization of when a subgroup is normal.

Proposition 9.1. *Suppose $H \leq G$. TFAE:*

(1) $H \lhd G$
(2) $aHa^{-1} = H$ *for all* $a \in G$
(3) $aHa^{-1} \subseteq H$ *for all* $a \in G$.
(4) *If* $h \in H$, *then* $aha^{-1} \in H$ *for all* $a \in G$.

Proof. (2) $\Rightarrow$ (3) $\Leftrightarrow$ (4) is obvious. It remains to prove (3) $\Rightarrow$ (2) $\Leftrightarrow$ (1). We first show (1) $\Leftrightarrow$ (2). Fix $a \in G$. If $aH = Ha$, then multiplying this equation on the right by a^{-1} gives $aHa^{-1} = Haa^{-1} = H1 = H$. Conversely, if $aHa^{-1} = H$, then multiplying this equation on the right by a gives $aHa^{-1}a = Ha$, which simplifies to $aH = Ha$. Thus $aH = Ha$ for all $a \in G$ (i.e., $H \lhd G$) iff $aHa^{-1} = H$ for all $a \in G$.

Next we prove (3) $\Rightarrow$ (2). Assume (3) and fix $a \in G$. Then applying (3) we get

$$(*) \qquad aHa^{-1} \subseteq H.$$

Next let $b = a^{-1}$; then another application of (3) gives $bHb^{-1} \subseteq H$, i.e., $a^{-1}Ha \subseteq H$. Multiply this last fact on the left by a and on right by a^{-1} to get

$$(**) \qquad H \subseteq aHa^{-1}.$$

The inclusions $(*)$ and $(**)$ give $aHa^{-1} = H$, and since a was arbitrary we have proved (2). $\square$

The proof of the next lemma uses a nice trick.

Lemma 9.2. *Suppose $H, K \lhd G$ and $H \cap K = \{1\}$. Then $hk = kh$ for all $h \in H$ and $k \in K$.*

Proof. We use the following trick. Given $a, b \in G$, their **commutator** is $[a, b] = a^{-1}b^{-1}ab$. It is easy to show that $ab = ba$ iff $[a, b] = 1$ (exercise). So now let $h \in H$ and $k \in K$ and consider $[h, k] = h^{-1}k^{-1}hk$. We can write

$$[h, k] = h^{-1}(k^{-1}hk).$$

Since $h \in H \lhd G$ and $k^{-1} \in G$ we get $k^{-1}hk \in H$, say $k^{-1}hk = h_1$. Then

$$[h, k] = h^{-1}h_1 \in H.$$

Similarly,

$$[h, k] = \underbrace{(h^{-1}k^{-1}h)}_{\in K} k \in K.$$

Hence $[h, k] \in H \cap K = \{1\}$, proving $[h, k] = 1$, so $hk = kh$. $\square$

If H, K are two subgroups of G, then $H \subseteq HK$ (because $1 \in K$) and $K \subseteq HK$ (because $1 \in H$), but HK does not need to be a subgroup. For example, in D_{12} let

$H = \langle s \rangle = \{1, s\}$ and $K = \langle sr \rangle = \{1, sr\}$. Then

$$\begin{aligned} HK &= \{1, s\}\{1, sr\} \\ &= \{1(1), 1(sr), s(1), s(sr)\} \\ &= \{1, sr, s, r\} \end{aligned}$$

This isn't a subgroup because, for example, r and s are HK but $rs \notin HK$.

The next Proposition shows that the failure in the previous example is due to the fact that neither H nor K is normal.

Proposition 9.3. *Suppose G is a group and $H, K \leq G$. If either $H \lhd G$ or $K \lhd G$, then $HK \leq G$.*

Proof. Assume for simplicity that $H \lhd G$. Thus $Hg = gH$ for any $g \in G$. Hence

$$(*) \qquad HK = \bigcup_{k \in K} Hk = \bigcup_{k \in K} kH = KH.$$

Now I'll use $(*)$ to prove $HK \leq G$. Certainly $HK \subseteq G$ and $HK \neq \varnothing$. To prove that HK is a subgroup, it remains to prove $(HK)(HK) \subseteq HK$ and $(HK)^{-1} \subseteq HK$.

- Using associativity, the fact that H and K are subgroups, and $(*)$,

  $$(HK)(HK) = H(KH)K \overset{(*)}{=} H(HK)K = (HH)(KK) = HK.$$

  Hence HK is closed under multiplication.
- Using the law of inverses, the fact that H and K are subgroups, and $(*)$,

  $$(HK)^{-1} = K^{-1}H^{-1} = KH \overset{(*)}{=} HK.$$

  Hence HK is closed under inverses. □

Before leaving this section, we show one way in which the previous result can be strengthened.

Definition. Suppose G is a group and $H \leq G$. The **normalizer** of H, denoted $N_G(H)$, is the set

$$N_G(H) = \{a \in G : aH = Ha\}.$$

Normalizers are useful in many contexts. For now, I simply point out that

(i) $N_G(H) \leq G$.
(ii) $H \lhd G$ iff $N_G(H) = G$.

(It is a good exercise to prove both of these claims.) What I want to point out is that the proof of the previous Proposition didn't need the full strength of the hypothesis $H \lhd G$, i.e., $N_G(H) = G$; it simply needed $Hk = kH$ to hold for all $k \in K$, which is equivalent to $K \subseteq N_G(H)$. Hence:

Corollary 9.4. *Suppose G is a group and $H, K \leq G$. If $K \subseteq N_G(H)$ (or $H \subseteq N_G(K)$), then $HK \leq G$.*

10. Direct products

Let $(G_1, \star)$ and $(G_2, \diamond)$ be groups. Their *direct product* is $(G_1 \times G_2, *)$ where

$$(a_1, a_2) * (b_1, b_2) = (a_1 \star b_1, a_2 \diamond b_2).$$

Fact: If G_1, G_2 are groups, then $G_1 \times G_2$ is also a group.

Proof sketch. We must show that the set $G_1 \times G_2$ is nonempty (it is), that $*$ is a binary operation on $G_1 \times G_2$ (it is), and that $*$ is associative, has an identity element, and every element of $G_1 \times G_2$ has an inverse element. Let's check existence of inverses. (The identity element is $\mathbf{1} = (1_1, 1_2)$ where 1_i is the identity element of G_i.) For any $\mathbf{a} = (a_1, a_2) \in G_1 \times G_2$, I claim that $\mathbf{a}^{-1} := (a_1^{-1}, a_2^{-1})$ is an inverse to $\mathbf{a}$.

$$\mathbf{a} * \mathbf{a}^{-1} = (a_1, a_2) * (a_1^{-1}, a_2^{-1}) \stackrel{df}{=} (a_1 \star a_1, a_2 \diamond a_2^{-1}) = (1_1, 1_2) = \mathbf{1}.$$

A similar proof shows $\mathbf{a}^{-1} * \mathbf{a} = \mathbf{1}$, so we're good. □

Notation.

(1) If both $\star$ and $\diamond$ are written as $+$, then we may also write $*$ as $+$.
(2) Products of more factors are defined analogously. $G^n = \underbrace{G \times G \times ... \times G}_{n}$.

Consider $(\mathbb{Z}_2, +)^2$. It has 4 elements: $(0,0), (0,1), (1,0), (1,1)$. Its table:

+	(0,0)	(1,0)	(0,1)	(1,1)
(0,0)	(0,0)	(1,0)	(0,1)	(1,1)
(1,0)	(1,0)	(0,0)	(1,1)	(0,1)
(0,1)	(0,1)	(1,1)	(0,0)	(1,0)
(1,1)	(1,1)	(0,1)	(1,0)	(0,0)

If we rename its elements $1, b, c, d$ a rename the operation $\cdot$, we get the table

$\cdot$	1	b	c	d
1	1	b	c	d
b	b	1	d	c
c	c	d	1	b
d	d	c	b	1

We recognize this; it is the table for $\mathbb{Z}_8^\times$. Hence we have proved $\mathbb{Z}_8^\times \cong (\mathbb{Z}_2, +)^2$. We have **factored** $\mathbb{Z}_8^\times$.

The next Theorem gives a general criterion for discovering factorizations.

Theorem 10.1. *Let G be a group. Suppose there exist $H, K \lhd G$ satisfying*

(1) $H \cap K = \{1\}$;
(2) $HK = G$.

Then $G \cong H \times K$.

