GROUP THEORY

SIDDHANT CHAUDHARY

Abstract. In this document I discuss topics in Group Theory and also include solutions to selected exercises from the book *Abstract Algebra* by *David Steven Dummit* and *Richard M.Foote*.

1. Exercise on Page 21

11. Consider $(\mathbb{Z}/12\mathbb{Z})^+$. We have that $|0| = 1$. Let $k \neq 0$ be in the group. Let $m = |k|$. Then, we have that

$$km \equiv 0 \pmod{12}$$

So, finding orders is pretty straight-forward: if $(k, 12) = 1$, then $|k| = 12$. If $(k, 12) > 1$, then $|k| = \frac{12}{(k,12)}$. In general, for any $k \in (\mathbb{Z}/m\mathbb{Z})^+$, we have

$$|k| = \frac{m}{(m, k)}$$

15. Let G be a group. Then, if a_1, a_2 ... a_n are in G, then

$$(a_1a_2...a_n)^{-1} = a_n^{-1}a_{n-1}^{-1}...a_1^{-1}$$

Proof: We prove this by strong induction. The base case $n = 1$ is trivially true. So, let the statement be true for all naturals upto some $n \in \mathbb{N}$. Let a_{n+1} be an additional element of G. Then,

$$\begin{aligned}(a_1a_2...a_na_{n+1})^{-1} &= ((a_1a_2...a_n)a_{n+1})^{-1} \\ &= a_{n+1}^{-1}(a_1a_2...a_n)^{-1} && \text{(Statment is true for } k = 2) \\ &= a_{n+1}^{-1}a_n^{-1}...a_1^{-1} && \text{(Statment is true for } k = n)\end{aligned}$$

So, by induction, the claim follows.

22. Let x and g be elements of a group G. Let $|x| = k$ and $|g^{-1}xg| = m$, where $k, m \in \mathbb{N}$. Now,

$$\begin{aligned}(g^{-1}xg)^k &= g^{-k}x^kg^k \\ &= g^{-k}g^k \\ &= 1\end{aligned}$$

This implies that $m \leq k$. Also, we have

$$\begin{aligned}(g^{-1}xg)^m = g^{-m}x^mg^m = 1 \\ \implies x^mg^m = g^m \\ \implies x^m = 1\end{aligned}$$

which means that $k \leq m$. Combining both the inequalities, we see that $k = m$.

Date: August 2019.

Now, let a and b be in G. Set $x = ab$, and set $g = a$. Then,

$$|x| = |g^{-1}xg|$$

which means that

$$|ab| = |a^{-1}aba| = |ba|$$

which proves the claim.

23. Let x be an element of G such that $|x| = n < \infty$ for some $n \in \mathbb{N}$. Suppose $n = st$, for some s and t in $\mathbb{N}$. Let $|x^s| = m$ for some $m \in \mathbb{N}$. The reason why $|x^s| < \infty$ is because

$$(x^s)^n = x^{sn} = x^{ns} = (x^n)^s = 1$$

and then apply the WOP.

Since $(x^s)^t = 1$, we immediately know that $m \leq t$. But, $(x^s)^m = 1$, which means that $st \leq sm$. From here, it is clear that $m = t$, and thus the claim follows.

25. Suppose G is a group such that $x^2 = 1$ for every $x \in G$. This means that $x^{-1} = x$ for all $x \in G$.

Let a and b be in G. By **15**, we know that

$$(ab)^{-1} = b^{-1}a^{-1} = ba$$

So, it follows that $ab = ba$, which proves that G is abelian.

30. Let A and B be two groups. Observe that

$$(a, 1)(1, b) = (a, b) = (1, b)(a, 1)$$

and hence the elements $(a, 1)$ and $(1, b)$ commute. Now, let $k = |(a, b)|$, $n_1 = |a|$, $n_2 = |b|$, and define $m = [n_1, n_2]$ (lcm).

Now, it follows that

$$(a, b)^k = (a^k, b^k) = (1, 1)$$

which means that $a^k = 1$ and $b^k = 1$, which means that $n_1|k$ and $n_2|k$, which means that $m|k$. Similarly, observe that

$$(a, b)^m = (a^m, b^m) = (1, 1)$$

which means that k_m. Hence, $k = m$.

31. Suppose G is a finite group of even order. Let $t(G)$ be the set of all $g \in G$ such that $g \neq g^{-1}$. It is clear that $1 \notin t(G)$. Also, for any $g \in t(G)$, g^{-1} is also in $t(G)$, and hence $t(G)$ has even order. Hence, it follows that the set $G - t(G)$ contains even number of elements, and hence there is an element of order 2 in the group.

32. Suppose X is a non-identity element of order n in G. We will show that the elements $1, x, ..., x^{n-1}$ are all distinct. Suppose there are $0 \leq k_1 < k_2 \leq n-1$ such that $x^{k_1} = x^{k_2}$. So, it follows that $x^{k_2-k_1} = 1$, which contradicts the fact that $\text{ord}(x) = n$. So, the elements are all distinct, and hence $|x| \leq |G|$.

2. Dihedral Group D_{2n}

The *Dihedral* group of order $2n$, denoted by D_{2n}[1], is the group of symmetries of a polygon with n vertices. We can explicitly write it as:

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

with the following properties:

- $r^n = 1$
- $s^2 = 1$
- $rs = sr^{-1}$, which means that it is a non-abelian group.
- $r^i s = sr^{-i}$

Intuitively, r denotes a clockwise rotation by an angle of $\frac{2\pi}{n}$ radians, and s denotes the reflection about the axes of symmetry passing through the vertex named 1. Note that as these are just permutations of the set $\{1, 2, 3, 4....n\}$, we can specify the effects of r and s:

$$\{1, 2, 3, 4, ..., n\} \xrightarrow{r} \{n, 1, 2, 3, ..., n-1\}$$
$$\{1, 2, 3, 4, ..., n\} \xrightarrow{s} \{1, n, n-1, n-2, ..., 2\}$$

From these relations, note that any element of D_{2n} can be written as $s^k r^i$, where $k \in \{0, 1\}$ and $1 \leq i \leq n-1$.

3. Exercises on Page 27

1. Here we will compute the order of a general element in the group D_{2n}. If $g = r^k$, for some $0 \leq k \leq n$, then

$$\text{ord}(g) = \frac{n}{(n, k)}$$

If $g = sr^k$, for some $0 \leq k \leq n-1$, and if g is the non-identity element, then

$$\text{ord}(g) = 2$$

2. Suppose x is any element of D_{2n}. Then, using the generators and relations, we see that x is either of the form r^k or sr^k. So, suppose $x = sr^k$ for some integer k. Then, observe that

$$rx = r(sr^k) = (rs)r^k = (sr^{-1})r^k = xr^{-1}$$

3. Consider the group $D_{2n} = \langle r, s \,|\, r^n = 1, s^2 = 1, rs = sr^{-1} \rangle$. Let $x \in D_{2n}$ such that $x = r^i s^j$, for some $i, j \in \mathbb{N}$. Since the order of r is n and the order of s is 2, we can make the restrictions

$$0 \leq i \leq n-1$$
$$0 \leq j \leq 1$$

[1]In some sources this group is denoted by D_n, but our notation is better because it specifies the order of the group.

So, any element of D_{2n} which is not a power of r can be written in the form $r^i s$, where $0 \leq i \leq n-1$. Now, we have

$$\begin{aligned}(r^k s)(r^k s) &= r^k(sr^k)s \\ &= r^k(r^{-k}s)s \\ &= (r^k r^{-k})s^2 \\ &= 1\end{aligned}$$

which means that the order of x is 2 (it clearly cannot be 1). We can use this fact to easily compute the order of every element in D_{2n} as follows: if x is not a power of r, then its order is 2. If $x = r^k$, for some $0 \leq k \leq n-1$, then the order of x is simply $\frac{n}{(k,n)}$.

Observe that $ssr = r$, which means that all powers of r can be generated by s and sr. It follows that the group is generated by s and sr.

4. Suppose $n = 2k$ where $n \geq 4$. Then, r^k is an element of order 2 in the group D_{2n}. Now, suppose x is any element of D_{2n}. If $x = r^{k_1}$, for some k_1, then x trivially commutes with r^k. If $x = sr^{k_1}$, then observe that

$$r^k x = r^k(sr^{k_1}) = (r^k s)r^{k_1} = (sr^k)r^{k_1} = xr^k$$

and hence x commutes with r^k. So, r^k commutes with all elements of the group D_{2n}. This is infact the only non-identity element which commutes with all other elements, which is not hard to prove.

6. Suppose x and y are elements of order 2 in a group G. Suppose $t = xy$. Observe that

$$tx = (xy)x = x(yx) = xt^{-1}$$

7. Consider the group with presentation $\langle a, b | a^2 = b^2 = (ab)^n = 1\rangle$. We will show that this is a presentation of D_{2n}.

First, consider the usual presentation of D_{2n}. Put $a = s$ and $b = rs$. Then, it is clear that $a^2 = b^2 = 1$. Also, $ab = srs = r^{-1}$, and hence $(ab)^n = 1$. So, the elements a and b also generate the group, and hence $\langle a, b | a^2 = b^2 = (ab)^n = 1\rangle$ is a valid presentation of the group.

Now, consider the given group presentation. Put $s = a$ and $r = ab$. Then, $sr = b$, and hence s, r generate the given group. Also, $s^2 = 1$, and $r^n = 1$, and so this presentation represents the group D_{2n}.

18. Suppose $Y = \langle u, v |\, u^4 = v^3 = 1, uv = v^2u^2\rangle$. We will show that this represents the trivial group through the following exercises:

(a) Since $v^3 = 1$, we have $vv^2 = 1$, and hence $v^{-1} = v^2$.

(b)

4. Exercises on Page 32

1. The cycle decompositions of σ and τ are given by

$$\sigma = (1\ 3\ 5)(2\ 4)$$
$$\tau = (1\ 5)(2\ 3)$$

So, the cycle decompositions of the following permutations are:

: $\sigma^2 = (1\ 5\ 3)$

: $\sigma\tau = (2\ 5\ 3\ 4)$

: $\tau\sigma = (1\ 2\ 4\ 3)$
: $\tau^2\sigma = (1\ 3\ 5\ 2\ 4)$

4. First, lets list the elements of S_3: 1, (2 3), (1 2), (1 2 3), (1 3 2), (1 3). Now, the orders of the elements are given in the following table:

1	1
(2 3)	2
(1 2)	2
(1 2 3)	3
(1 3 2)	3
(1 3)	2

5. Consider the cycle product (1 12 8 10 4)(2 13)(5 11 7)(6 9). If we multiply this cycle product by itself, notice what product we get:

$$((1\ 12\ 8\ 10\ 4)(2\ 13)(5\ 11\ 7)(6\ 9))^2 = (1\ 8\ 4\ 10\ 12)(5\ 7\ 11)$$

We observe that the elements within a cycle remain in the cycle, so it follows that the order of this cycle product is the lcm of the orders of each cycle. In this case, the lcm is $[5, 2, 3, 2] = 30$. Also, we can make the following conjecture: The order of a cycle $(a_1\ a_2\ ...\ a_n)$ is equal to the order of the cycle $(1\ 2\ ...\ n)$, which is equal to n.

Using this, we can compute the order of any cycle product.

6. Consider an element $\sigma \in S_4$ of order 4. By our previous conjecture (which seems to be true), the only way σ can have order 4 is if its length is 4. So, such σ are: (1 2 3 4), (1 2 4 3), (1 3 2 4), (1 3 4 2), (1 4 2 3), (1 4 3 2)

8. We show that there are infinitely many bijections from Ω to Ω. For $k \in \mathbb{N}$, define

$$f_k(n) = \begin{cases} k, & \text{if } n = 1 \\ 1, & \text{if } n = k \\ n & \text{otherwise} \end{cases}$$

It is not hard to see that f_k is a bijection. It follows that S_Ω is an infinite group.

9. I have this conjecture: suppose σ is the m-cycle given by $(a_1\, a_2\, ...\, n)$. Then, σ^i consists of $\dfrac{m}{(m,i)}$ disjoint cycles, each of length (m, i). So, σ^i is an m cycle if and only if i is relatively prime to m.

Using this conjecture, we can immediately solve this problem. In problem **11**, we will partially prove this conjecture.

10. Now we will prove that if σ is an n cycle, then $|\sigma| = n$. Suppose σ is given by $\sigma = (a_0\, a_2\, ...\, a_{n-1})$. Then, it is not hard to see that $\sigma^i(a_k) = a_{k+i}$, where $k + i$ is reduced mod n. So, for any element a_k, $\sigma^i(a_k) = a_k$ if and only if $i + k = k \bmod n$. The least positive integer for which this is true if $i = n$. Hence, $|\sigma| = n$.

11. Here, we will prove a general result. Suppose σ is an n-cycle given by $\sigma = (a_0\, ...\, a_{n-1})$. Let i be an integer. Then, σ^i consists of (n, i) cycles, each of length $\dfrac{n}{(n,i)}$. The proof is as follows: suppose a_k is a fixed element. Then, the cycle in which this fixed element lies under the action of σ^i is $(a_k\, a_{k+i}\, a_{k+2i}\, ...\, a_{k+(l-1)i})$, where $l = \dfrac{n}{(n,i)}$. So, it follows that there are (n, i) cycles, each of length $\dfrac{n}{(n,i)}$.

Using this fact, it follows that σ^i is an n-cycle if and only if $(n, i) = 1$.

12. This problem can be done by using the statement proved in the previous problem.

15. Here I'll only explain the proof strategy. The key fact we have to use here is: disjoint cycles commute, and if a, b are commuting elements of a group G, then $(ab)^n = a^n b^n$. Also, we know that the order of an m-cycle is m. Using these facts, the statement is not difficult to prove.

20. We know that every permutation can be represented as a product of transpositions. Also, the order of a transposition is 2. So, a presentation for S_3 is

$$S_3 = \langle a, b, c | a^2 = b^2 = c^2 = 1 \rangle$$

where a, b, c are the three transpositions.

5. Exercises on Page 35

2. All elements of $GL_2(\mathbb{F}_2)$ are:

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

5. It is clear that if F has finite number of elements, then $GL_n(F)$ only has finite number of elements. Also, if F has infinitely many elements, then $GL_n(F)$ also has infinitely many elements: we can just make infinitely many diagonal matrices, such that the diagonal entries are non-zero. Hence, we are done.

6. Suppose $|F| = q$. We will show that $|GL_n(F)| < q^{n^2}$. There are q^{n^2} possible matrices over the field F. Also, we know that the zero matrix is not in $GL_n(F)$. Hence, the claim follows.

