MA3102

Algebra I

Autumn 2021

Satvik Saha

19MS154

Indian Institute of Science Education and Research, Kolkata,
Mohanpur, West Bengal, 741246, India.

Contents

1   Symmetries

1.1   Symmetries of plane figures

A symmetry of a plane figure can be thought of as a rigid motion which *preserves its structure*, i.e. sends it to itself.

For example, consider an equilateral triangle; there is the identity symmetry (which does nothing), two rotations by $2\pi/3$ and $2\pi/3$, and three reflections. This gives us a total of 6 symmetries. Coincidentally, the plane symmetries of an equilateral triangle are precisely the set of $3! = 6$ permutations of its vertices.
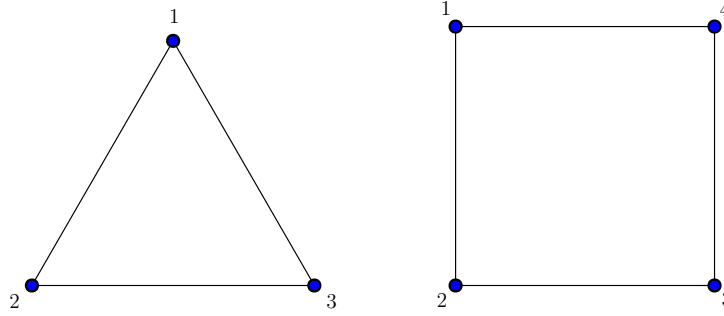
The same cannot be said of a square; there are $4! = 24$ of its vertices, but only 8 of them are rigid motions. Here, we see 4 rotations and 4 reflections.

In general, a regular n-gon has $2n$ plane symmetries, of which n are rotations and n are reflections. This can be seen by noting that a symmetry of an n-gon is completely determined by its action on an edge; once the final positions of the first two vertices is determined, the rest are forced. There are n positions for the first vertex, which leaves only 2 positions for the second vertex. One of these choices results in a rotation (since it preserves the cyclicity of the vertices) and the other a reflection (since it reverses the cyclicity of the vertices).

Note that these symmetries can be *composed*, i.e. applied in succession. For example, a rotation by $2\pi/n$ can be applied repeatedly to obtain every possible rotational symmetry. Similarly, we can perform rotations and reflections in succession, and we always end up with another symmetry. This composition is associative, there is an identity symmetry, and each symmetry has an inverse. The collection of such symmetries forms a *group*.

The group of plane symmetries of a regular n-gon is called the *dihedral group*, denoted as D_{2n}.

1.2   Symmetries of the Euclidean plane

Consider the class of isometries of the plane, i.e. all bijections $f\colon \mathbb{R}^2 \to \mathbb{R}^2$ such that $\|f(\boldsymbol{v}) - f(\boldsymbol{w})\| = \|\boldsymbol{v} - \boldsymbol{w}\|$. These constitute symmetries of the Euclidean plane $\mathbb{R}^2$. The three basic forms of such symmetries are rotations, reflections, and translations; it can be shown that every symmetry of $\mathbb{R}^2$ is a combination of at most three reflections. Another representation for each symmetry is

$$f(\boldsymbol{v}) = A\boldsymbol{v} + \boldsymbol{v}_0,$$

where $A \in O_2(\mathbb{R})$ is an orthogonal matrix, accounting for the rotational and reflectional part of the transformation.

To show this, set $\boldsymbol{v}_0 = f(\boldsymbol{0})$ and define $g = f - \boldsymbol{v}_0$. Thus, $g(\boldsymbol{0}) = \boldsymbol{0}$, and g is also an isometry. Not that for all $\boldsymbol{v}, \boldsymbol{w} \in \mathbb{R}^2$, we can write

$$\|g(\boldsymbol{v}) - g(\boldsymbol{w})\|^2 = \|g(\boldsymbol{v})\|^2 + \|g(\boldsymbol{w})\|^2 - 2\langle g(\boldsymbol{v}), g(\boldsymbol{w})\rangle,$$
$$\|\boldsymbol{v} - \boldsymbol{w}\|^2 = \|\boldsymbol{v}\|^2 + \|\boldsymbol{w}\|^2 - 2\langle \boldsymbol{v}, \boldsymbol{w}\rangle.$$

On the other hand, $\|g(\boldsymbol{v}) - g(\boldsymbol{w})\|^2 = \|\boldsymbol{v} - \boldsymbol{w}\|^2$, and $\|g(\boldsymbol{v})\|^2 = \|\boldsymbol{v}\|^2$, $\|g(\boldsymbol{w})\|^2 = \|\boldsymbol{w}\|^2$. This gives $\langle g(\boldsymbol{v}), g(\boldsymbol{w})\rangle = \langle \boldsymbol{v}, \boldsymbol{w}\rangle$, i.e. g preserves the inner product.

We claim that $g(\alpha\boldsymbol{v}) = \alpha g(\boldsymbol{v})$ for all $\alpha \in \mathbb{R}$, $\boldsymbol{v} \in \mathbb{R}^2$. Note that $\|g(\alpha\boldsymbol{v})\| = \|\alpha\boldsymbol{v}\| = \|\alpha g(\boldsymbol{v})\|$. Now,

$$\|g(\alpha\boldsymbol{v}) - \alpha g(\boldsymbol{v})\|^2 = \|g(\alpha\boldsymbol{v})\|^2 + \|\alpha g(\boldsymbol{v})\|^2 - 2\langle g(\alpha\boldsymbol{v}), \alpha g(\boldsymbol{v})\rangle$$
$$= \alpha^2 v^2 + \alpha^2 v^2 - 2\alpha\langle \alpha\boldsymbol{v}, \boldsymbol{v}\rangle$$
$$= 2\alpha^2 v^2 - 2\alpha^2 v^2$$
$$= 0.$$

This proves that $g(\alpha \boldsymbol{v}) = \alpha g(\boldsymbol{v})$.

Next, we claim that $g(\boldsymbol{v} + \boldsymbol{w}) = g(\boldsymbol{v}) + g(\boldsymbol{w})$ for all $\boldsymbol{v}, \boldsymbol{w} \in \mathbb{R}^2$. Write

$$
\begin{aligned}
\|g(\boldsymbol{v} + \boldsymbol{w}) - g(\boldsymbol{v}) - g(\boldsymbol{w})\|^2 &= \|g(\boldsymbol{v} + \boldsymbol{w}) - g(\boldsymbol{v})\|^2 + \|g(\boldsymbol{w})\|^2 - 2\langle g(\boldsymbol{v} + \boldsymbol{w}) - g(\boldsymbol{v}), g(\boldsymbol{w})\rangle \\
&= \|\boldsymbol{v} + \boldsymbol{w} - \boldsymbol{v}\|^2 + \|\boldsymbol{w}\|^2 - 2\langle \boldsymbol{v} + \boldsymbol{w}, \boldsymbol{w}\rangle + 2\langle \boldsymbol{v}, \boldsymbol{w}\rangle \\
&= w^2 + w^2 - 2\langle \boldsymbol{v}, \boldsymbol{w}\rangle - 2w^2 + 2\langle \boldsymbol{v}, \boldsymbol{w}\rangle \\
&= 0.
\end{aligned}
$$

This proves that $g(\boldsymbol{v} + \boldsymbol{w}) = g(\boldsymbol{v}) + g(\boldsymbol{w})$. Thus, g is a linear map.