Proof. Define a function $\varphi : H \times K \to G$ by $\varphi((h,k)) = hk$. Let's prove that φ is an isomorphism. First check that it is a bijection. It is surjective because $HK = G$. We'll prove that it's injective using $H \cap K = \{1\}$. Indeed, suppose

$\varphi((h_1, k_1)) = \varphi((h_2, k_2))$, i.e., $h_1 k_1 = h_2 k_2$. Multiply on left by h_2^{-1} and on right by k_1^{-1} to get $h_2^{-1} h_1 = k_2 k_1^{-1}$. The left side is in H while the right side is in K, so both sides are in $H \cap K = \{1\}$, proving $h_2^{-1} h_1 = 1 = k_2 k_1^{-1}$. These equations imply $h_1 = h_2$ and $k_1 = k_2$, proving φ is injective.

Finally we must prove that φ preserves the group operations. Let $*$ denote the group operation of $H \times K$, and for emphasis let $\cdot$ denote the operation of G. Then given two elements $(h_1, k_1), (h_2, k_2) \in H \times K$,

$$\begin{aligned}
\varphi\Big((h_1, k_1) * (h_2, k_2)\Big) &= \varphi\Big((h_1 h_2, k_1 k_2)\Big) && \text{(definition of } * \text{ in } H \times K) \\
&= (h_1 h_2)(k_1 k_2) && \text{(definition of } \varphi) \\
&= h_1 (h_2 k_1) k_2 \\
&= h_1 (k_1 h_2) k_2 && \text{by Lemma 9.2} \\
&= (h_1 k_1)(h_2 k_2) \\
&= \varphi((h_1, k_1)) \cdot \varphi((h_2, k_2)).
\end{aligned}$$

□

Example 10.2. Let $G = (\mathbb{Z}_6, +)$. Let $H = \langle 2 \rangle = \{0, 2, 4\}$ and $K = \langle 3 \rangle = \{0, 3\}$. Clearly

- $H, K \leq \mathbb{Z}_6$. (Cyclic subgroups are subgroups)
- $H, K \lhd \mathbb{Z}_6$. (Because $\mathbb{Z}_6$ is abelian)
- $H \cap K = \{0\}$
- $H + K = \{h + k : h \in \{0, 2, 4\} \text{ and } k \in \{0, 3\}\} = \mathbb{Z}_6$.

Hence by the Theorem, $(\mathbb{Z}_6, +) \cong H \times K$.

In the previous example, we can also apply Proposition 6.6 to the cyclic subgroups H, K to get $H \cong (\mathbb{Z}_3, +)$ and $K \cong (\mathbb{Z}_2, +)$. Hence $(\mathbb{Z}_6, +) \cong (\mathbb{Z}_3, +) \times (\mathbb{Z}_2, +)$.

A similar argument shows:

Corollary 10.3. $(\mathbb{Z}_{mn}, +) \cong (\mathbb{Z}_m, +) \times (\mathbb{Z}_n, +)$ *provided* $\gcd(m, n) = 1$.

Proof. Exercise. □

11. Homomorphisms

Definition. Let $G = (G, \star)$ and $H = (H, \diamond)$ be groups. A function $\varphi : G \to H$ is a **homomorphism** if

$$\varphi(x \star y) = \varphi(x) \diamond \varphi(y) \qquad \text{for all } x, y \in G.$$

Example 11.1.

(1) Any isomorphism is a homomorphism.
(2) The parity function $\text{par} : \mathbb{Z} \to \{0, 1\}$ given by

$$\text{par}(n) = \begin{cases} 0 & \text{if } n \text{ is even} \\ 1 & \text{if } n \text{ is odd} \end{cases}$$

is a homomorphism from $(\mathbb{Z}, +)$ to $(\mathbb{Z}_2, +)$, because $\text{par}(x+y)$, i.e., the parity of $x + y$, is the mod-2 sum of $\text{par}(x)$ and $\text{par}(y)$.
(3) More generally, the function $\mathbb{Z} \to \mathbb{Z}_n$ given by $x \mapsto (x \pmod n)$ is a homomorphism from $(\mathbb{Z}, +)$ to $(\mathbb{Z}_n, +)$.
(4) Let $G = (\mathbb{C}^\times, \cdot)$ and $H = (\mathbb{R}^\times, \cdot)$. The function $\varphi : \mathbb{C}^\times \to \mathbb{R}^\times$ given by $\varphi(z) = |z|$ is a homomorphism, because $\varphi(zw) = |zw| = |z||w| = \varphi(z)\varphi(w)$.

Definition. Let $\varphi : G \to H$ be a homomorphism.

(1) $\text{im}(\varphi)$ denotes the **image** (or **range**) of φ. That is, $\text{im}(\varphi) = \{\varphi(x) : x \in G\}$.
(2) The **kernel** of φ is the set

$$\{x \in G : \varphi(x) = 1\}.$$

It is denoted $\ker \varphi$.

Proposition 11.2. *Let $\varphi : G \to H$ be a homomorphism.*

(1) $\varphi(1_G) = 1_H$.
(2) $\varphi(g^{-1}) = \varphi(g)^{-1}$ *for all* $g \in G$.
(3) *More generally,* $\varphi(g^n) = \varphi(g)^n$ *for all* $n \in \mathbb{Z}$.
(4) $\ker \varphi \leq G$ *and* $\text{im}(\varphi) \leq H$.

Proof.

(1) Pick $g \in G$. We have $\varphi(1_G)\varphi(g) = \varphi(1_G \cdot g) = \varphi(g) = 1_H \cdot \varphi(g)$. Right cancellation in H gives $\varphi(1_G) = 1_H$.
(2) Let $h = \varphi(g)$. Then $h \cdot \varphi(g^{-1}) = \varphi(g)\varphi(g^{-1}) = \varphi(gg^{-1}) = \varphi(1_G) = 1_H = hh^{-1}$. Left cancellation gives $\varphi(g^{-1}) = h^{-1} = \varphi(g)^{-1}$.
(3) Exercise.
(4) Clearly $\ker\varphi \subseteq G$ and $\text{im}(\varphi) \subseteq H$. Since $\varphi(1_G) = 1_H$ by (1) we have $1_G \in \ker\varphi$ and $1_H \in \text{im}(\varphi)$, so $\ker\varphi, \text{im}(\varphi) \neq \varnothing$. Remains to check closure under products and inverses.

First $\ker \varphi$:

- Suppose $a, b \in \ker \varphi$, meaning $\varphi(a) = \varphi(b) = 1_H$. Then $\varphi(ab) = \varphi(a)\varphi(b) = 1_H \cdot 1_H = 1_H$, proving $ab \in \ker \varphi$.

- Suppose $a \in \ker\varphi$, meaning $\varphi(a) = 1_H$. Then $\varphi(a^{-1}) = \varphi(a)^{-1}$ (by (2)) $= (1_H)^{-1} = 1_H$, proving $a^{-1} \in \ker\varphi$.

Next $\mathrm{im}(\varphi)$:

- Suppose $x, y \in \mathrm{im}(\varphi)$. Write $x = \varphi(a)$ and $y = \varphi(b)$ with $a, b \in G$. Then $xy = \varphi(a)\varphi(b) = \varphi(ab)$. As $ab \in G$, this proves $xy \in \mathrm{im}(\varphi)$.
- Suppose $x \in \mathrm{im}(\varphi)$, say $x = \varphi(a)$ where $a \in G$. Then $x^{-1} = \varphi(a)^{-1} = \varphi(a^{-1})$ by (2). Since $a^{-1} \in G$, this proves $x^{-1} \in \mathrm{im}(\varphi)$. □

More is true:

Proposition 11.3. *Let $\varphi : G \to H$ be a homomorphism. Then $\ker\varphi \lhd G$.*

Proof. It suffices by Proposition 9.1($1 \Leftrightarrow 4$) to show $g \in \ker\varphi$ implies $aga^{-1} \in \ker\varphi$ for all $a \in G$. So suppose $g \in \ker\varphi$ and $a \in G$. To show $aga^{-1} \in \ker\varphi$, we evaluate it under φ:

$$\begin{aligned}\varphi(aga^{-1}) &= \varphi(a)\varphi(ga^{-1}) = \varphi(a)\varphi(g)\varphi(a^{-1}) = \varphi(a)\cdot 1_H \cdot \varphi(a^{-1}) \quad (\text{because } g \in \ker\varphi)\\ &= \varphi(a)\cdot\varphi(a^{-1}) = \varphi(a\cdot a^{-1}) = \varphi(1_G) = 1_H.\end{aligned}$$

Hence $aga^{-1} \in \ker\varphi$. □

12. Quotient Groups

Definition. Suppose G is a group and $H \leq G$. Then G/H denotes the set of all *left* cosets of H.