6. Exercises on Page 39

1. Let $\phi : G \to H$ be a homomorphism.

(a) We show that $\phi(x^n) = \phi(x)^n$ for all $n \in \mathbb{N}$, and $x \in G$. The case $n = 1$ is trivial. Also, observe that

$$\phi(x^{n+1}) = \phi(x^n \cdot x) = \phi(x^n)\phi(x) = \phi(x)^{n+1}$$

and hence the claim follows by induction.

(b) Now, observe that

$$\phi(xx^{-1}) = \phi(x)\phi(x^{-1}) = \phi(1_G) = 1_H$$

and hence

$$\phi(x^{-1}) = \phi(x)^{-1}$$

and hence it follows that

$$\phi(x^n) = \phi(x)^n$$

for all $n \in \mathbb{Z}$.

2. Suppose $\phi : G \to H$ is an isomorphism, and let $x \in G$. Consider the element $x \in G$ and $\phi(x) \in H$. Suppose $\text{ord}(x) = p$ and $\text{ord}(\phi(x)) = q$ in the respective groups.

Now, observe that

$$\phi(x)^p = \phi(x^p) = \phi(1_G) = 1_H$$

and hence $q|p$. Similarly, we have

$$\phi(x^q) = \phi(x)^q = 1_H$$

and since ϕ is an isomorphism, it follows that $x^q = 1_G$, and hence $p|q$. So, $p = q$, and the claim follows.

No, the result may not be true if ϕ is assumed to be only a homomorphism. For instance, let ϕ be the trivial homomorphism, i.e suppose $\phi(x) = 1_H$ for every $x \in G$. Then, for every element $x \in G$, $\text{ord}(\phi(x)) = 1$.

3. Suppose $\phi : G \to H$ is an isomorphism. We show that G is abelian if and only if H is abelian. Suppose G is abelian. Suppose $y_1, y_2 \in H$. Then, there are x_1, x_2 in G such that $y_1 = \phi(x_1)$ and $y_2 = \phi(x_2)$. Now,

$$y_1y_2 = \phi(x_1)\phi(x_2) = \phi(x_1x_2) = \phi(x_2x_1) = \phi(x_2)\phi(x_1) = y_2y_1$$

and hence H is abelian. Similarly, we can show that G is abelian if H is abelian, and hence the claim follows. If we only assume that ϕ is a homomorphism and G is abelian, then if ϕ is surjective, then H will also be abelian.

4. To show that $\mathbb{R} - \{0\}$ and $\mathbb{C} - \{0\}$ are not isomorphic, it is enough to observe that $\mathbb{C} - \{0\}$ contains an element of order 4, while $\mathbb{R} - \{0\}$ does not have any element of order 4.

5. To see why the additive groups $\mathbb{R}$ and $\mathbb{Q}$ are not isomorphic, it is enough to observe that there can be no bijection between $\mathbb{R}$ and $\mathbb{Q}$.

6. To see that the additive groups $\mathbb{Z}$ and $\mathbb{Q}$ are not isomorphic, observe that $\mathbb{Q}$ contains an element of order 2, which is $\frac{1}{2}$. However, $\mathbb{Z}$ does not have any element of order 2.

7. To see that D_8 and Q_8 are not isomorphic, it is enough to observe that D_8 has four elements of order 2, while Q_8 has only two elements of order 2.

9. To see that D_{24} and S_4 are not isomorphic, it is enough to observe that D_{24} contains an element of order 12, while S_4 doesn't.

10. Suppose Δ and Ω are two sets in bijection, and let θ be the bijection. We prove that the groups S_Δ and S_Ω are isomorphic.

(a) Let $\sigma \in S_\Delta$. Consider the map $\theta \circ \sigma \circ \theta^{-1}$, which is a map from Ω to Ω. We show that this map is a bijection, and hence it is a permutation of Ω. It is clearly injective, because θ, σ and θ^{-1} are all injective. To show that this is surjective, let $y \in \Omega$, and consider the element $x = \theta\sigma^{-1}\theta^{-1}(y)$, which is also in Ω. Also, $\theta\sigma\theta^{-1}(x) = y$, and hence this map is also surjective. Hence, it is bijective, and hence a permutation.

(b) So we define $\phi : S_\Delta \to S_\Omega$ by $\phi(\sigma) = \theta\sigma\theta^{-1}$. Now, we define a map $\chi : S_\Omega \to S_\Delta$ by $\chi(\sigma) = \theta^{-1}\sigma\theta$. We show that $\chi\phi$ is the identity map, and so is $\phi\chi$. Observe that

$$\chi\phi(\sigma) = \theta^{-1}(\theta\sigma\theta^{-1})\theta = \sigma$$

and similarly $\phi\chi$ is the identity. So, a two-sided inverse has been found for ϕ, and hence ϕ is a bijection.

13. Suppose $\Phi : G \to H$ is a homomorphism. We will show that $\Phi(G)$ is a subgroup of H. First, observe that $\Phi(1_G) = 1_H$, and hence $1_H \in \Phi(G)$. Second, suppose $x_1, x_2 \in \Phi(G)$. So, there are y_1, y_2 in G such that $\Phi(y_1) = x_1$ and $\Phi(y_2) = x_2$. Then, $\Phi(y_1 y_2) = x_1 x_2$, and hence $x_1 x_2 \in \Phi(G)$. Finally, suppose $x \in \Phi(G)$. Then, there is some $y \in G$ such that $x = \Phi(y)$. Observe that $x\Phi(y^{-1}) = 1_H$, and hence $x^{-1} \in \Phi(G)$. So, $\Phi(G)$ is a subgroup of H.

Further, suppose that Φ is injective. Consider the map $\chi : G \to \Phi(G)$ given by $\chi(x) = \Phi(x)$, for $x \in G$. Clearly, χ is both one-one and onto, because Φ is injective. Also, because Φ is a homomorphism, χ is also a homomorphism. So, it follows that $G \cong \Phi(G)$.

14. Suppose $\Phi : G \to H$ is a homomorphism. We will show that $\mathrm{Ker}\Phi$ is a subgroup of G. Clearly, $\Phi(1_G) = 1_H$, and hence $1_G \in \mathrm{Ker}\Phi$. If $x_1, x_2 \in \mathrm{Ker}\Phi$, then so is $x_1 x_2$. Finally, if $x \in \mathrm{Ker}\Phi$, then $\Phi(x) = 1_H$. But, $\Phi(x^{-1}) = \Phi(x)^{-1} = 1_H$, and hence $x^{-1} \in \mathrm{Ker}\Phi$. So, $\mathrm{Ker}\Phi$ is a subgroup of G.

The fact that Φ is one-one if and only if $\mathrm{Ker}\Phi$ is the identity subgroup of G is exactly similar to the corresponding statement for linear maps in vector spaces.

17. Suppose G is a group and consider the map from G to itself defined as $g \mapsto g^{-1}$. We will show that this map is a homomorphism if and only if G is abelian.

First, suppose G is abelian, and let the map be ϕ. Then,

$$\phi(xy) = y^{-1}x^{-1} = x^{-1}y^{-1} = \phi(x)\phi(y)$$

and hence ϕ is a homomorphism.

Conversely, suppose ϕ is a homomorphism. Let x, y be two elements of G. Then, by our assumption, we have

$$x^{-1}y^{-1} = y^{-1}x^{-1}$$

and taking inverses on both sides, we get $xy = yx$, and hence G is abelian.

19. Let $G = \{z \in \mathbb{C} | z^n = 1 \text{ for some } n\}$. Consider the map $z \to z^k$, where the integer $k > 1$ is fixed. It is clear that this map is a homomorphism. Also, it is not hard to see that this map is a surjective homomorphism. However, since $k > 1$, there are more than one $z \in G$ for which $z^k = 1$, and hence the kernel of this map is not the identity subgroup. So, it is not an isomorphism.

20. Let G be a group, and let $\mathrm{Aut}(G)$ be the set of all *automorphisms* of G. We will show that $\mathrm{Aut}(G)$ is also a group, and we will call this the *automorphism group* of G.

Suppose ϕ, χ are two automorphisms of G. Let x, y be elements of G. Then,

$$\phi(\chi(xy)) = \phi(\chi(x)\chi(y)) = \phi(\chi(x))\phi(\chi(y))$$

which implies that $\phi \circ \chi$ is a homomorphism from G to G. Since both χ and ϕ are bijective, $\phi \circ \chi$ is also bijective, and hence $\phi \circ \chi \in \mathrm{Aut}(G)$. Now, the identity automorphism of G forms the identity element of $\mathrm{Aut}(G)$. Finally, suppose $\phi \in \mathrm{Aut}(G)$. Then, ϕ^{-1} is also in $\mathrm{Aut}(G)$, which is not hard to see. Hence, $\mathrm{Aut}(G)$ forms a group under function composition.

21. Consider the additive group $\mathbb{Q}$, and let $k \in \mathbb{Q} - \{0\}$. Consider the map $q \mapsto kq$, and call this map ϕ. We will show that ϕ is an automorphism.

First, observe that $\text{Ker}\phi = \{0\}$, and hence ϕ is one-one. Since $k \neq 0$, this map is also onto. Finally, observe that

$$\phi(q_1 + q_2) = k(q_1 + q_2) = kq_1 + kq_2 = \phi(q_1) + \phi(q_2)$$

which means that ϕ is a homomorphism. Hence, ϕ is an automorphism.

7. Group Actions

In this section we will discuss a bit about group actions. Given a group G and a set A, a *group action* is a map from $G \times A$ to A, which has the following properties:

(1) $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$ for all $g_1, g_2 \in G$ and $a \in A$.
(2) $1 \cdot a = a$ for all $a \in A$.

The above action might as well be called a *left-action*. We can define a *right action* in a similar way. One of the best examples of a group action is scalar multiplication of vectors in vector space theory.

Let's prove two important properties of group actions:

Theorem 7.1. Suppose G is a group acting on a set A. For $g \in G$, define $\sigma_g : A \to A$ by

$$\sigma_g(a) = g \cdot a$$

Then, $\sigma_g \in S_A$, or, in simpler words, σ_g is a permutation of A.

Proof: We will show that σ_g is a bijective map. First, suppose $\sigma_g(a) = \sigma_g(b)$, which means that $g \cdot a = g \cdot b$. So, it follows that $g^{-1} \cdot (g \cdot a) = g^{-1} \cdot (g \cdot b)$, which implies that $a = b$, and hence σ_g is one-one. Next, suppose $a \in G$. Consider the element $g^{-1} \cdot a$. Observe that

$$\sigma_g(g^{-1} \cdot a) = a$$

and hence σ_g is onto. Hence, it is a bijection, and it follows that $\sigma_g \in S_A$.

Theorem 7.2. The map $\phi : G \to S_A$ given by $\phi(g) = \sigma_g$ is a homomorphism.

Proof: Suppose $g_1, g_2 \in G$. We want to show that $\phi(g_1 g_2) = \phi(g_1) \circ \phi(g_2)$. So, suppose $a \in A$. Then,

$$\begin{aligned}
\phi(g_1 g_2)(a) &= (g_1 g_2) \cdot a \\
&= g_1 \cdot (g_2 \cdot a) \\
&= \phi(g_1)(g_2 \cdot a) \\
&= \phi(g_1)(\phi(g_2)(a)) \\
&= \phi(g_1) \circ \phi(g_2)(a)
\end{aligned}$$

We can also define the kernel of a group action. Suppose G is a group acting on a set A. Then, the kernel of the action is defined to be the set $\{g \in G : g \cdot a = a \text{ for all } a \in G\}$. If $\phi : G \to S_A$ is the corresponding homomorphism, then the kernel of the action is the kernel of ϕ.

8. Exercises on Page 44

4. Suppose G is a group acting on a set A, and let $a \in A$ be fixed.

(a) First we will show that the kernel of the action is a subgroup of G. We have that

$$\text{kernel} = \{g \in G | g \cdot a = a\}$$

Cleary, $1 \in$ kernel. Suppose $g_1, g_2 \in$ kernel. Then, for any $a \in A$, we have

$$(g_1 g_2) \cdot a = g_1 \cdot (g_2 \cdot a) = g_1 \cdot a = a$$

and hence $g_1 g_2 \in$ kernel. Finally, suppose $g \in$ kernel. Observe that for any $a \in A$, we have

$$g^{-1} \cdot a = g \cdot (g^{-1} \cdot a) = (gg^{-1}) \cdot a = 1 \cdot a = a$$

which implies that $g^{-1} \in$ kernel, and hence kernel is a subgroup of G.

(b) Let's call the set $\{g \in G | g \cdot a = a\}$ the *stabilizer* of a (here a is fixed). We will show that this is also a subgroup of G. Clearly, $1 \in \text{Stab}(a)$. If $g_1, g_2 \in \text{Stab}(a)$, then $g_1 g_2 \in \text{Stab}(a)$, because

$$(g_1 g_2) \cdot a = g_1 \cdot (g_2 \cdot a) = g_1 \cdot a = a$$

Finally, if $g \in \text{Stab}(a)$, then similar to what we did in part **(a)**, we see that $g^{-1} \in \text{Stab}(a)$ as well. Hence, $\text{Stab}(a)$ is also a subgroup of G.

5. We already showed that the kernel of an action is the kernel of the corresponding permutation representation of the group.

6. Suppose G acts on A faithfully. So, the permutation representation is one-one, which means that the kernel of the permutation representation is $\{1\}$, which means that the kernel of the action is $\{1\}$.

Conversely, if the kernel of the group action is $\{1\}$, then the corresponding permutation representation is one-one, and hence the group action is faithful.

17. Suppose G is a group acting on itself by conjugation. For $g \in G$, we define the map $\sigma_g : G \to G$ by

$$\sigma_g(x) = gxg^{-1}$$

We already know that this map is a bijection. We will show that this is also a homomorphism, which will in turn show that this is an automorphism.

If $a, b \in G$, then observe that

$$\begin{aligned} \sigma_g(ab) &= g(ab)g^{-1} \\ &= (gag^{-1})(gbg^{-1}) \\ &= \sigma_g(a)\sigma_g(b) \end{aligned}$$

and hence the map is an automorphism. So, it follows that for any $x \in G$, $|x| = |gxg^{-1}|$. Also, it follows that for any subset A of G, $|A| = |gAg^{-1}|$.

18. Suppose H is a group acting on a set A. Define a relation $\sim$ on A as

$$a \sim b \text{ iff. } a = h \cdot b \text{ for some } h \in H$$

We will show that this is an equivalence relation. Clearly, the relation is reflexive, because $a = 1 \cdot a$. If $a = h \cdot b$, then $b = h^{-1} \cdot a$, which means that the relation is symmetric. Finally, if $a = h_1 \cdot b$ and $b = h_2 \cdot c$, then $a = (h_1 h_2) \cdot c$, which means that the relation is also transitive. Hence, it is an equivalence relation, and the set A can be partitioned into equivalence classes.