Now let $g(\boldsymbol{e}_1) = \boldsymbol{a}$ and $g(\boldsymbol{e}_2) = \boldsymbol{b}$. Clearly, $\|\boldsymbol{a}\| = \|\boldsymbol{b}\| = 1$. For arbitrary $\boldsymbol{v} \in \mathbb{R}^2$, we immediately get $g(\boldsymbol{v}) = v_x \boldsymbol{a} + v_y \boldsymbol{b}$, so by arranging $\boldsymbol{a}$ and $\boldsymbol{b}$ as the columns of a 2×2 matrix A, we have $g(\boldsymbol{v}) = A\boldsymbol{v}$. We clearly have $A^\top A = \mathbb{I}_2$ from $\boldsymbol{a}^\top \boldsymbol{a} = \boldsymbol{b}^\top \boldsymbol{b} = 1$, and $\langle \boldsymbol{a}, \boldsymbol{b}\rangle = \langle \boldsymbol{e}_1, \boldsymbol{e}_2\rangle = 0$. Thus, $A \in O_2(\mathbb{R})$. Substituting this back into f, we have

$$
f(\boldsymbol{v}) = A\boldsymbol{v} + \boldsymbol{v}_0
$$

as desired.

It can be further shown (algebraically) that every member of $O_2(\mathbb{R})$ is of the form

$$
\begin{bmatrix} \cos\theta & \mp\sin\theta \\ \sin\theta & \pm\cos\theta \end{bmatrix}.
$$

1.3   Symmetries of the Petersen graph

Consider a graph $G(V, E)$. A symmetry of G is a bijection $f : V \to V$ on the set of vertices, which preserves the edges. In other words, it preserves the adjacency function. Thus, it can be shown that the degree of each vertex will be preserved by a symmetry.

The following graph is called the Petersen graph, with 10 vertices and 15 edges.
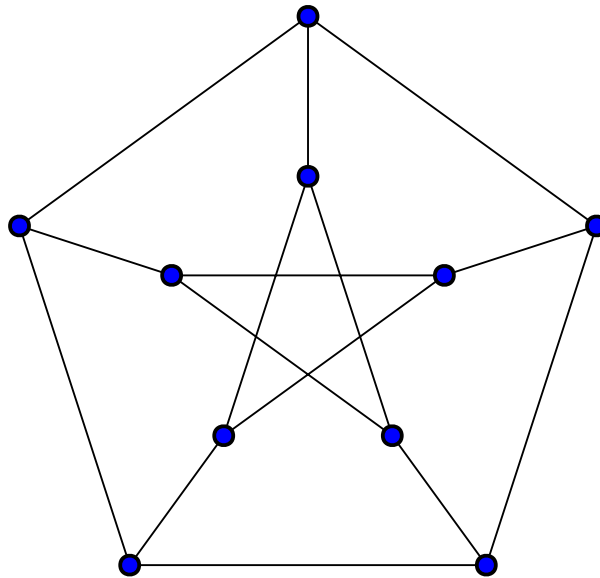
We can show that this graph has 120 symmetries. This can be done by looking at all 2 element subsets of $\{1, 2, 3, 4, 5\}$, of which there are 10. Place these subsets as the vertices of a new graph, and connect two such sets with an edge if they *are disjoint*. The resulting graph can be shown to be identical to the Petersen graph. It is immediately clear that any permutation of the set $\{1, 2, 3, 4, 5\}$ produces a relabelling of the vertices, which nevertheless preserves the Petersen graph. This gives us at least $5! = 120$ symmetries.

To show that there are at most 120 symmetries, note that every vertex has exactly 3 neighbours. Thus, when sending a vertex V to its image, we have 10 choices, but we have 3 choices for the first neighbour V_1, 2 for the second neighbour V_2. and 1 for the third neighbour V_3. Finally, choose a neighbour of V_3, say V_4 and place it in on of the 2 remaining positions. It can be shown that this completely determines the symmetry; each remaining vertex has a complete characterization in terms of the ones already fixed. Thus, we have an upper bound of $10 \times 3 \times 2 \times 1 \times 2 = 120$ symmetries.

2   Groups

2.1   Basic definitions

Definition 2.1. A group is a set G equipped with a binary operation, satisfying the following properties.

1. *Associativity*: For all $x, y, z \in G$, $x(yz) = (xy)z$.

2. *Existence of an identity element*: There exists $e \in G$ such that for all $x \in G$, $ex = e = xe$.

3. *Existence of inverse elements*: For every $x \in G$, there exists some $y \in G$ such that $xy = e = yx$. We denote $y = x^{-1}$.

Example. The integers $\mathbb{Z}$ form a group under addition.

Example. The set $\{-1, +1\}$ forms a group under multiplication.

Example. The symmetries of a tetrahedron form a group under composition of symmetries.

Lemma 2.1. *The identity element in a group is unique.*

Proof. Let G be a group, and suppose that $e, e' \in G$ satisfy

$$ex = x = xe, \qquad e'x = x = xe'$$

for all $x \in G$. Thus, we specifically have

$$ee' = e' = e'e, \qquad e'e = e = ee',$$

hence $e = e'$. □

Lemma 2.2. *The inverse of an element in a group is unique.*

Proof. Let G be a group, and let $x \in G$. Suppose that $y, y' \in G$ satisfy

$$xy = e = yx, \qquad xy' = e = y'x.$$

Thus

$$y = ye = y(xy') = (yx)y' = ey' = y'. \qquad □$$

Lemma 2.3. *The inverse of the inverse of an element in a group is the element itself.*

Proof. Let G be a group, and let $x \in G$. Set $w = (x^{-1})^{-1}$. We have

$$x^{-1}x = e = xx^{-1}, \qquad wx^{-1} = e = x^{-1}w.$$

Thus,

$$w = we = w(x^{-1}x) = (wx^{-1})x = ex = x. \qquad \square$$

Lemma 2.4 (Cancellation Law)**.** *Let G be a group, and let $x, a, b \in G$ such that $xa = xb$. Then, $a = b$. Analogously, if $ax = bx$, then $a = b$.*

Proof. Simply multiply by x^{-1} as appropriate. $\qquad \square$

Definition 2.2. The order of a group G is the number of elements it contains, i.e. $|G|$. The order of an element $g \in G$ is the smallest possible natural number n such that $g^n = e$.