Examples.

(1) If $G = (\mathbb{Z}, +)$ and $H = \langle 5 \rangle = 5\mathbb{Z}$, then
$$G/H = \mathbb{Z}/5\mathbb{Z} = \{5\mathbb{Z},\ 1{+}5\mathbb{Z},\ 2{+}5\mathbb{Z},\ 3{+}5\mathbb{Z},\ 4{+}5\mathbb{Z}\}.$$
(2) If $G = (\mathbb{C}^\times, \cdot)$ and $H = S = \{z : |z| = 1\}$, then $G/H = \mathbb{C}^\times/S = \{$all circles centred at $0\}$.

In general, we want to define an operation $\cdot$ on G/H. That is, given two left cosets C, D of H, we want to define another left coset $C \cdot D$. A natural choice is to define
$$C \cdot D \stackrel{\text{df}}{=} CD = \{cd : c \in C, d \in D\},$$
or equivalently, $(aH) \cdot (bH) = (aH)(bH)$. There is a problem: $(aH)(bH)$ might not be a left coset of H. However there is no problem when H is normal.

Proposition 12.1. *If $N \lhd G$, then $(aN)(bN) = (ab)N \in G/N$ for all $a, b, \in G$.*

Proof. $(aN)(bN) = a(Nb)N = a(bN)N$ (by normality) $= (ab)NN = (ab)N$, which is a left coset of N. □

Definition. If $N \lhd G$, then $\cdot$ is defined on G/N by $(aN) \cdot (bN) \stackrel{\text{df}}{=} (aN)(bN) = (ab)N$.

Notation. If the operation of G is $+$, then we write $+$ instead of $\cdot$ for the operation on G/N as well. In this case the definition is $(a + N) + (b + N) \stackrel{\text{df}}{=} (a + b) + N$.

Example 12.2. In $\mathbb{C}^\times/S$, let $C = \{z : |z| = r\}$ and $D = \{z : |z| = s\}$. What is $C \cdot D$?

Solution. Then $C = rS$ and $D = sS$, so
$$\begin{aligned} C \cdot D &= (rS)(sS) \\ &= \{(re^{i\theta})(se^{i\varphi}) : \theta, \varphi \in \mathbb{R}\} \\ &= \{rse^{i(\theta+\varphi)}) : \theta, \varphi \in \mathbb{R}\} \\ &= \{rse^{i(\psi)} : \psi \in \mathbb{R}\} \\ &= (rs)S. \end{aligned}$$

Example 12.3. Let $G = (\mathbb{Z}_5, +)$ and $N = 5\mathbb{Z}$. If $C = 3 + 5\mathbb{Z}$ and $D = 4 + 5\mathbb{Z}$, what is $C + D$?

Solution. $(3 + 5\mathbb{Z}) + (4 + 5\mathbb{Z}) = (3 + 4) + 5\mathbb{Z} = 7 + 5\mathbb{Z} = 2 + 5\mathbb{Z}$.

Proposition 12.4. *Suppose $N \lhd G$. Then $(G/N, \cdot)$ is a group.*

Proof. We've already seen that $\cdot$ is an operation on G/N. What remains is to prove that $\cdot$ is associative, has a 2-sided identity element, and every left coset of N has a 2-sided inverse (with respect to $\cdot$).

Associativity: For all $aN, bN, cN \in G/N$,

$$\begin{aligned} aN \cdot (bN \cdot cN) &= aN \cdot (bc)N \\ &= a(bc)N \\ &= (ab)cN \\ &= (ab)N \cdot cN \\ &= (aN \cdot bN) \cdot cN. \end{aligned}$$

Identity: Obviously $N = 1N \in G/N$. We will show that N is an identity element with respect to $\cdot$. For any $aN \in G/N$,

$$aN \cdot N = aN \cdot 1N = (a1)N = aN.$$

Similarly, $N \cdot aN = aN$.

Inverses: For any $aN \in G/N$, of course we have $a^{-1}N \in G/N$. We will show that $a^{-1}N$ is an inverse to aN.

$$\begin{aligned} aN \cdot a^{-1}N &= (aa^{-1})N \\ &= 1N \\ &= N \end{aligned}$$

and similarly $a^{-1}N \cdot aN = N$. □

Definition. Suppose $N \lhd G$. The group $(G/N, \cdot)$ is called the **quotient group of** G **by** N (or of G **modulo** N).

Example 12.5.

(1) $\mathbb{Z}/5\mathbb{Z}$. Though complicated (its elements are the 5 cosets of $5\mathbb{Z}$), this quotient group is easily seen to be isomorphic to $\mathbb{Z}_5$. The isomorphism $\mathbb{Z}_5 \to \mathbb{Z}/5\mathbb{Z}$ sends $a \mapsto a + 5\mathbb{Z}$. (In fact, many textbooks define $\mathbb{Z}_5$ to *be* $\mathbb{Z}/5\mathbb{Z}$.)

(2) More generally, $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

(3) $\mathbb{C}^\times/S$. One can show that this quotient group is isomorphic to $(\mathbb{R}^{>0}, \cdot)$ in the obvious way.

(4) Let N be the subgroup of D_{12} given by $N = \langle r^3 \rangle = \{1, r^3\}$. One can check (by tedious calculations) that $N \lhd D_{12}$. Hence we can form the quotient group D_{12}/N. Its elements are the left cosets of N in D_{12}. What is D_{12}/N isomorphic to?

13. 1st Isomorphism Theorem

Definition. Suppose $N \lhd G$. Define $\pi_N : G \to G/N$ by $\pi_N(g) = gN$.

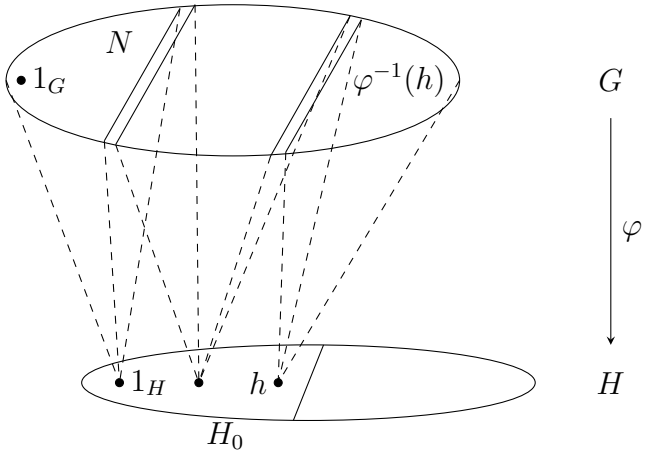
π_N is called the "mod N projection map."

Lemma 13.1. *If $N \lhd G$, then $\pi_N : G \to G/N$ is a homomorphism and* $\ker \pi_N = N$.

Proof. $\pi_N(ab) = (ab)N = (aN)(bN) = \pi_N(a)\pi_n(b)$, proving π_N is a homomorphism. $\ker \pi_N = \{g \in G : \pi_N(g) = 1_{G/N}\} = \{g \in G : gN = N\} = N$ (exercise). □

Consider now an arbitrary homomorphism $\varphi : G \to H$. In general we can't assume that φ is injective or surjective. Let $N = \ker \varphi$ and $H_0 = \mathrm{im}(\varphi)$ and recall that $N \lhd G$ and $H_0 \leq H$.

For each $h \in H_0$, the preimage $\varphi^{-1}(h) := \{g \in G : \varphi(g) = h\}$ is called the **fiber** of φ above h. Note that the fiber above 1_H is $\ker \varphi = N$.



Proposition 13.2. *Suppose $\varphi : G \to H$ is a homomorphism and $N = \ker \varphi$. The fibers of φ are precisely the left (= right) cosets of N.*

Proof. Let $h \in \mathrm{im}(\varphi)$ and choose $a \in \varphi^{-1}(h)$. I will show that $\varphi^{-1}(h) = aN$.

$\boxed{\varphi^{-1}(h) \subseteq aN.}$ Let $b \in \varphi^{-1}(h)$. Then

$$\varphi(a^{-1}b) = \varphi(a^{-1})\varphi(b) = \varphi(a)^{-1}\varphi(b) = h^{-1}h = 1_H.$$

Hence $a^{-1}b \in N$. So $b = a(a^{-1}b) \in aN$.