19. Here we will prove a general version of *Lagrange's theorem*. Let H be a subgroup of a group G, and let H act on G by left-multiplication. Let x be a fixed element of G, and let O be the orbit of x under the group action (the orbit is another word for the equivalence class to which x belongs). Consider the map $\phi : H \to O$ given by $\phi(h) = hx$. We will show that this is a bijection.

If $\phi(h_1) = \phi(h_2)$, then $h_1x = h_2x$, and hence $h_1 = h_2$, so that ϕ is one-one. The map is clearly surjective. Hence, it is bijective.

If G is finite, then it follows that all orbits have cardinality $|H|$, and since the orbits partition G, it follows that $|H|$ divides $|G|$, which is Lagrange's theorem.

9. Exercises on Page 48

5. Let G be a group, where $n = |G| > 2$. We will show that there can't by any subgroup H of order $n-1$. Suppose H is a subgroup of order $n-1$, and let $a \in G - H$. Let $x \in G$ such that $x \neq 1$ and $x \neq a$ (this is possible because $n > 2$). So, it follows that $x \in H$. Now, $ax \in G$, and since $x \neq 1$, it follows that $ax \in H$. But, this means that $axx^{-1} \in H$, which is a contradiction. Hence, such an H cannot exist.

In this problem, we can directly use Lagrange's theorem as well.

6. Let G be an abelian group, and consider the *torsion* subgroup of G, which is the set $T := \{g \in G| \ |g| < \infty\}$. We will prove that this is a subgroup. Clearly, $1 \in T$. If $g_1, g_2 \in T$, then $g_1g_2 \in T$, because for any k, $(g_1g_2)^k = g_1^k g_2^k$. Finally, it is easy to see that T is closed under inverses. So, T is a subgroup.

8. Let H and K be subgroups of G. We will show that $H \cup K$ is a subgroup if and only if either $H \subseteq K$ or $K \subseteq H$. First, if either $H \subseteq K$ or $K \subseteq H$, then it is clear that $H \cup K$ is a subgroup. Next, if neither of $H \subseteq K$ or $K \subseteq H$ is true, then take $a \in H - K$ and $b \in K - H$. So, it follows that $a^{-1} \in H - K$ and $b^{-1} \in K - H$. Consider the element $ab \in G$. We show that $ab \notin H \cup K$, implying that $H \cup K$ is not a subgroup. If $ab \in H \cup K$, then without loss of generality suppsose $ab \in H$, which implies that $b \in H$, a contradiction. So, both sides of the claim have been proved.

10. (b) Let G be a group, and let $\{H_\alpha\}_{\alpha \in I}$ be an arbitrary non-empty collection of subgroups of G. We show that

$$M = \bigcap_{\alpha \in I} H_\alpha$$

is also a subgroup. Clearly, $1 \in M$. Next, if $a \in M$, then trivially $a^{-1} \in M$. Similary, if $a, b \in M$, then $ab \in M$, and hence M is a subgroup.

15. Suppose $H_1 \leq H_2 \leq ...$ be an ascending chain of subgroups of G. We will show that $M = \cup_{i=1}^{\infty} H_i$ is a subgroup of G. It is clear that $1 \in M$. Next, suppose $a, b \in M$. Then, there are $k_1, k_2 \in \mathbb{N}$ such that $a \in H_{k_1}$ and $b \in H_{k_2}$. Without loss of generality suppose $H_{k_1} \leq H_{k_2}$. Then, $a, b \in H_{k_2}$, and hence $ab \in H_{k_2}$, which implies $ab \in M$. It is clear that M is closed under inverses. So, M is a subgroup.

10. Centralizers, Normalizers, Stabilizers and Kernels

Centralizers: Suppose G is a group, and let A be a subset of G. Then, the *centralizer* $C_G(A)$ of A is defined as the set of all elements of G which commute with all elements of A, i.e

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

It is not difficult to see that this is a subgroup of G. With this definition, the set $Z(G) := C_G(G)$ is called the *center* of the group G.

Normaliszers: Suppose G is a group, and let $A \subseteq G$. For $g \in G$, define $gAg^{-1} := \{gag^{-1} |\ a \in A\}$. The *normalizer* of A, denoted by $N_G(A)$, is defined as

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

Let's prove that $N_G(A)$ is a subgroup of G. Since $1A1 = A$, it follows that $1 \in N_G(A)$. Next, suppose $g_1 \in N_G(A)$. Then, $g_1Ag_1^{-1} = A$. We will show that $g_1^{-1}Ag_1 = A$, which will show that $N_G(A)$ is closed under inverses. Suppose $a \in A$. Then, there is some $b \in A$ for which $g_1bg_1^{-1} = a$, which means that $g_1^{-1}ag_1 = b \in A$, and hence $g_1^{-1}Ag_1 \subseteq A$. Second, suppose $a \in A$. Then, let $b = g_1ag_1^{-1}$, which means that $b \in A$. Clearly, $g_1^{-1}bg_1 = a$, and hence $A \subseteq g_1^{-1}Ag_1$. So, $A = g_1^{-1}Ag_1$.

Finally, suppose $g_1, g_2 \in N_G(A)$, which means that $g_1Ag_1^{-1} = A$ and $g_2Ag_2^{-1} = A$. By a very similar idea as we did above, we can prove that $(g_1g_2)A(g_2^{-1}g_1^{-1}) = A$, and hence $g_1g_2 \in N_G(A)$. Hence, the normalizer is also a subgroup.

It is also worth mentioning that very element in $C_G(A)$ is also in $N_G(A)$, and hence $C_G(A)$ is a subgroup of $N_G(A)$.

The fact that normalisers and centralizers are subgroups is a consequence of a general theorem, which is the fact that stabilizers and kernels of group actions are themselves subgroups (which we have already proven in the preceding exercises).

To show this, let G be a group, and consider the following theorem:

Theorem 10.1. Let $P(G)$ be the set of all subsets of G. For $g \in G$ and $B \subseteq G$, consider the map from $G \times P(G)$ to $P(G)$ given by

$$g \cdot B = gBg^{-1}$$

which is nothing but conjugation. This map is a group action.

Proof: First, it is clear that $1B1 = B$, which means that $1 \cdot B = B$. Secondly, suppose $g_1, g_2 \in G$. We will show that $g_1 \cdot (g_2 \cdot B) = (g_1g_2) \cdot B$ by showing that $g_1(g_2Bg_2^{-1})g_1^{-1} = (g_1g_2)B(g_1g_2)^{-1}$. But this fact is trivial by considering the fact that $(g_1g_2)^{-1} = g_2^{-1}g_1^{-1}$.

Now, if $B \subseteq G$, then observe that $N_G(B)$ is the stabilizer of B, with respect to the above group action, and hence $N_G(B) \leq G$. Proving it from scratch was much more difficult.

Now, lets prove that $C_G(B) \leq N_G(B)$, using group actions. Let the group $N_G(B)$ act on B by conjugation, i.e for $g \in N_G(B)$ and $b \in B$, define

$$g \cdot b = gbg^{-1}$$

Then, the kernel of this action is precisely the set $C_G(B)$, and hence it follows that $C_G(B) \leq N_G(B) \leq G$. If we set $B = G$, we get that $Z(G) \leq G$, i.e the center is also a subgroup. The proofs of these properties are now much simpler using group actions.

11. Exercises on Page 52

2. Let G be a group. We know that for any $g \in G$ and $a \in Z(G)$,

$$ag = ga$$

which implies that $C_G(Z(G)) = G$. Also, we know that $C_G(Z(G)) \leq N_G(Z(G)) \leq G$, which also implies that $N_G(Z(G)) = G$.

3. Suppose A and B are subsets of G such that $A \subseteq B$. Consider the subgroups $C_G(A)$ and $C_G(B)$. If $b \in C_G(B)$, then $b \in C_G(A)$, which implies that $C_G(B) \leq C_G(A)$.

4. In this exercise we will find the centers for each of the groups S_3, D_8 and Q_8.

S_3: Since $Z(S_3) \leq S_3$, it follows that $|Z(S_3)|$ divides 6. Also, since S_3 is non-abelian, it follows that $|Z(S_3)|$ has to be one of 1, 2 or 3. Now, none of the 2-cycles of S_3 can be in $Z(S_3)$, because they don't mutually commute. Also, none of the 3-cycles can be in $Z(S_3)$, because the $3-cycles$ don't commute. Hence, it follows that $Z(S_3) = \{1\}$.

D_8: We will show that $Z(D_8) = \{1, r^2\}$. If $sr^k \in Z(D_8)$ for some k, then it will follow that

$$rsr^k = sr^{k+1}$$

which will imply that $r^2 = 1$, which is not true. So, no reflection can be in the group center. If $r^k \in Z(D_8)$, for some k, then it will follow that

$$sr^k = r^k s$$

which will imply that $r^{2k} = 1$, which is only possible if $k = 2$. It is easy to see that r^2 actually commutes with every element. So, it follows that $Z(D_8) = \{1, r^2\}$.

Q_8: It is clear that $\{1, -1\} \leq Z(Q_8)$. Now, $i \notin Z(Q_8)$, because $ij \neq ji$. Same holds true for $-i$. By symmetry, none of j, $-j$, k and $-k$ is in $Z(Q_8)$. So, it follows that $Z(Q_8) = \{1, -1\}$.

6. Let H be a subgroup of the group G.

(a) We will show that $H \leq N_G(H)$. Define a map from $H \times H \to H$ as $h \cdot g = hgh^{-1}$, for $h, g \in H$. This map is a group action, and for fixed $h \in H$, the map $\sigma_h : H \to H$ given by $\sigma_h(g) = hgh^{-1}$ is a permutation of H, which means that $hHh^{-1} = H$, which means that $h \in N_G(H)$. So, $H \leq N_G(H)$.

If H is not a subgroup, then this is not necessarily true. For instance, consider Q_8, and let $H = \{i\}$. Clearly, H is not a subgroup. Also, observe that $i \notin N_G(H)$, so H is not a subset of $N_G(H)$'.

(b) We will show that $H \leq C_G(H)$. Suppose H is abelian. Then it is clear that $H \leq C_G(H)$. If $H \leq C_G(H)$, then all elements of H commute with each other, and hence H is abelian.

7. Suppose $n \in \mathbb{Z}$ with $n \geq 3$. First, let's show that no element of the form sr^k is in $Z(D_{2n})$. If it was the case, then we would have

$$rsr^k = sr^{k+1}$$

which would imply that $r^2 = 1$, which is a contradiction. If $r^k \in Z(D_{2n})$, for some k, then observe that

$$sr^k = r^k s$$

which implies that $r^{2k} = 1$, which is only possible if $2k = 0 (\text{mod } n)$. Because $1 \leq k \leq n$, if n is odd, then there is no such k. If n is even, then the only choice is $\dfrac{n}{2}$. Also, if n is even, then it is easy to see that $r^{\frac{n}{2}}$ commutes with all elements of the group. So, it follows that $Z(D_{2n}) = \{1\}$, if n is odd, and $Z(D_{2n}) = \{1, r^{\frac{n}{2}}\}$, if n is even.

8. Let $G = S_n$, and let $A = S$, and consider the group action defined by

$$\sigma \cdot a = \sigma(a)$$

for $\sigma \in G$, and $a \in A$. For $i \in A$, G_i as defined is nothing but $\text{Stab}_G(i)$, which is a subgroup of G (because stabilizers are subgroups). Also, the order of G_i must be $(n-1)!$, which is not hard to see.

9. Let H be a subgroup of G. First, we know that intersection of two subgroups is a subgroup, which means that $H \cap N_G(A)$ is a subgroup of G. Also, if $h \in N_H(A)$, then it is clear that $h \in H$ and $h \in N_G(A)$, which means that $h \in N_G(A) \cap H$. And if $h \in H \cap N_G(A)$, then by definition, $h \in N_H(A)$, which means that $N_H(A) = H \cap N_G(A)$. Hence, $N_H(A)$ is a subgroup of H.

10. Suppose H is a subgroup of order 2 in G, and let $H = \{1, h\}$. We will show that $N_G(H) \leq C_G(H)$. Suppose $g \in N_G(H)$, which means that $gHg^{-1} = H$. But, observe that $gHg^{-1} = \{1, ghg^{-1}\}$. So, this means that $ghg^{-1} = h$, which means that $g \in C_G(H)$. Hence, $N_G(H) \leq C_G(H)$. But, this means that $C_G(H) = N_G(H)$.

Now, if $N_G(H) = G$ then it follows that $C_G(H) = G$, which means that all elements of G commute with all elements of H, and hence $H \leq Z(G)$.

12. Let $R = \mathbb{Z}[x_1, x_2, x_3, x_4]$, the ring of polynomials in four variables.

(b) We define a group action on R by the group S_4. For $\sigma \in S_4$ and $p(x_1, x_2, x_3, x_4) \in R$, define

$$\sigma \cdot p(x_1, x_2, x_3, x_4) = p(x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)}, x_{\sigma(4)})$$

. Clearly, if 1 is the identity permutation, then

$$1 \cdot p(x_1, x_2, x_3, x_4) = p(x_1, x_2, x_3, x_4)$$

Also, if σ_1 and σ_2 are two permutations, then

$$\begin{aligned} \sigma_1 \cdot (\sigma_2 \cdot p(x_1, x_2, x_3, x_4)) &= \sigma_1 \cdot (p(x_{\sigma_2(1)}, x_{\sigma_2(2)}, x_{\sigma_2(3)}, x_{\sigma_2(4)})) \\ &= p(x_{\sigma_1\sigma_2(1)}, x_{\sigma_1\sigma_2(2)}, x_{\sigma_1\sigma_2(3)}, x_{\sigma_1\sigma_2(4)})) \\ &= (\sigma_1\sigma_2) \cdot p(x_1, x_2, x_3, x_4) \end{aligned}$$

So, this is a valid group action.

(c) Consider the polynomial $p(x_1, x_2, x_3, x_4) = x_4$. Clearly, all $\sigma \in S_4$ that fix 4 stabilize p under the group action. Also, it is easy to see that this stabilizer is isomorphic to S_3.

(d) Let $p(x_1, x_2, x_3, x_4) = x_1 + x_2$. Clearly, $1 \in S_4$ is a stabilizer. It is easy to see that the other stabilizers are (1 2), (3 4) and (1 2)(3 4). Since disjoint cycles commute, this is an abelian group of order 4.