2.2   Subgroups

Definition 2.3. Let G be a group, and let $H \subseteq G$. We call H a subgroup of G if

1. $e \in H$.
2. For all $x, y \in H$, $xy \in H$.
3. For all $x \in H$, $x^{-1} \in H$.

Note that this is enough to guarantee that H is a group under the same group operation as G.

Example. Consider the group $\mathbb{C} \setminus \{0\}$ of non-zero complex numbers under multiplication. The non-zero reals $\mathbb{R} \setminus \{0\}$ form a subgroup of this group.

Theorem 2.5. *Let $\mathbb{Z}$ be the group of integers under addition. Then, every subgroup of $\mathbb{Z}$ is of the form $\{0\}$ or $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$.*

Remark. The same argument shows that every subgroup of a cyclic group is cyclic.

Proof. Let $H \subseteq \mathbb{Z}$ be a subgroup. If $H = \{0\}$, we are done. Otherwise, H contains some positive integers; this is clear since H must contain some non-zero integers, whose inverses have the opposite sign. Let $n \in H$ be the smallest positive integer; we immediately have $n\mathbb{Z} \subseteq H$. Now let $m \in H$ be any other element. Now, use Euclid's Division Lemma to write $m = nq + r$, where $0 \le r < n$. Now, note that $n \in H$ implies that $nq \in H$, hence the quantity $r = m - nq \in H$. The minimality of n forces $r = 0$, hence $m = nq$. This gives $H \subseteq n\mathbb{Z}$. $\qquad \square$

Corollary 2.5.1. *If a and b are coprime integers, there exist integers m and n such that $am + bn = 1$.*

Proof. If a and b are coprime, they share no common factors greater than 1. Note that $a\mathbb{Z} + b\mathbb{Z}$ is a subgroup of the integers, and hence there is exists a unique positive integer d such that $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$. Since $a, b \in a\mathbb{Z} + b\mathbb{Z}$, we have $a, b \in d\mathbb{Z}$ so there exist r_1, r_2 such that $a = dr_1$, $b = dr_2$. This means that d is a common factor of a and b, forcing $d = 1$, i.e. $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$. Since $1 \in \mathbb{Z}$, $1 \in a\mathbb{Z} + b\mathbb{Z}$, hence there exists a combination $am + bn = 1$. $\qquad\square$

Corollary 2.5.2. *The unique positive integer d such that $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ is the greatest common divisor of a and b.*

Proof. Let d be the greatest common divisor of a and b. Write $a = a'd$, $b = b'd$, and note that a' and b' are coprime. Thus, pick m and n such that $a'm + b'n = 1$. This gives $d = am + bn$, so $d\mathbb{Z} \subseteq a\mathbb{Z} + b\mathbb{Z}$. Now, consider an arbitrary combination $ap + bq \in a\mathbb{Z} + b\mathbb{Z}$; simply write $ap + bq = (a'p + b'q)d \in d\mathbb{Z}$, hence $a\mathbb{Z} + b\mathbb{Z} \subseteq d\mathbb{Z}$. $\qquad\square$

Theorem 2.6. *Let $\mathbb{C}^\times$ be the group of non-zero complex numbers under multiplication. Then, every finite subgroup of $\mathbb{C}^\times$ is of the form $H_n = \{z^k : k \in \mathbb{N}\}$ for some n^{th} root of unity z.*

Proof. Let $H \subset \mathbb{C}^\times$ be a finite subgroup. Note that we demand $1 \in H$. If this is the only element of H, we are done, otherwise choose a different $z \in H$. Now, if $|z| \neq 1$, note that there are infinitely many elements $z, z^2, z^3, \dots$ which must belong to H, which is a contradiction; note that these generated elements are distinct as they have different magnitudes. Thus we demand $|z| = 1$, so write $e^{2\pi i x}$.

Examine the elements $1, z, z^2, \dots, z^n, \dots \in H$ for all $n \in \mathbb{N}$. Since H is finite, some pair of these must be equal. This means that $z^a = z^b$ for some $a < b$, so cancellation gives $z^{b-a} = 1$. Thus, z is a root of unity, which means that $z = e^{2\pi i k/n}$ for some $n \in \mathbb{N}$, $0 < k < n$.

We have shown that every non-identity element in H is a root of unity. Thus, pick $w = e^{2\pi i x} \in H$ such that $0 < x < 1$ and x is minimal. Furthermore, set $x = k/n$, $0 < k < n$ with k and n coprime. We claim that H consists solely of the nth roots of unity. The fact that H contains all powers of w, hence all n^{th} roots of unity is clear. Conversely, pick arbitrary $z = e^{2\pi i y} \in H$, $z \neq 1, w$; since z is a root of unity, write $y = k'/n'$ where $0 < k' < n'$, k' and n' are coprime. The minimality of x gives $x < y$, hence $y - x = (k'n - kn')/nn' > 0$. Set $p = k'n$, $q = kn'$, and using $p > q$ write $p = aq + r$ where $0 \leq r < q$. Then,

$$z = e^{2\pi i p/nn'} = e^{2\pi i(aq+r)/nn'} = e^{2\pi i aq/nn'} e^{2\pi i r/nn'} = w^a e^{2\pi i r/nn'}.$$

Thus, $zw^{-a} = e^{2\pi i r/nn'} \in H$. However, note that $r/nn' < q/nn' = x$; the minimality of x forces $r = 0$. This gives $z = w^a$, proving the result. $\qquad\square$

2.3 Cyclic groups

Definition 2.4. A group G is called cyclic if there exists an element $g \in G$ such that every element of G is a power of g. We say that G is generated by the element g, or $G = \langle g \rangle$.

Example. The additive group of integers $\mathbb{Z}$ is cyclic.

Example. The additive group of integers modulo n, $\mathbb{Z}/n\mathbb{Z}$ is a finite cyclic group.

Example. Let G be a cyclic group generated by g such that all the powers g^n are distinct. Clearly, G is infinite. Now, note that we can enumerate the elements of G as follows.

$$G = \{\ldots, g^{-2}, g^{-1}, e, g, g^2, \ldots\}.$$

We can construct a bijection $\varphi \colon G \to \mathbb{Z}$, $g^n \mapsto n$. This preserves the group operation, since $g^m g^n = g^{m+n} \mapsto m + n$, so $\varphi(g^m g^n) = \varphi(g^m) + \varphi(g^n)$. Thus, the groups G and $\mathbb{Z}$ are essentially the same.