$\boxed{aN \subseteq \varphi^{-1}(h).}$ Let $x \in aN$, so $x = an$ for some $n \in N$. Then

$$\varphi(x) = \varphi(an) = \varphi(a)\varphi(n) = h \cdot 1_H = h$$

so $x \in \varphi^{-1}(h)$. □

Observe that φ is injective iff each of its fibers consists of just one element. By Proposition 13.2 (and Lemma 7.2), this holds iff $|N| = 1$. This proves:

Corollary 13.3. *A homomorphism $\varphi : G \to H$ is injective iff* $\ker \varphi = \{1_G\}$.

We are ready for our second important theorem (the first was Lagrange's theorem).

Theorem 13.4 (1st Isomorphism Theorem)**.** *Suppose $\varphi : G \to H$ is a surjective homomorphism. Then $G/\ker\varphi \cong H$.*

Proof. Let $N = \ker\varphi$. Define $\overline{\varphi} : G/N \to H$ by the rule $\overline{\varphi}(aN) = \varphi(a)$. $\overline{\varphi}$ will be our isomorphism. We must first check that this is well-defined: i.e., if $aN = bN$ do we have $\varphi(a) = \varphi(b)$? Yes: if $aN = bN$, then a, b belong to the same coset of N, so they belong to the same fiber of φ by Proposition 13.2, meaning $\varphi(a) = \varphi(b)$.

Next we check that $\overline{\varphi}$ is a homomorphism. The question is whether, for any $aN, bN \in G/N$, we have

$$\overline{\varphi}(aN \cdot bN) \stackrel{?}{=} \overline{\varphi}(aN)\overline{\varphi}(bN).$$

Well, $\overline{\varphi}(aN \cdot bN) = \overline{\varphi}((ab)N) = \varphi(ab) = \varphi(a)\varphi(b) = \overline{\varphi}(aN)\overline{\varphi}(bN)$. So $\overline{\varphi}$ is a homomorphism.

Clearly $\overline{\varphi}$ is surjective (because φ is). It remains only to check that $\overline{\varphi}$ is injective, or equivalently by Corollary 13.3, that $\ker\overline{\varphi} = \{N\}$. Suppose $aN \in G/N$. Then

$$aN \in \ker\overline{\varphi} \iff \overline{\varphi}(aN) = 1_H \iff \phi(a) = 1_H \iff a \in N \iff aN = N.$$

Hence $\ker\overline{\varphi} = \{N\} = \{1_{G/N}\}$, proving $\overline{\varphi}$ is injective. In summary $\overline{\varphi} : G/N \cong H$. □

Example 13.5.

(1) Define $\varphi : \mathbb{C}^\times \to \mathbb{R}^{>0}$ by $\varphi(z) = |z|$. We've already seen that this is a homomorphism, and it is easy to see that it is surjective. Thus by the 1st Isomorphism Theorem, $\mathbb{C}^\times/\ker\varphi \cong \mathbb{R}^{>0}$. What is $\ker\varphi$? Clearly $\ker\varphi = \{z \in \mathbb{C}^\times : |z| = 1\} = S$, the unit circle. Thus $\mathbb{C}^\times/S \cong \mathbb{R}^{>0}$.

(2) Recall that $D_{12} = \{r^i : 0 \le i < 6\} \cup \{sr^i : 0 \le i < 6\}$ where r is a counter-clockwise rotation by $60°$ and s is the reflection through the x-axis. Let's write $D_6 = \{t^i : 0 \le i < 3\} \cup \{st^i : 0 \le i < 3\}$ where t is the counter-clockwise rotation by $120°$. Then clearly $t = r^2$, so $D_6 = \{1, r^2, r^4\} \cup \{s, sr^2, sr^4\}$.

Now define a function $\varphi : D_{12} \to D_6$ by $\varphi(r^i) = r^{2i}$ and $\varphi(sr^i) = sr^{2i}$. One can check (by a tedious consideration of cases) that $\varphi(xy) = \varphi(x)\varphi(y)$ for all $x, y \in D_{12}$; hence φ is a homomorphism. Clearly φ is surjective, and it's easy to calculate that $\ker\varphi = \{1, r^3\}$.

It follows by the 1st Isomorphism Theorem that $D_{12}/\{1, r^3\} \cong D_6$.

14. 2nd and 3rd Isomorphism Theorems

In the proof of the 1st Isomorphism Theorem, recall that $\overline{\varphi}$ satisfied (in fact was defined by)

$$\overline{\varphi}(aN) = \varphi(a) \qquad \text{for all } a \in G.$$

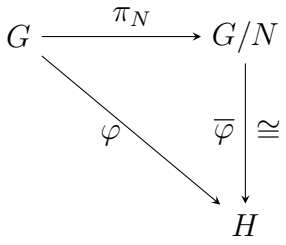
This can be restated as

$$\overline{\varphi}(\pi_N(a)) = \varphi(a) \qquad \text{for all } a \in G$$

which is equivalent to

$$\overline{\varphi} \circ \pi_N = \varphi.$$

We say that φ **factors through** π_N via $\overline{\varphi}$. Pictorially,



Applications

(1) Given any group, we can define $\varphi : G \to G$ by $\varphi(x) = x$. It is easy to see that φ is a surjective homomorphism and $\ker\varphi = \{1\}$. Hence by the 1st Isomorphism Theorem,

$$G/\{1\} \cong G.$$

(2) Suppose we have a group G, a normal subgroup $N \lhd G$, and another subgroup $H \leq G$. We can form G/N. Define a function $\varphi : H \to G/N$ by $\varphi(a) = aN$. It is easy to check that φ is a homomorphism: $a, b \in H$ implies $\varphi(ab) = (ab)N = (aN)(bN) = \varphi(a)\varphi(b)$. But φ need not be onto.

What is $\mathrm{im}(\varphi)$? As a ranges over H, aN ranges over the left cosets of N in HN. Hence $\mathrm{im}(\varphi) = HN/N$.

We know from Proposition 9.3 that $HN \leq G$ (because $N \lhd G$), so HN is a group. Clearly $N \leq HN$. Now

$$\begin{aligned} N \lhd G &\iff gNg^{-1} = N \text{ for all } g \in G \\ &\implies gNg^{-1} = N \text{ for all } g \in HN \\ &\iff N \lhd HN. \end{aligned}$$

Thus $N \lhd HN$, so HN/N is in fact a group. Thus φ is a **surjective** homomorphism from H to HN/N.

By the 1st Isomorphism Theorem, $HN/N \cong H/\ker\varphi$. So we calculate $\ker\varphi$:

$$\ker\varphi = \{h \in H : hN = N\} = \{h \in H : h \in N\} = H \cap N.$$

Hence $HN/N \cong H/(H \cap N)$. This proves:

Theorem 14.1 (2nd Isomorphism Theorem)**.** *Suppose G is a group and $H, N \leq G$ with $N \lhd G$. Then $HN/N \cong H/(H \cap N)$.*

(3) Now suppose G is a group and we have two normal subgroups $N, K \lhd G$ with $N \leq K$. We can form G/N and G/K. Define $\varphi : G/N \to G/K$ by $\varphi(aN) = aK$. We have to check that this is well-defined: if $aN = bN$, then $N = a^{-1}bN$, so $a^{-1}b \in N$. This implies $a^{-1}b \in K$, so $a^{-1}bK = K$, so $bK = aK$. This proves φ is well-defined.

Obviously φ is surjective.

We check that φ is a homomorphism: for all $aN, bN \in G/N$,

$$\varphi((aN) \cdot (bN)) = \varphi((ab)N) = (ab)K = (aK)(bK) = \varphi(aN)\varphi(bN).$$

Thus φ is a surjective homomorphism from G/N to G/K. Hence by the 1st Isomorphism Theorem, $G/K \cong (G/N)/\ker\varphi$. What is $\ker\varphi$? Calculate:

$$\ker\varphi = \{aN \in G/N : aK = K\} = \{aN : a \in K\} = K/N.$$

This proves:

Theorem 14.2 (3rd Isomorphism Theorem)**.** *Suppose G is a group and $N, K \lhd G$ with $N \leq K$. Then $K/N \lhd G/N$ and $(G/N)/(K/N) \cong G/K$.*

(4) Suppose G is a group and $N, K \lhd G$ satisfy $NK = G$ and $N \cap K = \{1\}$. Recall that Theorem 10.1 implies in this situation that $G \cong N \times K$. What can we say about G/N and G/K?