12. Cyclic Groups

H is called a *cyclic* group if $H = \{x^n |\ n \in \mathbb{Z}\}$, where $x \in H$. In that case, we write $H = \langle x \rangle$. Let's state some easy to prove theorems:

Theorem 12.1. Let G be a group, and let $x \in G$. If $x^n = 1$, for some $n \in \mathbb{Z}$, then $|x|$ divides n.

The next theorem proves a fundamental property of the structure of cyclic groups.

Theorem 12.2. Any two cyclic groups of the same order are isomorphic.

Proof: First, let's deal with finite cyclic groups. Suppose $A = \langle x \rangle$ and $B = \langle y \rangle$ are two cyclic groups of the same order, say $n \in \mathbb{N}$. Consider the map $\phi : A \to B$ given by

$$\phi(x^k) = y^k$$

for all $0 \leq k \leq n - 1$. Clearly, the map is a bijection. Also, it is not difficult to see that it is also a homomorphism. Hence, A and B are isomorphic.

Similarly, if $A = \langle x \rangle$ is an infinite cyclic group, then consider the map $\phi : \mathbb{Z} \to A$ given by

$$\phi(k) = x^k$$

Again, it is not hard to see that this is indeed an isomorphism.

Given $H = \langle x \rangle$, we will now determine which elements of H generate it.

Theorem 12.3. Let G be a group, and let $x \in G$, and $a \in \mathbb{Z} - \{0\}$.

(1) If $|x| = \infty$, then $|x^a| = \infty$.
(2) If $|x| = n < \infty$, then $|x^a| = \dfrac{n}{(n, a)}$.

Proof: To prove (1), suppose $|x^a| = m < \infty$. So, we have

$$(x^a)^m = x^{am} = 1$$

Without loss of generality, we can assume that $a > 0$ (as $|x^a| = |x^{-a}|$). But, this means that $am > 0$ and $x^{am} = 1$, contradicting the fact that $|x| = \infty$. Hence, $|x^a| = \infty$.

To prove (2), suppose $|x| = n$. Observe that

$$(x^a)^{\frac{n}{(a,n)}} = 1$$

and hence $|x^a| < \infty$. Now, if $|x^a| = k$, then $x^{ak} = 1$, which implies that $n|ak$. The least positive integer k for which this is true is $\dfrac{n}{(a, n)}$. So, $k = \dfrac{a}{(a, n)}$.

Theorem 12.4. Suppose $H = \langle x \rangle$.

(1) Suppose $|H| = \infty$. Then, $H = \langle x^a \rangle$ if and only if $a = \pm 1$.
(2) If $|H| = n < \infty$, then $H = \langle x^a \rangle$ if and only if $(a, n) = 1$. Hence, there are $\phi(n)$ generators.

Proof: (2) is easy to prove. So, we will prove (1). If $a = \pm 1$, then clearly $H = \langle x^a \rangle$. Now, suppose $H = \langle x^a \rangle$, for some $a \in \mathbb{Z}$. Then, for any $k \in \mathbb{Z}$, there is some $q \in Z$ such that

$$x^{qa} = x^k$$

Since distinct powers of x are distinct, it follows that

$$k = qa$$

which means that $a|k$. Since k was arbitrary, it follows that $a = \pm 1$.

We now prove a theorem that gives the complete structure of subgroups of a cyclic group:

Theorem 12.5. Suppose $H = \langle x \rangle$.

(1) Every subgroup of H is cyclic. If $K \leq H$, then either $K = \{1\}$, or $K = \langle x^d \rangle$, where d is the smallest positive integer such that $x^d \in K$.
(2) If H is an infinite group, then if $a, b \in \mathbb{Z}$ such that $a \neq b$, then $\langle x^a \rangle \neq \langle x^b \rangle$. Also, for every integer m, we have $\langle x^m \rangle = \langle x^{|m|} \rangle$.
(3) If H is a finite group, then for every positive divisor of a, there is a unique subgroup of order a, which is $\langle x^{\frac{n}{a}} \rangle$. Also, for every $m \in \mathbb{Z}$, we have $\langle x^m \rangle = \langle x^{(n,m)} \rangle$.

So, if H is a finite group, the subgroups of H are in bijection with $\mathbb{Z}$. If H is an infinite group, the subgroups are in bijection with the positive divisors of $|H|$.

Proof: To prove (1), suppose K is a subgroup of H such that $K \neq \{1\}$. Let $S := \{d \in \mathbb{N} : \ x^d \in K\}$. S is non-empty since $K \neq \{1\}$. So, let the least element of S be d. We will show that $K = \langle x^d \rangle$. Suppose $x^a \in K$, for some $a \in \mathbb{Z}$. Let $a = dq + r$, where $0 \leq r < d$. So, $x^a = x^{dq}x^r$, which implies that $x^r \in K$. Since d is the least element of S, it follows that $r = 0$, which means that $d|a$. So, it follows that $H = \langle x^d \rangle$.

To prove (2), suppose H is an infinite group. Let $a, b \in \mathbb{Z}$ be such that $a \neq b$. We might as well assume that $a, b \in \mathbb{N}$, and without loss of generality suppose $a < b$. Then, it follows that $x^a \notin \langle x^b \rangle$, and hence $\langle x^a \rangle \neq \langle x^b \rangle$. The fact that $\langle x^m \rangle = \langle x^{|m|} \rangle$ has been proven before.

Finally, to prove (3), suppose a is a positive divisor of n. Then, the group $\langle x^d \rangle$ has order a, where $d = \dfrac{n}{a}$. To prove that this group is unique, suppose there is another subgroup K of order a. Then, $K = \langle x^b \rangle$, where b is the least positive integer for which $x^b \in K$. Also, in this case, $0 \leq b < n$. Also, we know that the order of $\langle x^b \rangle$ is $\dfrac{n}{(n, b)}$. So, it follows that $\dfrac{n}{(n, b)} = a$, which means that $(n, b) = d$, which means that $d|b$. Hence, $\langle x^b \rangle \leq \langle x^d \rangle$, and because the orders of the two groups are same, it follows that $\langle x^b \rangle = \langle x^d \rangle$. Now, if $m \in \mathbb{Z}$, then $\langle x^m \rangle \leq \langle x^{(n,m)} \rangle$. Also, their orders are equal, and hence $\langle x^m \rangle = \langle x^{(n,m)} \rangle$.

To reiterate, the previous theorem says this: if H is an infinite cyclic group, then its subgroups are in bijection with $\mathbb{N}$. If H is a finite cyclic group, then its subgroups are in bijection with the positive divisors of $|H|$. In particular, there are exactly $\sigma_0(n)$ subgroups.

13. Exercises on Page 60

8. Consider the map ϕ_a from $\mathbb{Z}/48\mathbb{Z}$ to Z_{48} given by

$$\overline{1} \to x^a$$

For this to be an isomorphism, it is necessary and sufficient that x^a is a generator of Z_{48}. So, any a such that $(a, 48) = 1$ will work.

9. Let $Z_{36} = \langle x \rangle$, and for $a \in \mathbb{Z}$, consider the map $\phi : \mathbb{Z}/48\mathbb{Z} \to Z_{36}$ given by $\phi(\overline{1}) = x^a$. Suppose this map is well defined. So, for if $\overline{b} = \overline{c}$, it should be true that $\phi(\overline{b}) = \phi(\overline{c})$. Now, suppose $b = 48k + c$, and observe that

$$\phi(\overline{b}) = x^{ab} = x^{a(48k+c)} = x^{48ak}x^{ac} = x^{ac}$$

and if we set $k = 1$, we see that $x^{12a} = 1$, which means that $3|a$. So, the map will be well defined if and only if $3|a$, and it will automatically be a homomorphism.

Also, the map can never be surjective, because $x^{ak} \neq x$ for all $k \in \mathbb{Z}$, because $3|a$.

11. Here, we will find all cyclic subgroups of D_8. By Lagrange, the cyclic subgroup can only have order 1, 2, 4 or 8. By this observation, it is easy to see that the only cyclic subgroups are: $\{1\}$, $\{1, r^2\}$, $\{1, s\}$, $\{1, sr\}$, $\{1, sr^2\}$, $\{1, sr^3\}$, $\{1, r, r^2, r^3\}$. A proper subgroup of D_8 which is not cyclic is: $\{1, r^2, s, sr^2\}$.

14. Let $\sigma = (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12)$. We know that the order of this cycle is 12. So, $\sigma^a = \sigma^{a \mod m}$, where $a \mod m$ is the reduced residue mod m. Also, we proved earlier that σ^a consists of $\dfrac{12}{(12, a)}$ cycles, each of length $(12, a)$. This theorem will help make the computation a bit easy.

16. Suppose $|x| = n$ and $|y| = m$, and suppose that $xy = yx$. Let $|xy| = p$. If $[n, m]$ is the lcm, then $(x, y)^{[n,m]} = x^{[n,m]}y^{[n,m]} = 1$, because the elements commute, and hence $p|[n, m]$.

We now give an example of non-commuting elements where this need not hold. Let $x = (1\ 2)$ and $y = (1\ 3)$ in S_4. Then, $|x| = 2$ and $|y| = 2$, and observe that $xy = (1\ 3\ 2)$, so that $|xy| = 3$.

17. $Z_n = \langle x |\, x^n = 1\rangle$.

20. In this exercise, we will prove that $(1 + p)$ is an element of order p^{n-1} in the multiplicative group $\mathbb{Z}/p^n\mathbb{Z}$, where p is an odd prime.

23. We will show that $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is not cyclic for $n \geq 3$ by finding two subgroups of order 2. Clearly, one such subgroup if $\langle 2^n - 1\rangle$. Also, it can be checked that if $n \geq 3$, then $\langle 2^{n-1} - 1\rangle$ is also a subgroup of order 2. Clearly, these are distinct subgroups, and hence the given group is not cyclic.

24. Let G be a finite group, and suppose $x \in G$ with $|x| = n$.

(a) Suppose $g \in N_G(\langle x\rangle)$. Then, it follows that $g\langle x\rangle g^{-1} = \langle x\rangle$, and hence $gxg^{-1} = x^a$, for some $a \in \mathbb{Z}$.

(b) Conversely, suppose $gxg^{-1} = x^a$, for some $a \in \mathbb{Z}$. Since order is invariant under conjugation, it follows that $(a, n) = 1$. Also, observe that $gx^kg^{-1} = (gxg^{-1})^k = x^{ak}$, for any $k \in \mathbb{Z}$. This means that $g\langle x\rangle g^{-1} = \langle x^a\rangle$, and we know that x^a is a generator $(a, n) = 1$, and hence $g\langle x\rangle g^{-1} = \langle x^a\rangle = \langle x\rangle$, which means that $g \in N_G(\langle x\rangle)$.

This gives us a very useful test to find normalizers of cyclic subgroups.

25. Suppose G is a cyclic group of order n, and suppose k is an integer relatively prime to n. Consider the map from G to G given by $x \mapsto x^k$. In this case, x^k is also a generator, and hence the map is surjective.

Let's now prove the theorem for general finite groups G, and let the order of G be n. Let $x \in G$. Consider the cyclic subgroup $\langle x\rangle$. By Lagrange's theorem, it follows that if $|x| = m$, then $m|n$. So, it follows that $(k, m) = 1$, and hence $\langle x^k\rangle = \langle x^{(k,m)}\rangle = \langle x\rangle$. So, it follows that there is some $b \in \mathbb{Z}$ such that $x^{kb} = x$, which means that $(x^b)^k = x$. Hence, x has a k-th root in G, and so the map $x \mapsto x^k$ is surjective.

26. Let $Z_n = \langle y\rangle$. For $a \in \mathbb{Z}$, let $\sigma_a : Z_n \to Z_n$ be defined by $\sigma_a(x) = x^a$ for $x \in Z_n$.

(a) First, we will show that the map σ_a is a homomorphism for every $a \in \mathbb{Z}$. If $x_1, x_2 \in Z_n$, then $x_1 = y^{k_1}$ and $x = y^{k_2}$, for some $k_1, k_2 \in \mathbb{Z}$. So,

$$\sigma_a(x_1x_2) = y^{ak_1+ak_2} = \sigma_a(x_1)\sigma_a(x_2)$$

and hence this map is a homomorphism. So, the map σ_a is completely determined by the value $\sigma_a(y)$. Now, if (a, n), then $\sigma_a(y) = y^a$ is a generator of Z_n, and hence the map is an isomorphism. Conversely, if the map is an isomorphism, then $\sigma_a(y) = y^a$ must be a generator, which implies that $(a, n) = 1$. So, σ_a is an automorphism if and only if $(a, n) = 1$.

(b) Suppose $\sigma_a = \sigma_b$. This implies that $y^a = y^b$, which means that $a = b(\text{mod } n)$. Conversely, suppose $a = b(\text{mod } n)$. Then, $\sigma_a(y) = y^a = y^b = \sigma_b(y)$, and hence the maps are equal (because they are determined by $\sigma_a(y)$ and $\sigma_b(y)$).

(c) Suppose $\phi \in \text{Aut}(Z_n)$. Then, $\phi(y) = y^k$, for some $k \in \mathbb{Z}$. Since y generates Z_n, it follows that for every $x \in Z_n$, it is true that $\phi(x) = x^k$. So, ϕ is the map $x \mapsto x^k$, which is σ_k.

14. Subgroups generated by subsets

In vector space theory, we can generate subspaces using a subset of the vector space, which is just the set of all finite linear combinations of elements of the subset. In the same exact manner, there is a notion of a subgroup *generated* by a subset of a group. Let's make this notion precise as follows.

Suppose G is a group, and let A be a subset of G. Let M be the set of all subgroups of G that contain A (which is clearly not empty, because $G \in M$). We define

$$\langle A \rangle = \bigcap_{H \in M} H$$

and call this the *subgroup generated by* A. It is not hard to see that $\langle A \rangle$ is the smallest subgroup of G that contains A.

Now, we consider the set of all finite products of elements of A (analogous to finite linear combinations as in vector space theory), and claim that this set must be $\langle A \rangle$.

Theorem 14.1. If $A \subset G$, then

$$\langle A \rangle = \{a_1^{\alpha_1} a_2^{\alpha_2} ... a_n^{\alpha_n} \mid n \in \mathbb{N}\ , a_i \in A,\ \alpha_i = \pm 1\}$$

Note that, the a_is don't have to be distinct. The proof of this theorem is just like the proof as in vector space theory. Also, a point to be observed is that this definition doesn't require A to be a finite or even a countable set.

Exercises on Page 65

2. Let G be a group, and suppose $A \subset B \subset G$. We will show that $\langle A \rangle \leq \langle B \rangle$. If $x \in A$, then $x \in B$, and hence $x \in \langle B \rangle$. So, $\langle B \rangle$ is a subgroup of G containing A. By the definition of $\langle A \rangle$, it follows that $\langle A \rangle \leq \langle B \rangle$.