Example. Let G be a cyclic group generated by g such that the powers $g^m = g^n$, $m > n$. This immediately gives $g^{m-n} = e$. Let k be the smallest natural number such that $g^k = e$; we claim that $G = \{e, g, \ldots, g^{k-1}\}$. To see this, note that every element of G is of the form g^p. Use the Division Lemma to write $p = kq + r$ where $0 \le r < k$, hence $g^p = g^{kq+r} = (g^k)^q g^r = g^r$. Also, the elements $e, g, \ldots, g^{k-1}$ are distinct, by the minimality of k.

Using a construction similar to that in the previous example, we can show that the groups G and $\mathbb{Z}/k\mathbb{Z}$ are essentially the same.

Lemma 2.7. *Let G be a cyclic group of n elements. Then, it has $\phi(n)$ generators, where ϕ is Euler's Totient function denoting the number of positive integers less than and coprime to n.*

Proof. Write $G = \{e, g, \ldots, g^{n-1}\}$. We claim that g^m generates G if and only if m and n are coprime.

First, suppose that m and n are coprime; choose integers a and b such that $am + bn = 1$. Thus, we have $g = g^{am+bn} = g^{am} g^{bn} = g^{am}$, which means that $g^k = g^{amk}$ in general.

Next, suppose that g^m generates G. Further suppose that $d > 1$ is a common divisor of m and n, and write $m = m'd$, $n = n'd$. Note that since g^m generates G, so does g^d since $g^m = (g^d)^{m'}$. We claim that the subgroup generated by g^d has $n' < n$ elements, and hence cannot generate G, i.e. $\langle g^d \rangle = \{e, g^d, \ldots, g^{(n'-1)d}\}$. Clearly, given any power g^{kd}, we can write $kd = nq + r$ for $0 \le r < n$; since d divides both kd and nq, it must also divide r, hence $r = r'd$. Since $0 \le r < n$, we must have $0 \le r' < n'$, which means that $g^{kd} = g^{nq+r} = g^{r'd} \in \{e, g^d, \ldots, g^{(n'-1)d}\}$. This proves the result. $\square$

Lemma 2.8. *The order of an element $g \in G$ is the order of the cyclic subgroup $\langle g \rangle$ generated by it.*

2.4 Cosets and Lagrange's Theorem

Definition 2.5. Let G be a group, and let H be a subgroup of G. A left coset of H is the set
$$gH = \{gh : h \in H\}$$
for some $g \in G$.

Lemma 2.9. *All left cosets of H contain the same number of elements.*

Proof. Consider the bijection
$$f \colon H \to gH, \qquad h \mapsto gh.$$
This map is injective by cancellation, and surjective by construction. Thus, all cosets of H contain exactly the same number of elements as in H. $\qquad\square$

Lemma 2.10. *The left cosets of H partition the group G.*

Remark. Two left cosets are either equal, or disjoint.

Proof. Define the equivalence relation $\sim_H$, where $a \sim b$ if and only if $a = bh$ for some $h \in H$. Clearly, this is reflexive ($e \in H$), symmetric ($h^{-1} \in H$) and transitive ($h_1 h_1 \in H$ when $h_1, h_2 \in H$). Thus, this is an equivalence relation, and its equivalence classes partition the group G. However, we see that the equivalence class $[g]$ is precisely the left coset gH. $\qquad\square$

Definition 2.6. The index of H in G, denoted by $[G : H]$, is the number of left cosets of H in G.

Theorem 2.11 (Lagrange's Theorem)**.** *Let G be a finite group, and let H be a subgroup of G. The order of H divides the order of G. In fact,*
$$|G| = [G : H]|H|.$$

Proof. This follows directly from the previous two lemmas. Each coset of H contains $|H|$ many elements, are disjoint, and cover the entire group G. $\qquad\square$

Corollary 2.11.1. *Let G be a finite group of n elements. Then, $g^n = e$ for any $g \in G$.*

Proof. Consider the cyclic subgroup $H = \langle g \rangle$ of G, and suppose that it has m elements. Then, $g^m = e$. However, Lagrange's Theorem says that m divides n, so $g^n = e$. $\qquad\square$

Corollary 2.11.2. *Let G be a group with p elements where p is prime. Then, G is cyclic.*

Proof. Pick any non-identity element $g \in G$, and examine $H = \langle g \rangle$. Clearly $|H| > 1$, but $|H|$ must divide p, forcing $|H| = p$. Thus, $G = H$ is the cyclic group generated by g. $\qquad\square$

Theorem 2.12. *The set of integers between 1 and n which are coprime to n form a multiplicative group modulo n.*

Proof. Let $\mathbb{Z}_n^\times$ be the set of these integers. Clearly, $1 \in G$ which is our identity. Multiplication modulo n is associative. Finally, let $m \in \mathbb{Z}_n^\times$. Since m and n are coprime, we can find p and q such that $mp + nq = 1$, which means that $mp = 1$ modulo n. Furthermore, p is coprime to n, since any common divisor of p and n must also divide $mp + nq = 1$. Thus, every $m \in \mathbb{Z}_n^\times$ has an inverse, which proves that this is a multiplicative group. $\square$

Corollary 2.12.1 (Euler's Theorem)**.** *Let n be a positive integer, and let $1 \le a < n$ be coprime to n. Then,*
$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Proof. This follows directly from the fact that $|\mathbb{Z}_n^\times| = \phi(n)$. $\square$

Corollary 2.12.2 (Fermat's Little Theorem)**.** *Let p be a prime. Then,*

$$a^p \equiv a \pmod{p}.$$

Example. The only groups of order 4 are the cyclic group C_4 and the Klein four group V_4.

Let G be a group with $|G| = 4$, and pick a non-identity element $g \in G$. Note that we must have $|g| = 2, 4$. If $|g| = 4$, then $e, g, g^2, g^3 \in G$ are distinct, forcing $G \cong C_4$.

Otherwise, let $|g| = 2$, thus $g^2 = e$. Pick another non-identity element $h \in G$, and note that if $|h| = 4$, this reduces to the previous case. Thus, we consider $|h| = 2$, hence $h^2 = e$. Now, we also need $gh, hg \in G$; note that $gh \ne g, h$ and $hg \ne g, h$ from the distinctness of g, h. On the other hand, we only have room for one more element, so $gh = hg = k \in G$. Finally, $k^2 = e$. Calculate $gk = g(gh) = h = kg$, $hk = h(hg) = g = kh$. Thus, $G \cong V_4$.

2.5   Symmetric groups

Definition 2.7. Let $X_n = \{1, 2, \dots, n\}$. A permutation of X_n is a bijection $\sigma \colon X_n \to X_n$. The set of all such permutations of X_n forms the symmetric group S_n.

Lemma 2.13. *The group S_n contains $n!$ elements.*

Definition 2.8. The permutation which sends $n_1 \rightsquigarrow n_2 \rightsquigarrow \cdots \rightsquigarrow n_k \rightsquigarrow n_1$ is called a cycle, denoted by $(n_1\, n_2\, \dots\, n_k)$.