By the 2nd Isomorphism Theorem, $NK/K \cong N/(N \cap K)$. Since $NK = G$ and $N \cap K = \{1\}$, this gives $G/N \cong K/\{1\} \cong K$. By symmetry, $G/K \cong N$.

15. Group actions

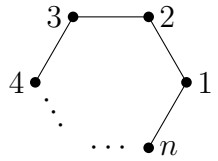
Definition. Let G be agroup and X a set. An **action of G on X** is a map $g \mapsto \pi_g$ which assigns to each $g \in G$ a permutation $\pi_g \in S_X$, and which "respects the operation of G," in the sense that if $g, h \in G$ then $\pi_{gh} = \pi_g \circ \pi_h$.

In other words, an action of G on X is a homomorphism $\pi : G \to S_X$.

Example 15.1.

(1) S_X acts naturally on X via the map $\sigma \mapsto \sigma$.

(2) D_{2n} acts naturally on the set $\{1, 2, \ldots, n\}$ via the picture



For example, in D_{12} we have $\pi_r = (1\ 2\ 3\ 4\ 5\ 6)$ and $\pi_s = (2\ 6)(3\ 5)$, and

$$\pi_{sr} = (1\ 6)(2\ 5)(3\ 4) = (2\ 6)(3\ 5) \circ (1\ 2\ 3\ 4\ 5\ 6) = \pi_s \circ \pi_r.$$

In general, we naturally have a map $\pi : D_{2n} \to S_n$ and it is a homomorphism.

(3) G naturally acts on itself in a number of ways. Here is one of them. For each $g \in G$ let $\psi_g : G \to G$ given by $\psi_g(x) = gxg^{-1}$. ψ_g is an automorphism of G so is certainly a permutation of G. Moreover, for any $g, h \in G$,

$$\begin{aligned} \psi_{gh}(x) &= (gh)x(gh)^{-1} = (gh)xh^{-1}g^{-1} = g(hxh^{-1})g^{-1} \\ &= g\psi_h(x)g^{-1} = \psi_g(\psi_h(x)) = (\psi_g \circ \psi_h)(x), \end{aligned}$$

true for all $x \in G$, so $\psi_{gh} = \psi_g \circ \psi_h$. Hence the map $g \mapsto \psi_g$ is a homomorphism $\psi : G \to S_G$.

Notation. If π is an action of G on X, and $g \in G$ and $a, b \in X$, then we express $\pi_g(a) = b$ by writing $g \cdot a = b$ and say *g moves a to b*. Note that $\pi_{gh} = \pi_g \circ \pi_h$ translates to $(gh) \cdot a = g \cdot (h \cdot a)$ for all $a \in X$. Note also that $\pi_1 = \mathrm{id}$, which translates to $1 \cdot a = a$ for all $a \in X$.

Warning. What I have defined is known elsewhere as a *left action* of G on X. Many group theorists prefer to work with *right actions*. In our terminology, a *right action* of G on X is a map $\pi : G \to S_X$ satisfying $\pi_{gh} = \pi_h \circ \pi_g$, i.e., the composition with π_g evaluated first and π_h second. This sort of action is usually accompanied by a decision to follow the convention that composition of functions is done from the left, rather than from the right; this allows us to write $\pi_{gh} = \pi_g \circ \pi_h$ so π is again a homomorphism. But now we get confusing equations like $(\pi_g \circ \pi_h)(x) = \pi_h(\pi_g(x))$. To avoid this, users also adopt the convention to apply functions "from the right," meaning they write $x\pi_g$ instead of $\pi_g(x)$. Thus they would write $x(\pi_g \circ \pi_h) = (x\pi_g)\pi_h$. It all works, but it is a form of madness that we will not poke into.

Definition. Let π be an action of G on X.

(1) The **kernel** of the action is the kernel of π as a homomorphism $G \to S_X$.
(2) The action is **faithful** if its kernel is $\{1\}$ (equivalently, if π is injective).
(3) Given $a \in X$, the **orbit** of a is the set $G \cdot a = \{g \cdot a : g \in G\}$ of elements of X to which a gets moved by the elements of G.

Note: if G acts faithfully on X, then G is isomorphic to a subgroup of S_X. (π is the isomorphism.)

Warning: $G \cdot a$ is not a coset of G. (It is not even a subset of G.)

Proposition 15.2. *Suppose G acts on X. The orbits of the action partition X.*

Proof. As $a \in G \cdot a$ for each $a \in X$, the orbits clearly cover X. Suppose $G \cdot a, G \cdot b$ are two orbits with $G \cdot a \cap G \cdot b \neq \varnothing$. Pick $x \in G \cdot a \cap G \cdot b$; thus pick $g, h \in G$ with $g \cdot a = x = h \cdot b$. Then

$$(h^{-1}g) \cdot a = h^{-1} \cdot (g \cdot a) = h^{-1} \cdot (h \cdot b) = (h^{-1}h) \cdot b = 1 \cdot b = b,$$

proving $b \in G \cdot a$. It is easy to show that $b \in G \cdot a$ implies $G \cdot b \subseteq G \cdot a$. Dually we get $G \cdot a \subseteq G \cdot b$. So $G \cdot a = G \cdot b$. □

Definition. An action of G on X is **transitive** if it has only one orbit (X).

Example 15.3. The natural action of D_{2n} on $\{1, 2, \ldots, n\}$ is transitive, since for any $i, j \in \{1, \ldots, n\}$ we can find $g \in D_{2n}$ such that $g \cdot i = j$.

Definition. Let π be an action of G on X. Given $a \in X$, the **stabilizer** of a is the set

$$G_a = \{g \in G : g \cdot a = a\}.$$

Proposition 15.4. *Suppose G acts on X. For every $a \in X$:*

(1) $G_a \leq G$.
(2) $|G \cdot a| = [G : G_a]$.

Hence if G is finite, then every orbit has size dividing $|G|$.

Proof. (1) Exercise.

(2) Recall that $G \cdot a = \{g \cdot a : g \in G\}$. Observe that for $g, h \in G$,

$$g \cdot a = h \cdot a \iff h^{-1} \cdot (g \cdot a) = h^{-1} \cdot (h \cdot a)$$
$$\iff (h^{-1}g) \cdot a = a \iff h^{-1}g \in G_a \iff hG_a = gG_a.$$

In other words, the value of $g \cdot a$ depends only on the left coset of G_a determined by g. Thus the number of distinct values of $g \cdot a$ equals the number of distinct left cosets of G_a in G. □

Example 15.5. Consider the natural action of $G = D_{2n}$ on $\{1, 2, \ldots, n\}$. This action is transitive. Thus for any $i \in \{1, 2, \ldots, n\}, |G \cdot i| = n$. Hence by the Orbit-Stabilizer Theorem, the stabilizer of i must have order 2. Obviously the identity element of D_{2n} is in the stabilizer of i. What is the other element in the stabilizer?

16. Permutation representations and Cayley's Theorem

Let G be a group. G acts on itself by left multiplication: $g \cdot a = ga$. Call this action λ; so for $g \in G, \lambda_g$ is the permutation in S_G given by $\lambda_g(a) = ga$.

Note that λ is a homomorphism $G \to S_G$, since for any $g, h \in G$,

$$\lambda_{gh}(a) = (gh)a = g(ha) = \lambda_g(\lambda_h(a)) = (\lambda_g \circ \lambda_h)(a) \qquad \text{for all } a \in G,$$

proving $\lambda_{gh} = \lambda_g \circ \lambda_h$.

Note also that if $g \neq 1$ then $\lambda_g(1) = g1 = g \neq 1$, so $\lambda_g \neq \mathrm{id}$. Hence $\ker \lambda = \{1\}$, so by Corollary 13.3, λ is injective (i.e., the action is faithful). Hence λ is an isomorphism from G to its image $\mathrm{im}(\lambda)$. As $\mathrm{im}(\lambda)$ is a subgroup of S_G by Proposition 11.2(4), we have proved the first statement in

Theorem 16.1 (Cayley's Theorem)**.** *Every group is isomorphic to a subgroup of a symmetric group. If $|G| = n$, then G is isomorphic to a subgroup of S_n.*

Proof. The first statement was proved above. If $|G| = n$ then any bijection $\tau : G \to \{1, 2, \ldots, n\}$ determines an isomorphism $\overline{\tau} : S_G \cong S_n$ (exercise), which composed with λ gives an isomorphism from G to a subgroup of S_n. □

We proved Cayley's theorem by exhibiting a faithful action of G on a $|G|$-element set (namely, G itself). Sometimes we can find smaller sets on which G faithfully acts.