Now, let $G = \mathbb{Z}_n = \langle x \rangle$, and set $B = G$, and $A = \{x\}$. Then, $A \subset B$ and $A \neq B$, but $\langle A \rangle = \langle B \rangle = G$.

3. Suppose H is a subgroup of an abelian group G. We will show that $\langle H, Z(G) \rangle$ is also abelian. Note that any element of $\langle H, Z(G) \rangle$ is a product of finitely many elements of H and $Z(G)$. Also, all elements of $Z(G)$ commute with all elements of H, and $Z(G)$ is itself abelian, so it follows that $\langle H, Z(G) \rangle$ is also abelian.

We will now show by explicit example that $\langle H, C_G(H) \rangle$ may not necessarily abelian. Intuitively, this is because $C_G(H)$ may not itself be abelian. For instance, let $G = D_8$, and let $H = \{1, r^2\}$. Then, it can be calculated that $C_G(H) = D_8$. Hence, $\langle H, C_G(H) \rangle = D_8$ is not abelian.

5. Any element of order 2 in S_3 must be a transposition. By Lagrange's theorem, a subgroup of S_3 can have order 1, 2, 3 or 6. If a and b are the chosen transpositions in S_3, then $\langle a, b \rangle$ contains the elements 1, a and b. Also, the product of any two transpositions distinct transpositions is not a transposition, and hence $\langle a, b \rangle = 6$, which means that $\langle a, b \rangle = S_3$.

6. Consider the subgroup of S_4 given by $\langle (1\ 2), (1\ 2)(3\ 4) \rangle$. Since these two elements commute, this subgroup is abelian. Also, since the order of each of the elements is 2, 4 is an upper bound to the order of the given subgroup. Also, observe that

$$(1\ 2)(1\ 2)(3\ 4) = (3\ 4)$$

and hence

$$\langle (1\ 2), (1\ 2)(3\ 4) \rangle = \{1, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}$$

which is an abelian group of order 4.

7. Consider the subgroup of S_4 given by $\langle (1\ 2), (1\ 3)(2\ 4)\rangle$. Put $a = (1\ 2)$ and $b = (1\ 3)(2\ 4)$. Then, we can see that $(1\ 3\ 2\ 4) = ab$. Also, observe that $(ab)^4 = 1$, and $a^2 = b^2 = 1$. So, we see that

$$\langle (1\ 2), (1\ 3)(2\ 4)\rangle = \langle a, b |\ a^2 = b^2 = 1,\ (ab)^4 = 1\rangle$$

which is a presentation for D_8. So, this subgroup is isomorphic to D_8, where the isomorphism is given by $a \mapsto s$, $ab \mapsto r$.

13. Consider the multiplicative group of positive rational numbers. If $\frac{p}{q}$ is in the group, then $(p, q) = 1$ and both p and q are positive. By the fundamental theorem of arithemetic, we can write $p = p_1^{\alpha_1}...p_n^{\alpha_n}$ and $q = q_1^{\beta_1}...q_m^{\beta_m}$, where no p_i is equal to any q_j. So, we have

$$\frac{p}{q} = \frac{p_1^{\alpha_1}...p_n^{\alpha_n}}{q_1^{\beta_1}...q_m^{\beta_m}}$$

which can be separated as powers of $\frac{1}{p_i}$s and powers of $\frac{1}{q_i}$s. Hence, this group is generated by the set $\left\{\frac{1}{p} : p \text{ is prime}\right\}$

14. (a) If G is a finite group, then it is trivially generated by all of its elements, and hence it is finitely generated.

(b) $\mathbb{Z} = \langle x\rangle$ is an infinite cyclic group, and hence it is finitely generated.

(c) Suppose H is a finitely generated subgroup of the additive group Q, say $H = \langle a_1, a_2, ..., a_n\rangle$, where each $a_i = \frac{p_i}{q_i}$ is a rational number. Let $Q = q_1q_2...q_n$. If $x \in H$, then

$$x = k_1a_1 + ... + k_na_n = \frac{k_1p_1r_1 + ... + k_np_nr_n}{Q}$$

where each k_i is an integer, and $r_i = \frac{Q}{q_i}$ is also an integer. This means that $x \in \left\langle \frac{1}{Q} \right\rangle$, and hence $H \leq \left\langle \frac{1}{Q} \right\rangle$. So, H must be cyclic as well.

(d) If Q were finitely generated, then it would mean that Q is cyclic, which is not true. So, Q is not finitely generated.

15. A proper subgroup of Q which is not cyclic is the subgroup of all positive rational numbers, as given in problem **13**.

16. (a) Let H be a proper subgroup of a finite group G. Consider the set $M := \{U < G : H \leq U\}$. Clearly, this set is non-empty and finite (a finite group can only have finitely many subgroups). So, out of all these subgroups, we can choose a maximal subgroup.

(b) Let D_{2n} be the dihedral group, and consider $R = \{1, r, r^2, ..., r^{n-1}\}$, the subgroup of all rotations. We will show that this subgroup is maximal. So, suppose H is a subgroup of D_{2n} containing R such that $H \neq \mathbb{R}$. Then, H contains a reflection, say sr^k, for some $0 \leq k \leq n-1$. Then, since $r^k \in H$, we see that

$$r^k sr^k = s$$

is also in H, and hence $H = D_{2n}$. So, it follows that R is maximal.

(c) Suppose $G = \langle x \rangle$ is a cyclic group of order $n \geq 1$. We will show the following: $H \leq G$ is maximal if and only if $H = \langle x^p \rangle$ for some prime p dividing n.

First, suppose H is maximal. We know that H is cyclic, so $H = \langle x^p \rangle$, for some $p \in \mathbb{Z}$ ($p \neq 0$ because H cannot be the trivial subgroup). Also, because $H \neq G$, it follows that $d = (p, n) > 1$. This means that $H \leq \langle x^d \rangle$, and since $(d, n) = d > 1$, it is also true that $\langle x^d \rangle \neq G$. So, the only possible way this is true is when $d = p$. So, $p|n$. Now, we will show that p is a prime. If not, then let k be a non-identity divisor of p. Then, $H < \langle x^k \rangle$, and since $(k, n) = k > 1$, it is also true that $\langle x^k \rangle \neq G$, which contradicts the maximality of H. So, p must be a prime.

The converse is easy to prove. Suppose p is a prime dividing n, and let $H = \langle x^p \rangle$, so that $H \neq G$. Suppose $K \leq G$ is a subgroup containing H, and let $K = \langle x^a \rangle$, for some $a \in \mathbb{Z}$. Assume also that $K \neq G$, so that $d = (a, n) > 1$. So, we have that $x^p \in K$, which means that $p = ak (\text{mod } n)$, which means that $d|p$. But, the only choice of d is $d = p$, and hence $a = p$, which means that $K = H$. So, the only subgroups of G containing H are H and G, so that H is maximal.

17. Let G be a non-trivial finitely generated group, say $G = \langle g_1, ..., g_n \rangle$ and let $\mathcal{S}$ be the set of all proper subgroups of G. Clearly, $\mathcal{S}$ is non-empty (because it contains the trivial subgroup), and $\mathcal{S}$ is a partially ordered set, the partial order being set inclusion "$\subset$". Let $\mathcal{C}$ be a chain in $\mathcal{S}$.

(a) Define $M = \bigcup_{H \in \mathcal{C}} H$. Let's show that M is a subgroup of G. Clearly, $1 \in M$. If $a \in M$, then $a \in H$, for some $H \in \mathcal{C}$, and hence $a^{-1} \in M$. Finally, suppose $a, b \in M$. Then, $a \in H_1$ and $b \in H_2$, for some H_1, H_2 in $\mathcal{C}$. But, since $\mathcal{C}$ is a chain, without loss of generality, suppose $H_1 \subset H_2$, which implies that $ab \in H_2$, and hence $ab \in M$. So, M is a subgroup of G.

(b) We will now show that M is a proper subgroup of G, which will mean that $M \in \mathcal{S}$. Suppose not, i.e suppose $M = G$. Then, $g_1 \in H_1$, $g_2 \in H_2$, for some $H_1, H_2 \in \mathcal{C}$, and continuing this way, we see that $g_i \in H_i$, for some $H_i \in \mathcal{C}$, for each i. However, $\mathcal{C}$ is a chain, and this will imply that $g_1, ..., g_n \in H_j$, for some $1 \leq j \leq n$, which means that $H_j = G$, a contradiction because H_j is a proper subgroup of G. So, M is a proper subgroup of G, and hence this chain $\mathcal{C}$ in $\mathcal{S}$ has an upper bound in $\mathcal{S}$.

(c) By Zorn's lemma, this means that $\mathcal{S}$ has a maximal element. By definition, this maximal element is a maximal subgroup of G. Hence, every non-trivial finitely generated group has a maximal subgroup.

19. (a) We will show that the additive group of rational numbers $\mathbb{Q}$ is divisible. Let $a \in \mathbb{Q}$, and let $k \in \mathbb{Z}$ be non-zero. Then, since

$$\frac{a}{k} \cdot k = a$$

the element a has a $k - th$ root, and hence $\mathbb{Q}$ is divisible.

15. Exercises on Page 71

16. Homomorphisms and Quotient Groups

In this section, we will see that quotienting of groups is just a study of homomorphisms between groups. Let's start with a simple case.

Suppose $\phi : G \to H$ is a group homomorphism between two groups G and H, and let $K = \text{Ker}(\phi)$. The *quotient group* G/K is defined as follows: for every $a \in \text{Im}(\phi)$,

consider the set $X_a := \{y \in G |\ \phi(y) = a\}$. For $a, b \in \text{Im}(\phi)$, we define $X_a X_b = X_{ab}$. The new group is denoted by G/K.

Like in vector space theory, if V is a vector space, and W is a subspace, then V/W consists of all translates of W, i.e

$$V/W := \{u + W : u \in V\}$$

where the choice of representatives of an equivalence class is immaterial. In the same aspect, let's prove the following theorem:

Theorem 16.1. Suppose $\phi : G \to H$ is a homomorphism with kernel K. For $a \in \text{Im}(\phi)$, let $X_a := \phi^{-1}(a)$ (the pre-image). Then, if $u \in X_a$, then

(1) $X_a = uK$ (the left coset).
(2) $X_a = Ku$ (the right coset).

In essence, this theorem says that the fibre of a looks like a translate of K, and the choice of u (the representative) does not matter.

Proof: Let's prove (1) first. Suppose $v \in X_a$, so that $\phi(v) = a$. This means that $u^{-1}v \in K$, and hence $v = uk$, for some $k \in K$, which means that $v \in uK$, and hence $X_a \subset uK$. Now, if $v \in uK$, then it is easy to see that $\phi(v) = a$, and hence $v \in X_a$. Hence, $X_a = uK$.

For (2), the proof is exactly similar, just observe that $vu^{-1} \in K$.

The above theorem implies that if $K \leq G$ is the kernel of some homomorphism from G to some group, then if $g_1 \in gK$, it follows that $g_1 K = gK$ (similarly for right cosets), which in simple words mean that *any* representative of a coset can be chosen. We will see that this is infact true for arbitrary subgroups of G.

We now prove that the quotient we have defined is actually a group, if K is the kernel of some homomorphism:

Theorem 16.2. Suppose G is a group and $K \leq G$ such that K is the kernel of some homomorphism from G to some other group. Then, the left cosets (or right cosets) of K in G form a group, with the operation given by

$$uK \cdot vK = (uv)K$$

and the group is well defined in the sense that any two representatives of the same coset can be chosen.

Proof: Suppose $u, v \in G$, and consider the cosets uK and vK. If $a = \phi(u)$ and $b = \phi(v)$, then we know that $uK = \phi^{-1}(a)$ and $vK = \phi^{-1}(b)$. Also, $(uv)K = \phi^{-1}(uv)$. Now, suppose u_1, v_1 are in uK and vK respectively. Then, we know that $u_1 K = uK$ and $v_1 k = vK$. Now,

$$(u_1 v_1)K = \phi^{-1}(u_1 v_1) = \phi^{-1}(uv) = (uv)K$$

and hence the choice of the representatives doesn't matter. Hence, the left cosets form a group. The same exact procedure can also be repeated for right cosets.

At this point, it is to be remarked that left cosets forming a group only makes sense if the **choice** of the representative does not matter. As mentioned before, we will see later that if uK is a left coset, and if $v \in uK$, then $uK = vK$, and it is true for arbitrary subgroups K of G.

From now on, we will not mention any homomorphism while studying quotient groups, we will only work with left (or right) cosets. The next theorem will show that the left (or right) cosets of a subgroup N of G partition G:

Theorem 16.3. Suppose N is a subgroup of a group G. The left cosets of N partition G. In particular, if uN is a left coset, and $v \in uN$, then $uN = vN$. The same also holds for right cosets. (This partition also induces an equivalence relation on G)

Proof: It is clear that the union of all left cosets is the group G. We will show that if the intersection of two left cosets is non-empty, then the cosets are equal.

So, suppose $u, v \in G$ such that $uN \cap vN \neq \phi$. So, let $k \in uN \cap vN$, so that

$$k = un = vm$$

for some $n, m \in N$. Consider the coset kN. If $x \in kN$, then $x = ky$, for some $y \in N$, which means that $x = uny$, which means that $x \in uN$, which means that $kN \subset uN$. Now, if $x \in uN$, then $x = uy$, for some $y \in N$, and hence $x = kn^{-1}y$, which means that $x \in kN$, and so $uN \subset kN$. So, $uN = kN$, and similarly, $uN = kN = vN$. For right cosets, the procedure is exactly the same. The claim follows.

We will now see which subgroups of a group G have the property that their left (or right) cosets form a group:

Theorem 16.4. Suppose G is a group and let N be a subgroup of G.

(1) The multiplication of left (or right) cosets given by
$$uN \cdot vN = (uv)N$$
is well defined if and only if $gng^{-1} \in N$ for all $g \in G$ and $n \in N$.
(2) If the operation is well defined, then the left (or right) cosets form a group, denoted by G/N.

Proof: We will prove only (1), since (2) is not hard to prove.

First, suppose the multiplication of left (or right) cosets is well defined. Let g, n be arbitrary elements of G and N respectively. Since $gg^{-1} \in N$ and $n \in N$, we have

$$(gn)N = (g1)N = gN$$

So, it follows that

$$(gnN)(g^{-1}N) = (gN)(g^{-1}N) = N$$

but $(gnN)(g^{-1}N) = (gng^{-1}N)$ and hence

$$(gng^{-1}N) = N$$

which means that $gng^{-1} \in N$.