Lemma 2.14.
$$(n_1 \, n_2 \, \ldots \, n_k) = (n_1 \, n_k)(n_1 \, n_{k-1}) \ldots (n_1 \, n_2).$$

Definition 2.9. Consider a permutation which is the product of disjoint cycles of lengths $n_1, n_2, \ldots, n_k$ (in ascending order). This permutation is said to have type $n_1, n_2, \ldots, n_k$.

Exercise 2.1. Count the number of permutations of type $1^2 2^3 3$ in S_{11}.

Solution. By creating boxes for the cycles,
$$(\cdot)(\cdot)(\cdot\,\cdot)(\cdot\,\cdot)(\cdot\,\cdot)(\cdot\,\cdot\,\cdot),$$

there are 11! ways of placing the 11 elements $a_1, \ldots, a_{11}$ into these boxes. However, in each cycle of length n, we have over counted since a single cycle can be written in n ways. Similarly, given a single permutation with cycle type n^k, the k cycles of length n can be rearranged in $k!$ ways. Thus, our answer must be
$$\frac{11!}{(1^2 \cdot 2!)(2^3 \cdot 3!)(3^1 \cdot 1!)} = 138600.$$

Lemma 2.15. *The number of permutations in S_n of type $a_1^{b_1} \ldots a_k^{b_k}$ is*
$$\frac{n!}{(a_1^{b_1} \cdot b_1!) \cdots (a_k^{b_k} \cdot b_k!)}.$$

2.6 Homomorphisms

Definition 2.10. Let $\varphi \colon G \to G'$ where G, G' are groups. We say that φ is a homomorphism if $\varphi(gh) = \varphi(g)\varphi(h)$ for all $g, h \in G$. In other words, φ preserves the multiplicative structure of G.

Example. The map sending every element from G to the identity element in G' is trivially a homomorphism.

Example. The absolute value map as well as the sign map are homomorphisms on $\mathbb{R}^\times$. The former sends the group to the multiplicative group of positive reals, the latter to the group $\{\pm 1\}$.

Example. The determinant map is a homomorphism from $GL_n(\mathbb{R})$ to $\mathbb{R}^\times$.

Lemma 2.16. *Let $\varphi\colon G \to G'$ be a homomorphism. Then, $\varphi(e) = e'$, i.e. φ sends the identity in G to the identity in G'.*

Proof. Note that
$$\varphi(e) = \varphi(ee) = \varphi(e)\varphi(e),$$
whence cancellation gives $\varphi(e) = e'$. $\qquad\square$

Lemma 2.17. *Let $\varphi\colon G \to G'$ be a homomorphism. Then, $\varphi(g^{-1}) = \varphi(g)^{-1}$ for all $g \in G$.*

Proof. Note that
$$e' = \varphi(e) = \varphi(g^{-1}g) = \varphi(g^{-1})\varphi(g). \qquad\square$$

Definition 2.11. Let $\varphi\colon G \to G'$ be a homomorphism. The set $\varphi^{-1}(e') \subseteq G$ is called the kernel of φ, and $\varphi(G) \subseteq G'$ is called its image.

Lemma 2.18. *The kernel of a homomorphism is a group, and so is its image.*

Definition 2.12. Let $\varphi\colon G \to G'$ be a homomorphism, and $g' \in \varphi(G)$. The set $\varphi^{-1}(g')$ is called a fibre of φ.

Lemma 2.19. *The fibres of a homomorphism are cosets of its kernel.*

Proof. Let $\varphi\colon G \to G'$, $N = \varphi^{-1}(e')$, and $g' \in \varphi(G)$. Select $g \in G$ such that $\varphi(g) = g'$. We claim that $\varphi^{-1}(g') = gN$. It is clear that $\varphi(gn) = \varphi(g) = g'$ for any $n \in N$, hence $gN \subseteq \varphi^{-1}(g')$. Conversely, pick $h \in \varphi^{-1}(g')$, and note that $\varphi(g^{-1}h) = g'^{-1}g' = e'$, hence $g^{-1}h \in N$. Thus, $h = g(g^{-1}h) \in gN$, giving $\varphi^{-1}(g') \subseteq gN$. $\qquad\square$

Corollary 2.19.1. *If $\varphi\colon G \to G'$ is a homomorphism, then*
$$|G| = |\operatorname{im}\varphi| \cdot |\ker\varphi|.$$

Corollary 2.19.2. *A homomorphism is injective if and only if its kernel is trivial.*

Example. Consider the sign homomorphism on the group of permutations, defined by

$$\operatorname{sgn}\colon S_n \to \{\pm 1\}, \qquad \sigma \mapsto \prod_{i>j} \frac{\sigma(i) - \sigma(j)}{i - j}.$$

To see that this is indeed a homomorphism, note that

$$\prod_{i>j} \frac{\sigma\tau(i) - \sigma\tau(j)}{i - j} = \prod_{i>j} \frac{\sigma\tau(i) - \sigma\tau(j)}{\tau(i) - \tau(j)} \cdot \prod_{i>j} \frac{\tau(i) - \tau(j)}{i - j}.$$

Now, note that the sign of any transposition (2-cycle) is always -1. Since every k-cycle is a product of $k-1$ transpositions, we see that the sign of any k-cycle is $(-1)^{k+1}$. Using the fact that any permutation can be decomposed into a product of cycles which in turn are products of transpositions, we have a simple way of computing the sign of any permutation.

Lemma 2.20. *The pre-image of a subgroup under a homomorphism is a subgroup.*

Definition 2.13. An endomorphism is a homomorphism from a group to itself.

2.7   Isomorphisms

Definition 2.14. An isomorphism $\varphi\colon G \to G'$ is a bijective homomorphism.

Lemma 2.21. *The inverse of an isomorphism is an isomorphism.*

Lemma 2.22. *An isomorphism preserves the orders of elements.*

Definition 2.15. An automorphism is an isomorphism from a group to itself.

Example. Conjugation is an automorphism, called an inner automorphism. Note that if the group G is abelian, then the inner automorphisms are just identity maps.

Lemma 2.23. *The automorphisms of a group G form a group of their own, denoted* $\operatorname{Aut}(G)$*, where the group operation is the composition of functions.*

Example. Consider the Klein four group $V_4 = \{e, a, b, c\}$. Then, $\operatorname{Aut}(G) \cong S_3$. It is easy to check that any permutation of $\{a, b, c\}$ gives an automorphism of V_4.

2.8   Normal subgroups

Definition 2.16. Let H be a subgroup of the group G. We say that H is a normal subgroup of for every $h \in H$, we have $g^{-1}hg \in H$ for all $g \in G$. We denote $H \trianglelefteq G$.