Example 16.2. Suppose $\{1\} < H < G$. Recall that G/H is the set of left cosets of H. G acts on G/H by left multiplication:

$$g \cdot aH = (ga)H.$$

It is easy to check that this is an action (i.e., the map $\lambda : G \to S_{G/H}$ where λ_g is the permutation $aH \mapsto (ga)H$ is a homomorphism). Let $N = \ker \lambda$. Note that if $g \in N$ then $\lambda_g = \mathrm{id}$, so $\lambda_g(H) = H$, meaning $gH = H$, which implies $g \in H$. Thus $N \subseteq H$.

Proposition 16.3. *Suppose G is a finite group, $\{1\} < H < G$, and G has no normal subgroups contained in H except for $\{1\}$. Then G is isomorphic to a subgroup of S_m where $m = [G : H]$.*

Proof. Let λ be the action of G on G/H by left multiplication. The kernel of λ is a normal subgroup of G (Proposition 11.3) contained in H (Example 16.2), so must be $\{1\}$. Hence λ is faithful, so $\lambda : G \cong \mathrm{im}(\lambda) \leq S_{G/H} \cong S_m$. □

The action of G on G/H is also the key to the proof of the following.

Proposition 16.4. *Suppose G is a finite group and p is the smallest prime dividing $|G|$. If $H \leq G$ with $[G : H] = p$, then $H \lhd G$.*

Proof. Let λ be the action of G on G/H by left multiplication. Let $N = \ker \lambda$. Thus $N \lhd G$ (Proposition 11.3) and $N \subseteq H$ (Example 16.2). Whether or not λ is injective, we know from the 1st Isomorphism Theorem that $G/N \cong \mathrm{im}(\lambda) \leq S_{G/H} \cong S_p$, so G/N is isomorphic to a subgroup of S_p. Hence $|G/N|$ divides $|S_p| = p!$ by Lagrange's theorem. What else can we say about $|G/N|$?

Because $N \subseteq H$, we can define $[H : N] = k$ and get

$$|G/N| = \frac{|G|}{|N|} = \frac{|G|}{|H|} \cdot \frac{|H|}{|N|} = pk.$$

Thus $pk|p!$, and hence $k|(p-1)!$ But k divides $|H|$, which divides $|G|$, so every prime divisor of k must be $\geq p$ (by choice of p). This forces $k = 1$, which implies $N = H$, so $H = N \lhd G$. □

Here is one final example of this kind. Suppose G is a group with $|G| = 52$, and $H \leq G$ with $|H| = 13$. I claim that these assumptions imply $H \lhd G$. Here's why. Let λ be the action of G on G/H. Let $N = \ker \lambda$. Then $N \lhd G$ and $N \subseteq H$. The latter fact implies $|N|$ divides $|H| = 13$ (by Lagrange's Theorem), so $|N| = 1$ or 13.

Suppose $N = 1$. Then λ is faithful, so $\lambda : G \cong \mathrm{im}(\lambda) \leq S_{[G/H]}$, proving G is isomorphic to a subgroup of S_4. But $|G| = 52$ while $|S_4| = 4! = 24$, so G can't possibly be isomorphic to a subgroup of S_4. This case is impossible.

Hence $|N| = 13$. But $N \subseteq H$ and $|H| = 13$. These facts imply $H = N \lhd G$.

Can you generalize this example?

17. Class equation and Cauchy's theorem

Let G be a group. Recall from Example 15.1(3) that G acts on itself by conjugation: the action $\psi : G \to S_G$ is given by $\psi_g(x) = gxg^{-1}$, or equivalently by $g \cdot a = gag^{-1}$. In this section we will explore some of the properties of this action.

Given $a \in G$, what is the orbit $G \cdot a$ under this action? Clearly,

$$G \cdot a = \{gag^{-1} : g \in G\}, \quad \text{the set of conjugates of } a.$$

Definition. The set $\{gag^{-1} : g \in G\}$ is called the **conjugacy class** of a and is denoted $\mathrm{Conj}(a)$.

Example 17.1. If $G = S_3$, then brute force calculations show:

$$\begin{aligned}
\mathrm{Conj}(\mathrm{id}) &= \{\pi \circ \mathrm{id} \circ \pi^{-1} : \pi \in S_3\} = \{\mathrm{id}\} \\
\mathrm{Conj}((1\ 2)) &= \{\pi \circ (1\ 2) \circ \pi^{-1} : \pi \in S_3\} = \{(1\ 2),\ (1\ 3),\ (2\ 3)\} \\
\mathrm{Conj}((1\ 2\ 3)) &= \{\pi \circ (1\ 2\ 3) \circ \pi^{-1} : \pi \in S_3\} = \{(1\ 2\ 3),\ (1\ 3\ 2)\}.
\end{aligned}$$

Note in the previous example that the displayed conjugacy classes partition G and their sizes are divisors of $|S_3|$. This holds generally.

Proposition 17.2. *Let G be a group.*

1. *G is partitioned by its conjugacy classes.*
2. *For any $a \in G$, define $C_G(a) = \{x \in G : xa = ax\}$. Then $C_G(a) \leq G$ and $|\mathrm{Conj}(a)| = [G : C_G(a)]$.*

In particular, $|\mathrm{Conj}(a)|$ divides $|G|$ when G is finite.

Notation. The subgroup $C_G(a)$ is called the **centralizer** of a (in G).

Proof. (1) follows from Proposition 15.2. (2) follows from Proposition 15.4 and the following calculation:

$$G_a = \{g \in G : g \cdot a = a\} = \{g \in G : gag^{-1} = a\} = \{g \in G : ga = ag\} = C_G(a). \quad \square$$

Again let G be an arbitrary group acting on itself by conjugation. Of particular interest in this context are the 1-element orbits (conjugacy classes.) Recall that the **center** of a group G is the set $Z(G) = \{x \in G : xa = ax \text{ for all } a \in G\}$, which is a subgroup of G. Next, let us agree to call a conjugacy class **trivial** if it is a 1-element set, and **nontrivial** otherwise. Finally, observe that

$$\begin{aligned}
\mathrm{Conj}(a) = \{a\} \quad &\iff \quad |\mathrm{Conj}(a)| = 1 \\
&\iff \quad [G : C_G(a)] = 1 \\
&\iff \quad C_G(a) = G \\
&\iff \quad ga = ag \text{ for all } g \in G \\
&\iff \quad a \in Z(G).
\end{aligned}$$

Thus $Z(G)$ is the union of the trivial conjugacy classes, which with Proposition 17.2(1) proves:

Proposition 17.3 (Class equation)**.** *Every group G is the disjoint union of $Z(G)$ and its nontrivial conjugacy classes.*

Here are some useful consequences of the Class equation.

Theorem 17.4. *If p is a prime and $|G| = p^n$, then $Z(G) \neq \{1\}$.*

Proof. By the class equation,

$$p^n = |G| = |Z(G)| + \sum_{i=1}^{m} |\mathrm{Conj}(a_i)|$$

where $\mathrm{Conj}(a_1), \ldots, \mathrm{Conj}(a_m)$ are the nontrivial conjugacy classes. Each $|\mathrm{Conj}(a_i)|$ divides p^n and is > 1. Hence $|Z(G)| \equiv 0 \pmod{p}$, so $|Z(G)| \geq p$. □

Theorem 17.5 (Cauchy's Theorem)**.** *Suppose G is a finite group. If p is prime and p divides $|G|$, then there exists an element in G of order p.*

Proof. Note that it suffices to prove the existence of $a \in G$ such that p divides $\circ(a)$. (If $\circ(a) = pk$, then $\circ(a^k) = p$; exercise.)

We first prove the theorem for *abelian* groups, by induction on $|G|$.

Base: $|G| = p$. Then G is cyclic of order p by Corollary 7.7, done.

Inductive Step: $|G| = pm, m > 1$. Pick any element $a \in G \backslash \{1\}$.

Case 1: p divides $\circ(a)$. Then we're done by the note at the start of the proof.

Case 2: p does not divide $\circ(a)$.