Conversely, suppose $gng^{-1} \in N$ for all $g \in G$ and $n \in N$. Then, suppose u, u_1 and v, v_1 are in G such that $u = u_1k_1$ and $v = v_1k_2$, for some $k_1, k_2 \in N$. We wish to show that

$$(uv)N = (u_1v_1)N$$

So, suppose $x \in (uv)N$. Then, $x = uvk$, for some $k \in N$. Observe that

$$y = v_1^{-1}k_1v_1k_2k \in N$$

and it can be checked that $(uv)k = (u_1v_1)y$, which means that $(uv)N \subset (u_1v_1)N$. Similarly, the reverse containment can be proven, and hence $(uv)N = (u_1v_1)N$, which proves the claim.

Such subgroups N of G are called *normal* subgroups, and we use the notation to denoted these subgroups.

The following theorem is not hard to prove:

Theorem 16.5. If N is a subgroup of G, then the following are equivalent:

(1) $N \trianglelefteq G$.

(2) $N_G(N) = G$.
(3) $gNg^{-1} \subset N$.
(4) $gN = Ng$ for all $g \in G$.

So, to check whether a subgroup is normal, we can use any of the above criterion.

We now show that normal subgroups are precisely those subgroups which are kernels of homomorphisms (remember that we started the discussion with kernels of homomorphisms):

Theorem 16.6. A subgroup N of G is normal if and only if it is the kernel of some homomorphism.

Proof: We will already shown that if N is the kernel of some homomorphism, then it is normal. We now prove the converse.

Now, suppose N is normal, and consider the map ϕ from G to G/N given by:

$$g \mapsto gN$$

Let's show that this is a homomorphism. Observe that

$$\phi(g_1g_2) = g_1g_2N = (g_1N)(g_2N) = \phi(g_1)\phi(g_2)$$

and hence this is a homomorphism. It is easy to see that the kernel of this homomorphism if N. This proves the claim.

The homomorphism constructed in this proof is also called the *natural projection* of G onto G/N.

Exercises on Page 85

1. Suppose $\phi : G \to H$ be a homomorphism, and let $E \leq H$. We will show that $\phi^{-1}(E) \leq G$. Clearly, $1 \in \phi^{-1}(E)$. If $x \in \phi^{-1}(E)$, then $\phi(x) \in E$, which means that $[\phi(x)]^{-1} \in E$, which means that $\phi(x^{-1}) \in E$, and hence $x^{-1} \in \phi^{-1}(E)$. That $\phi^{-1}(E)$ is closed under the operation is straightforward. Hence, $\phi^{-1}(E) \leq G$.

Next, suppose $E \trianglelefteq H$. We will show that $\phi^{-1}(E) \trianglelefteq G$. Suppose $g \in G$, and $e \in \phi^{-1}(E)$. Then, $\phi(geg^{-1}) = \phi(g)\phi(e)\phi(g)^{-1} \in E$, and hence $geg^{-1} \in \phi^{-1}(E)$, which means that $\phi^{-1}(E) \trianglelefteq G$. Hence, it follows that $\mathrm{Ker}(\phi) \trianglelefteq G$, because the trivial group of H is a normal subgroup.

3. Let A be an abelian group, and let B be a subgroup, so that $B \trianglelefteq A$, and hence A/B is defined. Suppose uB and vB are two elements of A/B. So, we have

$$uBvB = (uv)B = (vu)B = vBuB$$

and hence A/B is abelian.

Now, we will give an example of a non-abelian group G which has a proper normal subgroup N such that G/N is abelian. Let $G = D_8$, and let $N = Z(D_8) = \{1, r^2\}$. Then, we can compute that

$$D_8/Z(D_8) = \{\{1, r^2\}, \{r, r^3\}, \{s, sr^2\}, \{sr, sr^3\}\}$$

and since this is a group of order 4, it follows that $D_8/Z(D_8)$ is isomorphic to either Z_4 or V_4, both of which are abelian. Hence, this group is abelian.

4. Consider the quotient group G/N. We will prove that if $gN \in G/N$, then

$$g^\alpha N = (gN)^\alpha$$

for all $\alpha \in \mathbb{Z}$.

For positive α, the equality follows by induction. The equality is trivial for $\alpha = 0$. If α is negative, then observe that

$$g^\alpha N = (g^{-\alpha})^{-1}N = (g^{-\alpha}N)^{-1} = [(gN)^{-\alpha}]^{-1} = (gN)^\alpha$$

and hence the claim follows.

5. Let $g \in G$, and consider the coset gN. We wish to compute the order of the coset in G/N. From the previous exercise, we know that if $n \in \mathbb{N}$, then

$$(gN)^n = (g^n)N$$

and hence the order of gN is the least positive integer k such that $g^k \in N$. If no such integer exists, then gN has infinite order.

We will now give an example where the order of gN in G/N is strictly less than the order of g in G. An obvious example is $G = \mathbb{Z}$, and $N = m\mathbb{Z}$ for any $m \in \mathbb{Z}$. Any non-identity element of $\mathbb{Z}$ has infinite order, but every element in $\mathbb{Z}/m\mathbb{Z}$ has finite order.

Using this fact, we can show that quotient groups of a cyclic group are cyclic. Suppose $G = \langle x \rangle$ is a cyclic group. Let N be any subgroup of G, so that $N = \langle x^d \rangle$, where d is the smallest power of x in N. Since G is abelian, N is normal. Now, we have

$$G/N = \{gN |\ g \in G\} = \{x^k N |\ k \in \mathbb{Z}\}$$

and since

$$(x^k)N = (xN)^k$$

it follows that

$$G/N = \langle xN \rangle$$

The order of the quotient group G/N is equal to $\dfrac{|G|}{|N|}$, by Lagrange's theorem, if G is a finite group.

15. Let G be a divisible abelian group, and let N be a proper subgroup. We will show that G/N is also divisible. Suppose $gN \in G/N$. If $k \in \mathbb{Z}$, then there is some $x \in G$ such that $g = x^k$. So, it follows that

$$(x^k)N = (xN)^k = gN$$

and hence G/N is divisible. Since $\mathbb{Q}$ is a divisible abelian group, it follows that $\mathbb{Q}/\mathbb{Z}$ is also divisible.

16. Suppose $G = \langle S \rangle$ for some subset S of G. Let N be a normal subgroup of G, and let $\overline{G} = G/N$. Let $\overline{S}$ be the set of all left cosets of elements of S. We will show that

$$\overline{G} = \langle \overline{S} \rangle$$

It is clear that $\langle \overline{S} \rangle \leq \overline{G}$. To show the reverse inclusion, let $gN \in \overline{G}$. Since $g = x_1 ... x_n$, for some $x_1, .., x_n \in S$, it follows that

$$gN = (x_1 N)...(x_n N)$$

and hence $gN \in \langle \overline{S} \rangle$, which means that $\overline{G} \leq \langle \overline{S} \rangle$. The equality follows.

17. Consider D_{16}, and its center $Z(D_{16}) = \{1, r^4\}$. We consider the quotient group $\overline{G} = D_{16}/Z(D_{16})$.

(a) By Lagrange's theorem, the order of this subgroup is 8.

(b) Since $D_{16} = \langle s, r\rangle$, it follows that

$$D_{16}/Z(D_{16}) = \langle \overline{s}, \overline{r}\rangle$$

Now, it can be computed that

$$D_{16}/Z(D_{16}) = \{\{1, r^4\}, \{r, r^5\}, \{r^2, r^6\}, \{r^3, r^7\}, \{s, sr^4\}, \{sr, sr^5\}, \{sr^2, sr^6\}, \{sr^3, sr^7\}\}$$

and in terms of powers of $\overline{s}, \overline{r}$, we have

$$D_{16}/Z(D_{16}) = \{1, \overline{r^1}, \overline{r^2}, \overline{r^3}, \overline{s}, \overline{s}\overline{r^1}, \overline{s}\overline{r^2}, \overline{s}\overline{r^3}\}$$

Intuition says that this is isomorphic to D_8, and this is infact true.

(e) Consider the subgroup $\langle \overline{s}, \overline{r^2}\rangle$ of this group. We will show that it is normal. Observe that

$$\overline{r^k}\overline{s}\overline{r^k}^{-1} = \overline{r^k s r^{-k}} = \overline{r^{2k}s} \in \langle \overline{s}, \overline{r^2}\rangle$$

and we have

$$\overline{sr^k}\overline{s}\overline{sr^k}^{-1} = \overline{sr^k s r^{-k} s} = \overline{sr^{2k}} \in \langle \overline{s}, \overline{r}\rangle$$

and similarly we can show the same thing for $\overline{r^2}$. Hence, this is a normal subgroup.

22. (a) Suppose H, K are normal subgroups of G. Now, if $g \in G$, and $h \in H \cap K$, then we have that $ghg^{-1} \in H \cap K$, and hence $H \cap K$ is also a normal subgroup.

(b) The same idea as above can be used to prove that the intersection of an arbitrary collection of normal subgroups is a normal subgroup.

23. Suppose $\{K_\alpha\}_{\alpha \in I}$ is an arbitrary collection of normal subgroups of G, and let

$$M = \bigcup_{\alpha \in I} K_\alpha$$

We will show that $\langle M\rangle$ is also a normal subgroup. Suppose $g \in G$, and $m \in \langle M\rangle$. Then, $m = k_1 k_2 ... k_n$, where $k_i \in K_{\alpha_i}$, for $\alpha_i \in I$. Observe that

$$gmg^{-1} = g(k_1...k_n)g^{-1} = (gk_1g^{-1})...(gk_ng^{-1}) \in \langle M\rangle$$

because K_{α_i} is normal. So, $\langle M\rangle$ is a normal subgroup.

26. (c) Suppose $N = \langle S\rangle$ for some subset S of G. Suppose $N \trianglelefteq G$. Then, given any $s \in S$ and $g \in G$, we see that $gsg^{-1} \in N$, and hence $gSg^{-1} \subset N$. Conversely, suppose $gSg^{-1} \subset N$ for all $g \in G$. Then, given any $n \in N$, we have

$$n = s_1...s_n$$

for $s_1, ..., s_n \in N$, and hence

$$gng^{-1} = g(s_1...s_n)g^{-1} = (gs_1g^{-1})...(gs_ng^{-1}) \in N$$

and hence N is normal.

31. Suppose $H \leq G$ and $N \trianglelefteq H$. It then follows that $hNh^{-1} = N$ for all $h \in H$, and hence $H \leq N_G(N)$. Hence, $N_G(N)$ is the largest subgroup of G in which N is normal.

40. Suppose G is a group, and let N be a normal subgroup of G. Let $\overline{G} = G/N$.

Suppose $\overline{xy} = \overline{yx}$. This means that

$$xyN = yxN$$

which implies that $x^{-1}y^{-1}xy \in N$.

Conversely, if $x^{-1}y^{-1}(xy) \in N$, then $xy = yxk$, for some $k \in N$, and hence

$$xyN = yxN$$

Let's now define the *product* of two subgroups H and K of a group G. This product is defined as

$$HK = \{hk : h \in H \text{ and } k \in K\}$$

We will now prove a theorem regarding the cardinality of HK:

Theorem 16.7. Suppose H and K are subgroups of a group G. Then,

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

Proof: First, observe that

$$HK = \bigcup_{h \in H} hK$$

So, we need to count the distinct number of cosets of the form hK, for $h \in H$, and multiply that with $|K|$, since each coset contains $|K|$ elements. Now,

$$h_1K = h_2K \iff h_1 = h_2k$$

for some $k \in H \cap K$. Now, there are $|H|$ elements in H, and hence we have $|H|$ cosets with overcounting, and each coset is overcounted $|H \cap K|$ times. Hence, the distinct number of cosets is

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

and hence the formula follows.

Notice that for this formula to work, HK need not be a subgroup of G. We now present a condition in which HK will be a subgroup.

Theorem 16.8. HK is a subgroup of G if and only if $HK = KH$.

The proof of this fact is not difficult, and hence I am not writing it here.

We have a another sufficient condition to determine when HK is a subgroup:

Theorem 16.9. Suppose $K \leq G$ and $H \leq N_G(K)$. Then, HK is a subgroup of G.

Proof: If $hk \in HK$, then observe that $hk = (hkh^{-1})h$, and since $hkh^{-1} \in K$, it follows that $hk \in KH$, proving that $HK \subset KH$. Similarly, the reverse containment is proved. Hence, HK is a subgroup of G.

17. Exercises on Page 95

4. Suppose G is a group of order pq, where p and q are primes (not necessarily distinct). If $Z(G) = 1$ then we are done. So, suppose $Z(G)$ is non-trivial. It follows that $|Z(G)|$ is one of p, q or pq. If it is pq, then G is abelian, and we are done. If it is p, then the quotient group $G/Z(G)$ has order q, and hence it is cyclic, which implies that G is abelian. Similarly, the case $|Z(G)| = q$ can be handled. So, in all cases, G is abelian.

5. Suppose $H \leq G$, and let $g \in G$ be fixed.

(a) First, let us prove that $gHg^{-1} \leq G$. Clearly, $1 \in gHg^{-1}$. Secondly, if $k \in gHg^{-1}$, then $k = ghg^{-1}$, for some $h \in G$, and hence

$$k^{-1} = gh^{-1}g^{-1} \in gHg^{-1}$$

so that it is closed under inverses. Finally, that it is closed under the group operation is not hard to see. Hence, it is a subgroup.

Consider the mapping from H to gHg^{-1} given by

$$h \mapsto ghg^{-1}$$

It is clear that this mapping is one-one and onto. Hence, the order of the two subgroups is the same.

(b) Now, if $n \in \mathbb{Z}^+$, and if H is the unique subgroup of order n, then observe that $gHg^{-1} = H$, for all $g \in G$, which means that $N_G(H) = G$, and hence $H \trianglelefteq G$.

6. Let $H \leq G$ and let $g \in G$. Suppose $Hg = kH$, for some $k \in G$. We will show that $gH = Hg$, and that $g \in N_G(H)$. Since $Hg = kH$, we have that

$$g = kh_1$$

for some $h_1 \in H$, and hence

$$k = gh_1^{-1}$$

which means that $kH = gH$. Hence, it follows that $gH = Hg$. As we have proven earlier, this condition is equivalent to the fact that $g \in N_G(H)$.

8. Suppose H and K are finite subgroups of G such that their orders are relatively prime, and let $|H| = p$ and $|K| = q$. Now, $H \cap K$ is a subgroup of both H and K, so its order should divide both p and q. The only possible way this is true is when $H \cap K = 1$, and hence $H \cap K = 1$.

10. Suppose H and K are subgroups of G with finite index, where G can also be an infinite group. Let $|G : H| = m$ and $|G : K| = n$.