Lemma 2.24. *A subgroup H is normal if and only if $gH = Hg$ for all $g \in G$. In other words, the left and right cosets of H coincide.*

Example. Every subgroup of an abelian group is normal.

Example. The kernel of a homomorphism is a normal subgroup of the domain.

Corollary 2.24.1. *Any subgroup $H \subset G$ of index 2 is normal.*

Proof. Let $g \notin H$, and note that H, gH are the only left cosets of H, and H, Hg are the only right cosets of H. This forces $gH = Hg$. $\qquad\square$

Lemma 2.25. *Let $H \trianglelefteq G$. Then, the product of two cosets is a coset.*

Proof. We claim that $(xH)(yH) = xyH$. Note that given any element $xyh \in xyH$, we have $xyh = (xe)(yh) \in (xH)(yH)$, so $xyH \subseteq (xH)(yH)$. Now, using the fact that H is normal, let $xh_1 \in xH$ and $h_2y \in Hy = yH$. Then, $xh_1 h_2 y = xh_3 y$ for some $h_3 \in H$; but $h_3 y \in Hy = yH$ hence $h_3 y = yh_4$ for some $h_4 \in H$, hence $(xh_1)(h_2y) = xyh_4 \in xyH$ so $(xH)(yH) \subseteq xyH$. $\qquad\square$

Lemma 2.26. *Conjugacy is an equivalence relation. Thus, this partitions a group into conjugacy classes.*

Proof. It is clear that every element is conjugate to itself. If $x = gyg^{-1}$, then $y = g^{-1}xg$. Finally, if $x = g_1 y g-^{-1}$ and $y = g_2 z g_2^{-1}$, then $x = (g_1 g_2) z (g_1 g_2)^{-1}$. $\qquad\square$

Lemma 2.27. *The conjugacy class of an element in a symmetric group is precisely the set of elements with the same cycle type.*

Proof. Pick the conjugate elements $h, h' = ghg^{-1} \in S_n$. Observe that if $h(\alpha) = \beta$, then $(ghg^{-1})(g(\alpha)) = g(\beta)$. This is sufficient to show that h and h' have the same cycle types.

Furthermore, given $h, h' \in G$ with the same cycle type, it can be shown that they are conjugate. Suppose that h and h' have a k-cycle, h containing $(a_1 \ \ldots \ a_k)$ and h' containing $(a_1' \ \ldots \ a_k')$. Define the permutation $s(a_i) = a_i'$, hence $shs^{-1} = h'$ for the elements $a_1', \ldots, a_k'$. We can extend the definition of s to cover all the cycles in h and h'. $\qquad\square$

Corollary 2.27.1. *The group of all $2, 2$ cycles in S_4 (which is isomorphic to the Klein four group) is a normal subgroup.*

Lemma 2.28. *A group G in which $g^2 = e$ for every $g \in G$ is abelian.*

Proof. Let $g, h \in G$. Then, $g^2 = h^2 = e$, $(gh)^2 = e$ hence $ghgh = e$. On the other hand, $ghhg = gg = e$, hence cancellation gives $gh = hg$. $\qquad\square$

Lemma 2.29. *Let G be a finite group of even order. Then, G contains an element of order 2.*

Proof. Suppose to the contrary that G contains no element of order 2. In other words, $g \neq g^{-1}$ for any $g \in G \setminus \{e\}$. Thus, each of the pairs $\{g, g^{-1}\}$ for $g \neq e$ contains 2 elements, and every element in $G \setminus \{e\}$ appears in exactly one such pair. This is a contradiction, since $G \setminus \{e\}$ contains an odd number of elements. $\qquad\square$

Example. The only groups of order 6 are the cyclic group C_6 and the symmetric group S_3.

Let G be a group with $|G| = 6$. The order of each element is either $1, 2, 3, 6$ by Lagrange's Theorem.

If G contains an element of order 6, we immediately have $G \cong C_6$.

If every element of G has order 2, G is abelian. Pick $x, y \in G$, $x, y \neq e$, $x \neq y$. Now, $x^2 = y^2 = (xy)^2 = e$, and $xy = yx$. Thus, $\{1, x, y, xy\} \cong V_4$ is a subgroup of G, which contradicts Lagrange's Theorem.

Thus, pick $x, y \in G$ where x has order 2, y has order 3. Then, $x^2 = e$, $y^3 = e$. The elements $\{e, x, y, y^2, xy, xy^2\}$ are all distinct and hence exhaust G, and we can verify that indeed $G \cong S_3 \cong D_3$.

Note that in the latter case, we must argue that $yx = xy^2$. We do this by noting that $\{e, y, y^2\}$ must be a normal subgroup of G, hence yx must be one of y, xy, xy^2. The first is ruled out since $x \neq e$; the second is ruled out because it implies that $xy = yx$ i.e. G is abelian, forcing xy to have order 6.

2.9   Quotient groups

Definition 2.17. Let $H \trianglelefteq G$, and let G/H be the quotient space defined by the partition of G into the cosets of H. Then, G/H is a quotient group whose elements are the cosets gH for $g \in G$. The group operation is defined as

$$(xH)(yH) = xyH.$$

Remark. It is easy to verify that this operation is associative. The group identity is the coset H. The inverse of gH is $g^{-1}H$.

Example. The quotient group $\mathbb{Z}/n\mathbb{Z}$ represents the integers modulo n. All integers of the form $nk + m$ have been identified to the same class $[m] = n\mathbb{Z} + m$.

Lemma 2.30. *The map $\pi\colon G \to G/H$, $g \mapsto gH$ where $H \trianglelefteq G$ is a homomorphism.*

Theorem 2.31 (Correspondence)**.** *Let $H \trianglelefteq G$. There is a bijection between the set of subgroups of G containing H, and the subgroups of G/H, given by the map $X \mapsto \pi(X)$.*

Theorem 2.32 (First isomorphism theorem)**.** *If $\varphi\colon G \to G'$ is a homomorphism, then $G/\ker\varphi \cong \operatorname{im}\varphi$.*

Proof. Set $N = \ker\varphi$. Define the map $f\colon G/\ker\varphi \to \operatorname{im}\varphi$ which sends the coset $gN \mapsto \varphi(g)$. It can be shown that this map is well defined, and is a homomorphism. Furthermore, the kernel of f is the singleton set N, hence f is injective. Given any $g' \in \operatorname{im}\varphi$, we can choose $g \in G$ such that $\varphi(g) = g'$, hence $f(gN) = g'$ which shows that f is also surjective. $\qquad\square$

2.10   Group actions

Definition 2.18. Let G be a group and let X be a set. We say that G acts on X if there is a map $G \times X \to X$ sending $(g,x) \mapsto gx$, such that $(e,x) \mapsto x$ and $g(h(x)) = (gh)(x)$ for all $x \in X$, $g, h \in G$.