Let $N = \langle a \rangle$. Clearly $\{1\} < N < G$. Also, $N \lhd G$ (as G is abelian) so G/N is a group. $|N| > 1$ implies $|G/N| < |G|$. Also $|G| = |N| \cdot |G/N|$ so p divides $|G/N|$. In fact, G/N is an *abelian* group (exercise), so the inductive hypothesis applies and we get an element $bN \in G/N$ of order p. (The order is calculated in the quotient group.)

Let $m = \circ(b)$. Then $b^m = 1$, so $(bN)^m = b^m N = N$. If we apply Proposition 3.3 to the group G/N and its element bN, we get that the order of bN (i.e., p) must divide m, so $p|m$. Thus back in G, the order of b (i.e., m) is a multiple of p so we're done by the note at the start of the proof. This finishes the proof in the abelian case.

Now we prove the general case, again by induction on G. Look at the class equation:

$$|G| = |Z(G)| + \sum_{i=1}^{m} |\mathrm{Conj}(a_i)|.$$

Case 1. For some i we have that $|\mathrm{Conj}(a_i)|$ is *not* divisible by p.

Since $|\mathrm{Conj}(a_i)| = \frac{|G|}{|C_G(a_i)|}$ by Proposition 17.2, it must be that p divides $|C_G(a_i)|$. Note that $C_G(a_i) \leq G$, and $C_G(a_i) \neq G$ (as $a_i \notin Z(G)$). So we can apply the inductive hypothesis to $C_G(a_i)$ to get an element of order p.

Case 2. p divides every $|\mathrm{Conj}(a_i)|$.

Then the Class equation implies that p divides $|Z(G)|$. Note that $Z(G)$ is abelian so our argument in the abelian case gives an element of $Z(G)$ of order p. □

18. Finite abelian groups

Lemma 18.1. *Suppose G is an abelian group and $m \in \mathbb{Z}$. Define $G^{(m)} = \{a \in G : a^m = 1\}$. Then $G^{(m)} \leq G$.*

Proof. $1 \in G^{(m)}$. $a, b \in G^{(m)} \Rightarrow a^m = b^m = 1 \Rightarrow (ab)^m = a^m b^m = 1 \Rightarrow ab \in G^{(m)}$. Similarly, $a \in G^{(m)} \Rightarrow (a^{-1})^m = (a^m)^{-1} = 1 \Rightarrow a^{-1} \in G^{(m)}$. □

Lemma 18.2. *Suppose G is finite abelian and $|G| = mk$ with $\gcd(m, k) = 1$. Then*

1. *$G \cong G^{(m)} \times G^{(k)}$*
2. *$|G^{(m)}| = m$ and $|G^{(k)}| = k$.*

Proof. (1) We will use Theorem 10.1 with $H = G^{(m)}$ and $K = G^{(k)}$. First, suppose $a \in G^{(m)} \cap G^{(k)}$. Then $a^m = a^k = 1$. Pick $x, y \in \mathbb{Z}$ with $mx + ky = 1$. Then

$$a = a^{(mx+ky)} = (a^m)^x \cdot (a^k)^y = 1^x \cdot 1^y = 1.$$

This proves $\boxed{G^{(m)} \cap G^{(k)} = \{1\}}$

Next note that if $a \in G$ then $1 = a^{mk} = (a^k)^m = (a^m)^k$, providing $a^k \in G^{(m)}$ and $a^m \in G^k$. Hence

$$a = a^{mx+ky} = \underbrace{(a^k)^y}_{\in G^{(m)}} \cdot \underbrace{(a^m)^x}_{\in G^{(k)}} \in G^{(m)} \cdot G^{(k)}.$$

This proves $\boxed{G = G^{(m)} \cdot G^{(k)}}$. Obviously $\boxed{G^m, G^k \lhd G}$. So we can apply Theorem 10.1 to get $G \cong G^{(m)} \times G^{(k)}$.

(2) Let $|G^{(m)}| = m'$ and $|G^{(k)}| = k'$. Clearly $mk = |G| = m'k'$, by (1). Suppose $\gcd(m, k') \neq 1$. Then we can choose a prime p dividing both m and k'. By Cauchy's theorem, there exists $a \in G^{(k)}$ with $\circ(a) = p$. But $p|m$ implies $a^m = 1$, so $a \in G(m)$. Thus $a \in G^{(m)} \cap G^{(k)}$. But we proved $G^{(m)} \cap G^{(k)} = \{1\}$ in the proof of (1), so $a = 1$, contradiction. This proves $\gcd(m, k',) = 1$.

Now $m|m'k'$ and $\gcd(m, k') = 1$ imply $m|m'$ and hence $m \leq m'$. A similar argument gives $k \leq k'$. As $mk = m'k'$, this can only happen if $m = m'$ and $k = k'$. □

Repeated applications of Lemma 18.2 yield:

Corollary 18.3. *Suppose G is finite abelian and $|G| = n = p_1^{n_1} \dots p_k^{n_k}$ where $p_1, \dots, p_k$ are distinct primes.*

1. *$G \cong G^{(p_1^{n_1})} \times \cdots \times G^{(p_k^{n_k})}$*
2. *$|G^{(p_i^{n_i})}| = p_i^{n_i}$ for each i.*

The equation in Corollary 18.3(1) is called the **primary decomposition** of G.

Example 18.4. Let $G = (\mathbb{Z}_{13}^\times, \cdot)$. $|G| = 12 = 2^2 \cdot 3$.

$$G^{(4)} = \{a \in \mathbb{Z}_{13}^\times : a^4 = 1\} = \{1, 5, 8, 12\}$$
$$G^{(3)} = \{a \in \mathbb{Z}_{13}^\times : a^3 = 1\} = \{1, 3, 9\}$$

By Lemma 18.2, $(\mathbb{Z}_{13}^\times, \cdot) \cong (\{1, 5, 8, 12\}, \cdot) \times (\{1, 3, 9\}, \cdot)$ where the multiplication in both subgroups is (mod 13).

19. Finite abelian groups (continued)

Definition. Fix a prime p. A finite group is a p-**group** if $|G| = p^n$ for some $n \geq 1$.

In Corollary 18.3 we saw that every finite abelian group can be factored as a direct product of finite abelian p-groups, where p varies over the prime divisors of $|G|$. In this section we will see how to further factor the finite abelian p-groups.

Definition. Let G be an abelian group. A **basis** for G is a sequence $a_1, \ldots, a_t \in G$ satisfying

(1) $a_i \neq 1$ for all i.
(2) $G = \langle a_1 \rangle \langle a_2 \rangle \ldots \langle a_t \rangle$
(3) For all $i = 1, 2, \ldots, t-1$, if $H_i = \langle a_1 \rangle \langle a_2 \rangle \cdots \langle a_i \rangle$ then

$$H_i \cap \langle a_{i+1} \rangle = \{1\}$$

Suppose $a_1, \ldots, a_t$ is a basis for G. For each i let $N_i = \langle a_i \rangle$. Condition (3) says $H_i \cap N_{i+1} = \{1\}$ for all $i < t$. Note that $H_i N_{i+1} = H_{i+1}$. Since G is abelian we of course have $H_i, N_{i+1} \lhd H_{i+1}$. Hence by Theorem 10.1, $H_{i+1} \cong H_i \times N_{i+1}$ (for each $i < t$). Thus

$$\begin{aligned} G = H_t & \qquad \text{by (2)} \\ &\cong H_{t-1} \times N_t \\ &\cong H_{t-2} \times N_{t-1} \times N_t \\ &\vdots \\ &\cong N_1 \times N_2 \times \ldots \times N_t \end{aligned}$$

This proves:

Proposition 19.1. *If G is abelian and G has a basis, then G is isomorphic to a direct product of cyclic groups.*

Theorem 19.2. *Every finite abelian p-group has a basis.*

Proof sketch. Let $|G| = p^n$ with $n \geq 1$. Start be choosing a_1 to be an element of G with $\circ(a_1)$ maximum, say $\circ(a_1) = p^{n_1}$. We have $n_1 > 0$ by Cauchy's Theorem, so $a_1 \neq 1$. If $n_1 = n$ then $G = \langle a_1 \rangle$ and we're done. Otherwise, let $H_1 = \langle a_1 \rangle$, form G/H_1 the quotient group, and pick an element $bH_1 \in G/H_1$ with $\circ(bH_1)$ maximum **calculated in the quotient group**. Observe that $|G/H_1| = p^n/p^{n_1} = p^{n-n_1} > 1$, so $\circ(bH_1) = p^{n_2}$ for some $n_2 \leq n - n_1$, and clearly $n_2 > 0$.