18. The Isomorphism Theorems

These theorems are a set of observations about the relationships between groups and their quotient groups:

Theorem 18.1. *First Isomorphism Theorem*: Suppose $\phi : G \to H$ is a homomorphism. Then,

$$G/\mathrm{Ker}(\phi) \cong \mathrm{Im}(\phi)$$

This theorem is very easy to prove, and I will not write the proof here. One property that we can immediately verify however is the fact that

$$|G : \mathrm{Ker}(\phi)| = |\phi(G)|$$

There is a commutative diagram which is very useful for interpreting the first isomorphism theorem.

Now, let us prove the *Second Isomorphism theorem*:

Theorem 18.2. *Diamond Isomorphism Theorem*: Suppose A, B are subgroups of a group G, such that $A \leq N_G(B)$. Then, AB is a subgroup of G, and we have the following relations:

(1) $B \trianglelefteq AB$.
(2) $A \cap B \trianglelefteq A$.

(3) $AB/B \cong A/(A \cap B)$.

Remark: It is not necessary that $A \trianglelefteq AB$.

Proof: Suppose A and B are subgroups of G such that $A \leq N_G(B)$. It then follows that AB is a subgroup of G, and also $A, B \leq AB$.

First, let us show that $B \trianglelefteq AB$. So, suppose $a'b' \in AB$, and let $b \in B$. So, we have $(a'b')b(b'^{-1}a'^{-1}) \in B$, and hence $B \trianglelefteq AB$.

Now, consider the natural projection map from $\pi : AB \to AB/B$, and consider the restriction of π to, A, i.e consider

$$\pi : A \to AB/B$$

If $xB \in AB/B$, then we know that $x = ab$, for some $a \in A$ and $b \in B$. And hence,

$$xB = abB = (aB)(bB) = aB$$

which implies that this restriction is surjective. Also, observe that $\text{Ker}(\phi) = A \cap B$, so that $A \cap B \trianglelefteq A$. By the first isomorphism theorem, we have

$$A/A \cap B \cong \text{Im}(\phi) = AB/B$$

and this completes the proof. The reason why this is called the Diamond Isomorphism theorem (or also the Parallelogram Isomorphism theorem) is because of the lattice structure of the mentioned subgroups.

The *Third Isomorphism Theorem* is concerned with taking quotient groups of quotient groups:

Theorem 18.3. *Third Isomorphism Theorem*: Let G be a group, and let H, K be normal subgroups of G such that $H \leq K$. Then, $K/H \trianglelefteq G/H$, and we have

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

Remark: This is just like cancelling in fractions.

Proof: First, let us show that $K/H \trianglelefteq G/H$. So, suppose $gH \in G/H$ and $kH \in K/H$. Then, observe that

$$(gH)(kH)(gH)^{-1} = (gkg^{-1})H \in K/H$$

and hence $K/H \trianglelefteq G/H$.

So, the quotient group $(G/H)/(K/H)$ is well-defined. Now, consider the map $\phi : G/H \to G/K$ given by

$$\phi(gH) = gK$$

First, let us show that this map is well defined. So, let $g_1H = g_2H$. This means that $g_1g_2^{-1} \in H$, and hence $g_1g_2^{-1} \in K$, since $H \leq K$, and hence $g_1K = g_2K$.

The map is clearly surjective. Also, it is a homomorphism, since

$$\phi(g_1Hg_2H) = \phi(g_1g_2H) = g_1g_2K = \phi(g_1H)\phi(g_2H)$$

and its kernel is given by

$$\text{Ker}(\phi) = K/H$$

Hence, by the First Isomorphism theorem, we have

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

The last isomorphism theorem, called the *Lattice Isomorphism theorem*, gives the group structure of G/N in terms of the structure of G. This theorem is very useful to determine the lattice of G/N given the lattice or G:

Theorem 18.4. *Fourth Isomorphism Theorem*: Suppose G is a group, and let N be a normal subgroup of G. Every subgroup of $\overline{G} = G/N$ is of the form $\overline{A} = A/N$, where A is a subgroup of G containing N. The following are true for all $A, B \leq G$ with $N \leq A$ and $N \leq B$:

(1) $A \leq B$ if and only if $\overline{A} \leq \overline{B}$.
(2) If $A \leq B$, then $|B : A| = |\overline{B} : \overline{A}|$
(3) $\overline{\langle A, B\rangle} = \langle \overline{A}, \overline{B}\rangle$.
(4) $A \trianglelefteq G$ if and only if $\overline{A} \trianglelefteq \overline{G}$.

Proof: First, let us give a bijection ϕ from the subgroups of G containing N to subgroups of G/N. Let π be the natural projection homomorphism from $G \to G/N$.

For $A \leq G$ such that $N \leq A$, define

$$\phi(A) = \pi(A)$$

where $\pi(A)$ is the image of A under the natural homomorphism. Let us show that $\pi(A)$ is a subgroup of G/N.

Clearly, $N \in \pi(A)$, because $1 \in A$. Next, if $gN \in \pi(A)$, then $gN = g'N$, for some $g' \in A$. So, $(gN)^{-1} = (g'N)^{-1} = g'^{-1}N \in \pi(A)$, because $g'^{-1} \in A$. If $aN, bN \in A$, then $aN = g_1N$ and $bN = g_2N$, for some $g_1, g_2 \in A$. So, $(aN)(bN) = (g_1g_2)N \in \pi(A)$, because $g_1g_2 \in A$. So, it follows that $\pi(A)$ is a subgroup of G/N.

Remark: Before continuing the proof, I will make the following remark. Note that, in the previous paragraph, we never used the fact that A contains N. This is infact true; any subgroup A of G can be mapped to a subgroup of G/N by its image under the natural homomorphism. But, to get a bijection, we only deal with subgroups containing N, as we will see further in the proof.

Now, let us show that ϕ is a bijection (Here is the importance of using only those subgroups which contain N). Suppose $\pi(A) = \pi(B)$. Now, let $a \in A$. So, $aN \in \pi(A)$, and hence $aN \in \pi(B)$. This means that $aN = a_1B$, for some $a_1 \in B$. Hence, $a = a_1n$, for some $n \in N$, and since $N \leq B$, it follows that $a \in B$, and hence $A \leq B$. Similarly, the reverse containment may be proven, and hence $A = B$, so that this map is injective. To show that this map is surjective, suppose $\overline{H} \leq G/N$. Then, we know that the complete pre-image, $\pi^{-1}(H)$, is a subgroup of G (the pullback in a homomorphism is a subgroup), and this subgroup contains N (because $\overline{H}$ contains the coset N). Hence, we then get $\overline{H} = \phi(\pi^{-1}(\overline{H}))$, and hence the map is surjective. So, it follows that the subgroups of G/N are in bijection with subgroups of G containing N.

To prove (1), suppose $A \leq B$. Let $aN \in A/N$. So, $aN \in B/N$, and hence $A/N \leq B/N$. Conversely, if $A/N \leq B/N$, it is easy to see that $A \leq B$, and hence we are done.

To prove (2), if $A \leq B$, then we have $A/N \leq B/N$ by (1). Also,

$$|B : A| = \frac{|B|}{|A|} = \frac{|N||B|}{|N||A|} = \frac{|B/N|}{|A/N|} = |B/N : A/N|$$

and we are done.

The proofs of (3) and (4) are not difficult but a bit involved, so I'll skip that.

To prove (5), suppose $A \trianglelefteq G$. Let $aN \in A/N$ and $gN \in G/N$, so that $aN = a_1N$, for some $a_1 \in A$. Observe that

$$(gN)(aN)(gN)^{-1} = (ga_1g^{-1})N \in A/N$$

because $ga_1g^{-1} \in A$. So, $A/N \trianglelefteq G/N$.

Conversely, suppose $A/N \trianglelefteq G/N$. Let $a \in A$, and let $g \in G$. Observe that

$$(gN)(aN)(gN)^{-1} = (gag^{-1}N) \in A/N$$

because $A/N \trianglelefteq G/N$. So,

$$gag^{-1}N = a_1N$$

for some $a_1 \in A$, and hence $gag^{-1} = a_1n$, for some $n \in N$. Because $N \leq A$, it follows that $a_1n \in A$, and hence $gag^{-1} \in A$, proving that $A \trianglelefteq G$. (Note that, here we again used the fact that $A \leq G$).

19. Exercises on page 101

1. Let F be a finite field of order q and let $n \in Z^+$. We know that det is a homomorphism from $\mathrm{GL}_n(F)$ to $F - \{0\}$, and the kernel is $\mathrm{SL}_n(F)$. By the first isomorphism theorem, we have

$$|GL_n(F) : SL_n(F)| = |\mathrm{Im}(\det)| = q - 1$$

because det is surjective.

3. Suppose $H \trianglelefteq G$ such that $|G : H| = p$ for some prime p. First, let us show that if $K \leq G$ such that $H \leq K$, then either $K = H$ or $K = G$ (H is a maximal subgroup). To prove this, consider the group G/H. The order of this group is p, and hence the only subgroups of G/H is the trivial group and the whole group. If $H \leq K \leq G$, then K/H is a subgroup of G. So, either $K/H = 1$ or $K/H = G/H$. In the first case, we have $K = H$, and in the second case, we have $K = G$ (by the fourth isomorphism theorem).

Now, suppose $K \leq G$. Then, either $K \leq H$, or there is some $k \in K$ such that $k \notin H$. In that case, H is a proper subgroup of HK, and by what we proved above, it follows that $G = HK$. By the second isomorphism theorem, we have

$$HK/H \cong K/H \cap K$$

and hence

$$|HK : H| = p = |K : K \cap H|$$

4. Let $C \trianglelefteq A$ and $D \trianglelefteq B$. We will show that $C \times D \trianglelefteq A \times B$. Suppose $(c, d) \in C \times D$ and let $(a, b) \in A \times B$. We have

$$(a, b)(c, d)(a, b)^{-1} = (aca^{-1}, bdb^{-1}) \in C \times D$$

and hence $C \times D \trianglelefteq A \times B$.

Now, define the map $\phi : A \times B \to A/C \times B/D$ by

$$(a, b) \mapsto (aC, bD)$$

It is clear that this is a well defined map, and a homomorphism. The kernel of this map is $C \times D$, and hence by the first isomorphism theorem, we have

$$(A \times B)/(C \times D) \cong A/C \times B/D$$

because ϕ is surjective.

7. Suppose M, N are normal subgroups of G such that $G = MN$. We will show that

$$G/(M \cap N) \cong (G/M) \times (G/N)$$

Consider the map $\phi : G \to G/M \times G/N$ defined by

$$g \mapsto (gM, gN)$$

Clearly, the map is a well defined homomorphism, and the kernel is $M \cap N$. Let's prove that the map is onto (here is when we use the requirement that $G = MN$).

Suppose $a, b \in G$. We have that $b^{-1}a \in MN = NM$, and hence $b^{-1}a = n_1 m_1$, for some $n_1 \in N$ and $m_1 \in M$. Hence, we have

$$am_1^{-1} = bn_1 = p$$

So, we have

$$\phi(p) = (pM, pN) = (aM, bN)$$

and hence this map is onto. By the first isomorphism theorem, we have

$$G/M \cap N \cong G/M \times G/N$$

8. Suppose p is a prime and let $G = \{z \in \mathbb{C} |\ z^{p^n} = 1 \text{ for some } n\}$. Consider the map from G to G given by

$$z \mapsto z^p$$

It is clear that the map is a homomorphism. To prove that it is surjective, let $z \in G$, and consider $z^{\frac{1}{p}}$. Given that $z^{p^n} = 1$ for some n, observe that

$$(z^{\frac{1}{p}})^{p^{n+1}} = z^{p^n} = 1$$

proving that the homomorphism is surjective. Now, the kernel of this homomorphism is the set of all p^{th} roots of unity. So, the kernel is proper, and hence

$$G/\text{kernel} \cong G$$

and hence G is isomorphic to a proper quotient of itself.

9. Suppose G is a group of order $p^a m$, where a is the highest power of p dividing $|G|$. Suppose P is a subgroup of G of order p^a, and let N be a normal subgroup of G of order $p^b n$, where b does not divide n. Observe that both $|P|$ and $|N|$ divide $|PN|$, and hence $|PN| = p^a k$, where $n|k$ and p does not divide k. Also, we know that $|P \cap K| = p^l$, for some $l \leq b$. Now, we have

$$|P \cap N| = \frac{|P||N|}{|PN|} = \frac{p^b n}{k}$$

and since $(k, p^b) = 1$, it follows that $k|n$ and hence $k = n$. So, $|P \cap N| = p^b$, and hence $|PN/N| = p^{a-b}$.

20. Composition Series

First, we will see the proof of Cauchy's theorem for finite abelian groups using induction; the basic philosophy is this: if you know some information about subgroups/quotient groups of a group, then there are cases where this information can be forced to the bigger group. Let's see an example of this:

Theorem 20.1. Cauchy's Theorem (for finite abelian groups): Let G be a finite abelian group. If p is a prime divisor of $|G|$, then G contains a subgroup of of order p.

Proof: If $|G| = p$ then we are done. So, we assume that $|G| > p$.

First, let x be any non-identity element of G. If $|x| = p$, we are done. If p divides $|x|$, then again we are done by induction. So, suppose p does not divide $|x|$. Consider the quotient group $G/\langle x\rangle$ (because G is abelian, every subgroup is normal). Clearly, p divides $|G/\langle x\rangle|$, and by induction hypothesis, this group contains a subgroup of order p. This subgroup must be cyclic, and let it be $\{1\langle x\rangle, g\langle x\rangle, ..., g^{p-1}\langle x\rangle\}$ So, we observe that $g \notin \langle x\rangle$ but $g^p \in \langle x\rangle$. It follows that $\langle g^p\rangle \neq \langle g\rangle$, which means that $\langle g^p\rangle$ is a proper subgroup of $\langle g\rangle$. So, it follows that $(|g|, p) > 1$, and hence p divides $|g|$. We are again done by induction hypothesis.

A group G is called *simple* if $|G| > 1$ and the only normal subgroups of G are 1 and G. If $|G|$ is a prime, then it is easy to see that G is simple. Simple groups have the property that they cannot be factored into subgroups like N or G/N, and hence they are just like primes in integers.

Let G be a group. A sequence of subgroups

$$1 = N_0 \leq N_1 \leq ... \leq N_k = G$$

is called a composition series if $N_i \trianglelefteq N_{i+1}$ for every i, and each group N_{i+1}/N_i is simple.