Remark. Fix $g \in G$. Then the map $x \mapsto gx$ is a bijection.

Example. The left multiplication map $G \times G \to G$, $(g,h) \mapsto gh$ is a group action.

Example. The conjugation map $G \times G \to G$, $(g,h) \mapsto ghg^{-1}$ is also a group action.

Definition 2.19. The orbit of $x \in X$ is the set $Gx = \{gx : g \in G\}$.

Consider the equivalence relation on X where $x \sim y$ if there exists $g \in G$ such that $x = gy$. This induces a partition of X. The equivalence class of $x \in X$ is precisely its orbit.

Definition 2.20. The stabilizer of $x \in X$ is the set of all elements $g \in G$ such that $gx = x$. We denote this as G_x.

Lemma 2.33. *The stabilizer of an element in X is a subgroup of G. Thus, $|G_x|$ always divides $|G|$.*

Lemma 2.34. *Let $\mathcal{O} \subseteq X$ be an orbit, and let $x, y \in \mathcal{O}$. Then, $|G_x| = |G_y|$.*

Proof. If $x = gy$, then $G_x = gG_yg^{-1}$. Indeed, $G_x \cong G_y$ since conjugation by an element is an isomorphism. $\qquad\square$

Theorem 2.35 (Orbit-Stabilizer theorem)**.** *Let $\mathcal{O} \subseteq X$ be an orbit, and let $x \in \mathcal{O}$. Then, $|G| = |G_x| \cdot |\mathcal{O}|$.*

Definition 2.21. We say that G acts transitively on X if there is only one orbit, namely X.

Definition 2.22. The center of a group G is the set of elements which commute with every element of G. This can also be characterized as the union of all singleton orbits under the conjugation action.

Lemma 2.36. *The center $Z(G)$ of a group G is a normal subgroup of G.*

Definition 2.23. We say that G is a p-group where p is prime if $|G| = p^n$ for some $n \in \mathbb{N}$.

Lemma 2.37. *The center of a p-group is non-trivial.*

Proof. Let G be a group with $|G| = p^n$. Note that G can be written as the union of $Z(G)$ and those conjugacy classes with more than one element. Let C be a conjugacy class with $|C| > 1$. Then, the orbit-stabilizer theorem guarantees that $|C| = p^k$ for some $1 \le k < n$. Now, $p \,|\, |G|$ and $p \,|\, |C|$ for every other conjugacy class, hence $p \,|\, |Z(G)|$ which forces $|Z(G)| \ge p > 1$. $\quad\square$

Lemma 2.38. *If $G/Z(G)$ is cyclic, then G is abelian.*

Proof. Consider the natural homomorphism $\varphi\colon G \to G/Z(G)$. Let $\bar{x}$ be a generator of $G/Z(G)$, and let $\varphi(x) = \bar{x}$. In other words, $\bar{x} = xZ(G)$. It is easy to see that for any power, $\bar{x}^k = x^k Z(G)$ because $Z(G)$ commutes with every element of G. Thus, every element of $G/Z(G)$ is of this form, so G is a union of all such cosets.

Pick arbitrary $a, b \in G$, and suppose that $a \in x^m Z(G)$ and $b \in x^n Z(G)$. Then we can write $a = x^m z_a$, $b = x^n z_b$ for $z_a, z_b \in Z(G)$. Thus, $ab = x^m z_a x^n z_b = z_a x^{m+n} z_b = z_b x^{m+n} z_a = ba$. $\quad\square$

Theorem 2.39. *A group G with $|G| = p^2$ for some prime p is abelian.*

Proof. Recall that $|Z(G)|$ is either p or p^2, so $|G/Z(G)|$ is either p or 1. This forces it to be cyclic, hence G is abelian. $\square$

Theorem 2.40. *A group G with $|G| = p^2$ is either C_{p^2} or $C_p \times C_p$.*

Proof. If G contains an element of order p^2, we immediately have $G \cong C_{p^2}$. Otherwise, every non-identity element must have order p. Pick non-identity $x \in G$, and let $H = \langle x \rangle$. Next, pick y from $G \setminus H$, and let $K = \langle y \rangle$. Now, both $|H| = |K| = p$, and $H \cap K = \{e\}$. Clearly, $H, K \cong C_p$, hence $H \times K \cong C_p \times C_p$. We now claim that the map $(h, k) \mapsto hk$ is an isomorphism. The fact that this map is a homomorphism follows directly from the fact that G is abelian. The fact that G is injective follows from the fact that the kernel of this map is trivial: to see this, if $(h, k) \mapsto e$, then $hk = e$ or $h = k^{-1}$. Since $H \cap K = \{e\}$, we must have $h = k = e$. $\square$

2.11   Sylow's Theorems

Definition 2.24. Let G be a finite group, and let p be a prime number which divides $|G|$. In other words, $|G| = p^k n$ where $k \geq 1$ is the highest possible power. A p-Sylow subgroup of G is one of order p^k.

Lemma 2.41. *Let p be a prime, and let $n \in \mathbb{N}$. Then,*

$$\binom{p^k n}{p^k} \equiv n \pmod{p}.$$

Proof. Note that for any integer x, we have

$$(1 + x)^p \equiv 1 + x^p \pmod{p}.$$

Again,

$$(1 + x)^{p^2} \equiv ((1 + x)^p)^p \equiv 1 + x^{p^2} \pmod{p}.$$

Repeating,

$$(1 + x)^{p^k} \equiv 1 + x^{p^k} \pmod{p}.$$

Now,

$$(1 + x)^{p^k n} \equiv (1 + x^{p^k})^n \equiv 1 + n x^{p^k} + \binom{n}{2} x^{2p^k} + \cdots + x^{p^k} \pmod{p}.$$

Comparing the coefficients of $x^{p^k n}$ on both sides,

$$\binom{p^k n}{p^k} \equiv n \pmod{p}. \qquad \square$$

Theorem 2.42. *A p-Sylow subgroup always exists.*

Proof. Let X be the set of subsets of G, each of size p^k. The number of such choices are

$$\binom{p^k n}{p^n} \equiv n \pmod{p}.$$

Using the fact that p and n are relatively prime, we see that p does *not* divide $|X|$. Now, let G act on X by left multiplication as follows: for $g \in G$ and $A \in X$, $g \cdot A = gA$. Now, X is precisely the disjoint union of the orbits of its elements. Thus, there must exist an orbit $\mathcal{O} \subseteq X$ such that p does not divide $|\mathcal{O}|$. Pick $A \in \mathcal{O}$, and use the orbit-stabilizer theorem to write

$$|G| = |G_A| \cdot |\mathcal{O}|.$$

Since p^k divides $|G|$ but not $|\mathcal{O}|$, it must divide $|G_A|$, which is a subgroup of G. It remains to show that $p^k = |G_A|$. Note that G_A stabilizes A, and $|A| = p^k$. Fix $a \in A$, and note that $g \in Aa^{-1}$ for all $g \in G_A$ forcing $|G_A| \leq |Aa^{-1}| = p^k$. This completes the proof. $\qquad\square$