Also let $\circ(b) = p^k$. Then $k \leq n_1$ (by choice of a_1). Furthermore, $b^{p^k} = 1$, so $(bH_1)^{p^k} = b^{p^k} H_1 = H_1$, so (arguing as in the proof of Cauchy's Theorem) the order of bH_1 calculated in the quotient group (i.e., p^{n_2}) divides p^k. This proves $n_2 \leq k$ and thus $n_2 \leq n_1$.

Claim. *There exists $a_2 \in bH_1$ with $\circ(a_2) = p^{n_2}$.*

Proof. From $(bH)^{p^{n_2}} = H$ we get $b^{p^{n_2}} \in H_1 = \langle a_1 \rangle$. Write $b^{p^{n_2}} = a_1^i$. Then

$$a_1^{ip^{n_1-n_2}} = (b^{p^{n_2}})^{p^{n_1-n_2}} = b^{p^{n_1}}.$$

Note that $k \leq n_1$ (proved above), so $\circ(b) = p^k | p^{n_1}$, so $\boxed{b^{p^{n_1}} = 1}$. Hence $a_1^{ip^{n_1-n_2}} = 1$, which implies $\circ(a_1) | ip^{n_1-n_2}$, i.e., $p^{n_1} | ip^{n_1-n_2}$, which implies $p^{n_2} | i$, say $i = jp^{n_2}$. This implies $b^{p^{n_2}} = (a_1^j)^{p^{n_2}}$. Now define $a_2 = ba_1^{-j}$. Note that:

(1) $a_2 \in bH_1$. (Since $a_1 \in H_1$)
(2) $(a_2)^{p^{n_2}} = (ba_1^{-j})^{p^{n_2}} = b^{p^{n_2}}((a_1^j)^{p^{n_2}})^{-1} = b^{p^{n_2}}(b^{p^{n_2}})^{-1} = 1$.
(3) For any $t \in \mathbb{Z}$, if $a_2^t = 1$, so $(ba_1^{-j})^t = 1$, then $b^t \in \langle a_1 \rangle = H_1$, so $(bH_1)^t = H_1$ calculated in G/H_1. As $\circ(bH_1) = p^{n_2}$, this forces $p^{n_2} | t$.

The last two facts prove $\circ(a_2) = p^{n_2}$ as claimed. □

In particular, $a_2 \neq 1$ since $n_2 > 0$. Thus a_1, a_2 satisfy property (1) in the definition of *basis*. Next we will show that a_1, a_2 satisfy property (3) in the definition of *basis* in the case $i = 1$.

Claim. $H_1 \cap \langle a_2 \rangle = \{1\}$.

Proof. Assume $0 \leq t < p^{n_2}$ and $a_2^t \in H_1$. The calculation proving item (3) above can be easily adjusted to still obtain $b^t \in H_1$, so $(bH_1)^t = H_1$, so $p^{n_2} | t$, and so $t = 0$. Thus $H_1 \cap \{1, a_2, a_2^2, \ldots, a_2^{p^{n_2-1}}\} = \{1\}$ □

Now we let $H_2 = \langle a_1 \rangle \langle a_2 \rangle$. If $H_2 = G$ then we're done. Otherwise, form G/H_2, and pick an element $cH_2 \in G/H_2$ with $\circ(cH_2)$ maximum. We get $\circ(cH_2) = p^{n_3}$ for some $n_3 \leq n - (n_1 + n_2)$. We can prove $c^{p^{n_1}} = 1$ and $(cH_1)^{p^{n_2}} = H_1$ by our choice of a_1, bH_1. (For example, $\circ(cH_1) = p^\ell$ for some ℓ, and $\circ(cH_1) \leq \circ(bH_1) = p^{n_2}$ by our choice of bH_1, so $\ell \leq n_2$, so $p^\ell | p^{n_2}$, so $(cH_1)^{p^{n_2}} = H_1$.) Hence, $\boxed{c^{p^{n_1}} = 1}$ and $\boxed{c^{p^{n_2}} \in H_1}$.

Claim. *There exists $a_3 \in cH_2$ with $\circ(a_3) = p^{n_3}$.*

Proof sketch. $(cH_2)^{p^{n_3}} = H_2 = \langle a_1 \rangle \langle a_2 \rangle$, so $c^{p^{n_3}} = a_1^{i_1} a_2^{i_2}$ for some i_1, i_2. The two boxed facts above can be used to deduce $p^{n_3} | i_1$ and $p^{n_3} | i_2$ respectively.

(Details: recall that $c^{p^{n_2}} \in H_1$. But

$$c^{p^{n_2}} = (c^{p^{n_3}})^{p^{n_2-n_3}} = (a_1^{i_1} a_2^{i_2})^{p^{n_2-n_3}} = (a_1^{i_1 p^{n_2-n_3}})(a_2^{i_2 p^{n_2-n_3}}).$$

Hence $a_2^{i_2 p^{n_2-n_3}} = c^{p^{n_2}}(a_1^{i_1 p^{n_2-n_3}})^{-1} \in H_1$ as both factors are in H_1. This implies $(a_2 H_1)^{i_2 p^{n_2-n_3}} = H_1$, so $\circ(a_2 H_1) = p^{n_2} | i_2 p^{n_2-n_3}$, which in turn implies $p^{n_3} | i_2$. Next we prove $p^{n_3} | i_1$. Start with the fact, proved above, that $c^{p^{n_1}} = 1$. This implies

$$1 = c^{p^{n_1}} = (c^{p^{n_3}})^{p^{n_1-n_3}} = (a_1^{i_1} a_2^{i_2})^{p^{n_1-n_3}} = (a_1^{i_1 p^{n_1-n_3}})(a_2^{i_1 p^{n_1-n_3}}).$$

which implies

$$a_1^{i_1 p^{n_1-n_3}} = (a_2^{i_1 p^{n_1-n_3}})^{-1} \in \langle a_2 \rangle.$$

Obviously $a_1^{i_1 p^{n_1-n_3}} \in \langle a_1 \rangle = H_1$. So $a_1^{i_1 p^{n_1-n_3}} \in H_1 \cap \langle a_2 \rangle$, implying $a_1^{i_1 p^{n_1-n_3}} = 1$. But $\circ(a_1) = p^{n_1}$, so $p^{n_1} | i_1 p^{n_1-n_3}$, implying $p^{n_3} | i_1$.)

Now let $i_1 = j_1 p^{n_3}$ and $i_2 = j_2 p^{n_3}$ and define $a_3 = c a_1^{-j_1} a_2^{-j_2}$. This works (left as an exercise). □

Claim. $H_2 \cap \langle a_3 \rangle = \{1\}$. (Proved similarly to $H_1 \cap \langle a_2 \rangle = \{1\}$.)

Now if $G = H_2\langle a_3 \rangle$, then we can stop. Otherwise, we must look for a_4. Start by letting $H_3 = H_2\langle a_3 \rangle$ and forming G/H_3. Choose $dH_3 \in G/H_3$ with $\circ(dH_3)$ maximum ...

And so on. As G is finite, this process must eventually stop, at which point $a_1, a_2, \ldots, a_t$ will be a basis for G. □

By combining Theorem 19.2 with Proposition 19.1 and Corollary 18.3 we get the following:

Theorem 19.3. *Every finite abelian group is isomorphic to a direct product of cyclic groups whose orders are powers of primes.*

Since every cyclic group of order p^n is isomorphic to $(\mathbb{Z}_{p^n}, +)$ (Proposition 6.6), it follows that every finite abelian group G satisfies

$$(*) \qquad G \cong (\mathbb{Z}_{p_1^{n_1}}, +) \times (\mathbb{Z}_{p_2^{n_2}}, +) \times \cdots \times (\mathbb{Z}_{p_k^{n_k}}, +)$$

for some (not necessarily distinct) primes $p_1, \ldots, p_k$ and positive integers $n_1, \ldots, n_k$. The list of prime powers $p_1^{n_1}, \ldots, p_k^{n_k}$ occurring in $(*)$ is called the list of **elementary divisors** of G; they are uniquely determined by G. This fact (which we will not prove), together with Theorem 19.3, form one version of what is known as the *Fundamental Theorem of Finite Abelian Groups*.