Theorem 2.43. *Any two p-Sylow subgroups are conjugate.*

Proof. Let P be a p-group, i.e. $|P| = p^k$, and let P act on a finite set X. Denote X^P as the set of fixed points of X; this is the union of all singleton orbits. Now examine $X \setminus X^P$ – this is the union of all orbits which have more than one element. Furthermore, all orbits are disjoint and the cardinality of each orbit divides $|P| = p^k$. As a result, p divides $|X \setminus X^P|$, hence $|X| \equiv |X^P|$ (mod p). This means that if p does not divide $|X|$, then $|X^P|$ is non-empty, i.e. X has a fixed point.

Let P, Q be two p-Sylow subgroups of G. Note that G acts on G/P (the left cosets of P) in the natural way, and $|G/P| = n$ which is not divisible by p. By considering Q acting on G/P, we see that there is at least one left coset of P, say gP, which is fixed by the action of Q. In other words, for all $q \in Q$, we have $qgP = gP$, hence $(g^{-1}qg)P = P$. This forces $g^{-1}qg \in P$, or $q \in gPg^{-1}$ for all $q \in Q$. This immediately gives $Q = gPg^{-1}$. $\qquad\square$

Corollary 2.43.1. *Any two p-Sylow subgroups are isomorphic.*

Corollary 2.43.2. *A p-Sylow subgroup is normal if and only if it is the only such p-Sylow subgroup.*

Theorem 2.44. *Let s_p be the number of p-Sylow subgroups. Then, $s_p \equiv 1$ (mod p), and $s_p | n$ where $|G| = p^k n$.*

Proof. Let S be the set of p-Sylow subgroups, and let G act on S by conjugation. The previous theorem shows that there is only one orbit, i.e. G acts transitively on S. This means that $|G| = |S| \cdot |G_P|$ for any $P \in S$. Note that G_P is the *normalizer* of P, i.e the set of all $g \in G$

such that $g^{-1}Pg = P$. It is clear that $P \subseteq G_P$, hence $|G_P|$ is some multiple of p^k. This means that $|S| = s_p$ must divide n.

Now by considering the action of P on S, we have $|S^P| \equiv |S| \pmod{p}$. However, it is clear that $|S^P| = 1$, with the only fixed point being P itself. To see this, note that if $Q \in S$ is fixed by P, then $gQg^{-1} = Q$ for all $g \in P$. This means that $P \subseteq G_Q$, but we also know that $Q \subseteq G_Q$. By definition, Q is a normal subgroup in G_Q; the corollary of the second Sylow theorem shows that this is the only Sylow subgroup in G_Q, hence $Q = P$. This gives $s_p \equiv 1 \pmod{p}$.   □

> *Example.* Any group of size 15 is cyclic. To see this, note that if G contains 15 elements, then G has one 3-Sylow subgroup H, and one 5-Sylow subgroup K. Since each of these are unique, they are normal. Also, $H \cap K = \{e\}$, because the intersection of subgroups is itself a subgroup. Furthermore, H and K are cyclic, since they have prime orders. This is enough to show that $G \cong H \times N$, which is also cyclic.

2.12   Simple groups

> **Definition 2.25.** A group is called simple if it contains no normal subgroup apart from $\{e\}$ and G itself.

> *Example.* Groups of of prime order are simple.

> **Lemma 2.45.** *If G is a simple, abelian group, then G is a cyclic group of prime order.*

Proof. Any non-identity element from G generates a normal subgroup of G. Since G is simple, these must all be G itself, hence G is cyclic. Since G contains no cyclic subgroups, the order of G is prime.   □

> **Lemma 2.46.** *If G is a simple p-group, then G is a cyclic group of prime order.*

Proof. The center of G is a normal subgroup – since G is a p-group, the center is non-trivial and hence must be G itself. Thus, G is also abelian, from which the result follows.   □

> **Lemma 2.47.** *If $|G| = p^2 q$ for primes p, q, then G is not simple.*

> **Theorem 2.48** (Burnside)**.** *No group of the form $p^\alpha q^\beta$ is simple.*

> **Lemma 2.49.** *Let H be a subgroup of a simple group G, with $[G : H] = n \geq 3$. Then, $|G| \leq n!$.*

Proof. Let G act on $X = G/H$; then each element $g \in G$ gives a permutation of X (each left coset is sent to another left coset). This gives a homomorphism $\varphi \colon G \to S_n$. Now, we claim that the normal subgroup $\ker G$ is a proper subgroup. To see this, pick $g \in \ker G$, hence g is the identity permutation, $gx = x$ for all $x \in X$. Choose $x = H$, hence $gH = H$ or $g \in H$. Thus, $\ker G \subseteq H$ which is a proper subgroup of G. Since G is simple, this forces $|\ker G| = 1$, i.e. φ is injective. Thus, $|G| \leq |S_n| = n!$. $\qquad\square$

Theorem 2.50. *The group A_5 is the smallest non-abelian simple group, with order 60.*

Theorem 2.51. *The groups A_n for $n \geq 5$ are simple.*

Proof. We show this by induction. Note that A_5 is simple; now suppose that A_{n-1} is simple. Realize A_{n-1} as a subgroup of A_n, being a certain subset of the permutations of $\{1, \ldots, n\}$. Observe that A_{n-1} is a maximal subgroup of A_n. This will follow from the following claim: if $t \in A_n \setminus A_{n-1}$, then $A_n = A_{n-1} \cup A_{n-1}tA_{n-1}$. To show this, let $t \in A_n \setminus A_{n-1}$, i.e. $t(n) = m$, $m \neq n$, and let $s \in A_n$. If $s(n) = n$, then $s \in A_{n-1}$; otherwise if $s(n) = k$, $k \neq n$, then let p, q be distinct from n, m, k. Set $a = (k\,m)(p\,q) \in A_{n-1}$: now the composition $t^{-1}as$ sends $n \to k \to m \to n$, hence $t^{-1}as = b \in A_{s-1}$. In other words, $s = atb \in A_{n-1}tA_{n-1}$.

Now, suppose that $N \trianglelefteq A_n$; it follows that $N \cap A_{n-1} \trianglelefteq A_{n-1}$. This will $N \cap A_{n-1}$ to be either $\{e\}$ or A_{n-1}; the latter is not normal in A_n. In either case, it will follow that N is trivial. $\qquad\square$

Updated on November 10, 2021