Next, we look at *solvable groups*. A group G is said to be *solvable* if there is a chain of subgroups

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq ... \trianglelefteq G_s = G$$

such that G_i/G_{i-1} is *abelian* for every i. Solvable groups present themselves in Galois Theory.

We have the following proposition which is again an example of how information about smaller groups can be put together to a larger group:

Proposition 20.2. If $N \trianglelefteq G$ and both N and G/N are solvable, then G is also solvable.

Proof: Let $1 = H_0/N \trianglelefteq H_1/N \trianglelefteq ... \trianglelefteq H_{k_1}/N = G/N$ be a sequence of subgroups such that $(H_i/N)/(H_{i-1}/N) \cong H_i/H_{i-1}$ is abelian for every i. Here, each H_i is a normal subgroup of G containing N. Combining this with such a series for N, we obtain a series for G, proving that G is solvable.

21. Exercises on Page 106

1. Suppose G is an abelian simple group. We show that $G \cong Z_p$ for some prime p. Note that any subgroup of G must be normal, and hence the only subgroups of G are G and 1. Hence G must be a cyclic group. Moreover, it cannot be the infinite cyclic group, and hence it is finite. In that case, it is clear that $G \cong Z_p$ for some prime p.

2. Here we find all 3 composition series for Q_8 and all seven composition series for D_8 and list the composition factors.

4. Let G be a finite abelian group, and let n be a positive divisor of $|G|$. We will show that G contains a subgroup of order n. If n is prime then this is just Cauchy's theorem for finite abelian groups. So, suppose n is not a prime, and let p be a prime dividing n. Then, there is an element of order p, and hence a subgroup of order p. Let this subgroup be K. Then n/p divides the order of G/K, and hence G/K has a subgroup of order n/p (by induction), so that G has a subgroup of n.

5. Here we show that subgroups and quotient groups of solvable groups are solvable.

Let G be a solvable group, and let

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq ... \trianglelefteq N_k = G$$

be a series of subgroups such that N_i/N_{i-1} is abelian. Let $H \leq G$, and consider the series

$$1 = H \cap N_0 \trianglelefteq H \cap N_1 \trianglelefteq ... \trianglelefteq H \cap N_k = H$$

22. Alternating Group

In this section, let us study the permutation group in more detail. Let Δ be the following polynomial of n independent variables:

$$\Delta = \prod_{1 \leq i < j \leq n} (x_i - x_j)$$

So, Δ contains all factors of the form $x_i - x_j$, for all $i < j$. Let the group S_n act on Δ as follows: if $\sigma \in S_n$, define

$$\sigma(\Delta) = \prod_{1 \leq i < j \leq n} (x_{\sigma(i)} - x_{\sigma(j)})$$

The following observation can be made for all $\sigma \in S_n$

$$\sigma(\Delta) = \pm\Delta$$

We define the *sign* of σ as the sign occuring in the above equation (this is one way of defining the sign of a permutation. There is another beautiful way of defining it using determinants, which is inluded in my Linear Algebra notes).

Theorem 22.1. $\epsilon : S_n \to \{-1, 1\}$ is a homomorphism.

Proof: The proof of this fact is easy using the determinant definition of the sign of a permutation, which is given in my Linear Algebra notes.

We also know that all transpositions are odd permutations. Hence, it follows that ϵ is a surjective homomorphism.

We define the *Alternating* group A_n to be the kernel of the homomorphism $\epsilon : S_n \to \{-1, 1\}$. By the first isomorphism theorem, we have

$$S_n/A_n \cong \{-1, 1\}$$

and hence

$$|A_n| = \frac{S_n}{2}$$

Let us now determine a quick way of finding the sign of a permutation from its cycle decomposition:

Theorem 22.2. Let $(a_1\ a_2\ ...\ a_k)$ be a cycle in S_n. Then, the sign of this cycle is $(-1)^{k-1}$.

Proof: Observe that

$$(a_1\ a_2\ ...\ a_k) = (a_1\ a_2)(a_2\ a_3)...(a_{k-1}\ a_k)$$

and hence the sign of the cycle is $(-1)^{k-1}$.

Using the above fact, we can find the sign of any permutation very easily.

23. Group Actions

Let's begin by proving the following fundamental relationship between actions and homomorphisms into the symmetric group:

Theorem 23.1. For any group G and any non-empty set A there is a bijection between the actions on G on A and the homomorphisms of G into S_A.

Proof: Given an action A_1 of G on A, there is a homomorphism from G to S_A, which is nothing but the permutation representation of A_1. Let's show that this map from the set of actions to homomorphisms is one-one and onto. First, suppose A_1 and A_2 are two actions having the same permutation representations. Given any $g \in G$, we have

$$\sigma_{g,A_1} = \sigma_{g,A_2}$$

which implies that

$$\sigma_{g,A_1}(a) = \sigma_{g,A_2}(a)$$

for all $a \in A$, and hence the two actions are the same. So, this map is one-one.

To show that the map is onto, let $\phi : G \to S_A$ be any homomorphism. Define a map $A_1 : G \times A \to A$ as

$$A_1(g, a) = \phi(g)(a)$$

Then, observe that

$$A_1(1, a) = \phi(1)(a) = a$$

If $g_1, g_2 \in g$, then

$$A_1(g_1, A_1(g_2, a)) = A_1(g_1, \phi(g_2)(a)) = \phi(g_1)(\phi(g_2)(a)) = \phi(g_1 g_2)(a) = A_1(g_1 g_2, A)$$

and hence A_1 is a group action. This completes the proof.

Let's now see how equivalence relations can be defined using group actions:

Theorem 23.2. Let G be a group acting on a set A. For $a, b \in G$, we say that $a \sim b$ if $a = g \cdot b$, for some $g \in G$. This relation is an equivalence relation, and the number of elements in the equivalence class of a is $|G : G_a|$, which is the index of G_a.

Proof: First, observe that $a = 1 \cdot a$, and hence the relation is symmetric. Second, if $a = g \cdot b$, then observe that $b = g^{-1} \cdot a$, and hence the relation is symmetric. Finally, if $a = g_1 \cdot b$ and $b = g_2 \cdot c$, then we have that $a = (g_1 g_2) \cdot c$, and the relation is transitive. So, it is an equivalence relation.

Now, we will show a bijection between the equivalence class of a and the left cosets of G_a in G. Let

$$C_a = \{g \cdot a | \, g \in G\}$$

be the equivalence class of a. For $b \in C_a$ such that $b = g \cdot a$, consider the map $b \mapsto gG_a$. This map is clearly surjective. It is injective because if $g_1 G_a = g_2 G_a$, then $g_1 = g_2 h$, for some $h \in G_a$, and hence

$$g_1 \cdot a = (g_2 h) \cdot a = g_2 \cdot a$$

and hence it follows that the number of elements in the equivalence class of a is the index of G_a.

The equivalence class containing a is called the *orbit* of a. An action which produces only one orbit is said to be *transitive*.

Using this theory, the existence of a unique (upto ordering) cycle decomposition of a permutation can be proven. A good proof is given on page 115 of the book.

24. Exercises on Page 116

1. Suppose G is a group acting on a set A. In this exercises, we will see the relationship between stabilizers of two related elements under this action.

Suppose $b = g \cdot a$, where $a, b \in A$ and $g \in G$. We will show that

$$G_b = gG_ag^{-1}$$

So, suppose $g_0 \in G_b$. Then, $g_0 \cdot b = b$. So, we have that

$$g_0 \cdot (g \cdot a) = g \cdot a$$

and hence

$$(g_0 g) \cdot a = g \cdot a$$

Letting g^{-1} act on both sides, we get

$$(g^{-1}g_0 g) \cdot a = a$$

and hence $g^{-1}g_0 g \in G_a$, which means that $g_0 \in gG_ag^{-1}$. Conversely, if $g_0 = gg'g^{-1}$ for some $g' \in G_a$, then we have

$$g_0 \cdot b = (gg'g^{-1}) \cdot b = (gg') \cdot a = g \cdot a = b$$

and hence $g_0 \in G_b$. This completes the proof.

Now, suppose G acts transitively on A. So, for any $b \in A$, we have $b = g \cdot a$ for some $g \in G$. Now, the kernel of the action is nothing but

$$\ker = \bigcap_{b \in A} G_b$$

and hence we get

$$\ker = \bigcap_{g \in G} gG_ag^{-1}$$

2. Let G be a permutation group on the set A. Let $\sigma \in G$ and let $a \in A$. Observe that

$$\sigma(a) = \sigma \cdot a$$

and hence by the preceding exercise, we have

$$G_{\sigma(a)} = \sigma G_a \sigma^{-1}$$

If G acts transitively on A, then the kernel of the action is

$$\bigcap_{\sigma \in G} \sigma G_a \sigma^{-1}$$

But, G being a permutation group, acts faithfully on A. So, the kernel must be trivial, and hence

$$\bigcap_{\sigma \in G} \sigma G_a \sigma^{-1} = 1$$

3. Let G be an abelian transitive subgroup of S_A.

We will show the following: for every element $a \in A$, $G_a = \{1\}$, where 1 is the identity permutation. So, let $\sigma \in G_a$ for some $a \in G$. Since the action of G is transitive, for any $b \in A$, we have that $b = \sigma'(a)$, for some $\sigma' \in G$. It then follows that

$$G_b = \sigma' G_a \sigma'^{-1}$$

which means that $\sigma'\sigma\sigma'^{-1} \in G_b$. Since G is abelian, we have

$$\sigma'\sigma\sigma'^{-1} = \sigma$$

and hence $\sigma \in G_b$. Since b was arbitrary, it follows that σ is the identity permutation. So, $G_a = \{1\}$ for all $a \in G$.

Now, the action is transitive, and hence there is only one orbit. So, it follows that

$$|A| = |G : G_a| = |G|$$

4. Let S_3 act on the set $\Omega = \{(i,j) |\, 1 \leq i, j \leq 3\}$. There are two orbits of Ω under this action:

$$\{(1,1),(2,2),(3,3)\}, \{(1,2),(1,3),(2,1),(2,3),(3,1),(3,2)\}$$

Let the ordered pairs be labelled in the ordering as given above. Let $\phi : \Omega \to S_9$ be the permutation representation. We will find the cycle decomposition of $\phi(\sigma)$ for each $\sigma \in S_3$.

$$\begin{aligned}
\phi(1) &= 1 \\
\phi((1\ 2)) &= (1\ 2)(4\ 6)(5\ 7)(8\ 9) \\
\phi((1\ 3)) &= (1\ 3)(4\ 9)(5\ 8)(6\ 7) \\
\phi((2\ 3)) &= (2\ 3)(4\ 5)(6\ 8)(7\ 9) \\
\phi((1\ 2\ 3)) &= (1\ 2\ 3)(4\ 7\ 8)(5\ 6\ 9) \\
\phi((1\ 3\ 2)) &= (1\ 3\ 2)(4\ 8\ 7)(5\ 9\ 6)
\end{aligned}$$

Finally, observe that

$$G_{(1,1)} = \{1, (2\ 3)\}$$

and

$$G_{(1,2)} = \{1\}$$

All other stabilizers are conjugates of these (since there are only two orbits).

7. Suppose G is a transitive permutation group acting on the finite set A.

(a) Suppose B is a block containing the element a of A. Define the set $G_B = \{\sigma \in G |\, \sigma(B) = B\}$. Clearly, the identity permutation is in G_B. If $\sigma_1, \sigma_2 \in G_B$, then it is easy to see that $\sigma_1\sigma_2 \in G_B$. That it is closed under inverses is also easy to see. Now, if $\sigma \in G_a$, then $\sigma(a) = a \in B$, and hence $\sigma(B) \cap B \neq \phi$, and therefore $\sigma(B) = B$ (because B is a block), showing that $\sigma \in G_B$. So, $G_a \leq G_B$.

Now, we will look at groups acting on themselves. As we have seen before, a group can act on itself via left multiplication. It turns out that this action is faithful and transitive, as we will prove.

We will generalise the above concept as follows: Let G be a group, and let $H \leq G$. We can define an action of G on the set of left cosets of H as follows:

$$g \cdot aH = gaH$$

It is clear that this is indeed an action. Let's prove some properties of this action:

Theorem 24.1. Suppose $H \leq G$, and let G act on the set of left cosets of H, which we denote by A. Let π_H be the associated permutation representation of the action.

(1) G acts on A transitively.
(2) The stabilizer of $1H$ is H. (and hence since the action is transitive, the stabilizer of any other point is a conjugate of H).
(3) The kernel of π_H is $\cap_{x\in G} xHx^{-1}$, and this kernel is the largest normal subgroup of G contained in H.

Proof: To prove (1), let a_1H and a_2H be any two left cosets of H. Observe that

$$a_2H = (a_2a_1^{-1}) \cdot a_1H$$

and hence the action is transitive.

To prove (2), observe that

$$\begin{aligned} G_{1H} &= \{g \in G |\, g \cdot 1H = H\} \\ &= \{g \in G |\, gH = H\} \\ &= H \end{aligned}$$

Finally, observe that $\ker(\pi_H)$ is the intersection of all stabilizers, and since the action is transitive, the stabilizers are conjugates of H. So, we have

$$\ker(\pi_H) = \bigcap_{x\in G} xHx^{-1}$$

First, it is immediate that $\ker(\pi_H) \trianglelefteq G$. Now, let N be any normal subgroup of G contained in H. If $h \in N$, then for any left coset aH we have

$$h \cdot aH = haH = aH$$

implying that $h \in \ker(\phi_H)$, and hence $N \leq \ker(\pi_H)$. This completes the proof.

Let us now prove **Cayley's theorem**:

Theorem 24.2. Cayley: 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: Consider the action of G on itself by left-multiplication. The kernel of this action is just the trivial group. If π is the permutation representation, then $\ker(\pi) = 1$, and by the first isomorphism theorem we have

$$G \cong G/\ker(\pi) \cong H$$

where H is the subgroup of some symmetric group. This completes the proof.

The next theorem is a generalisation to the normality of subgroups of index 2, and is a very useful tool:

Theorem 24.3. Let G be a group, and let H be a subgroup of index p, where p is the smallest prime dividing $|p|$. Then H is normal.

Proof: Let π_H be the permutation representation of the action of G on the left cosets of H. We will prove that H is normal by proving that $H = \mathrm{Ker}\pi_H$.

First, we know that $K \leq H$, and let $|H : K| = k$. So, we have that

$$|G : K| = |G : H||H : K| = pk$$

Since H has p distinct left cosets, it follows that the group G/K is isomorphic to some subgroup of S_p (by the first isomorphism theorem). This means that $pk|p!$, which implies that $k|(p-1)!$. Now, all prime factors of k must be greater than or equal to p

(since p is the smallest prime dividing G) and hence we see that $k = 1$. So, it follows that $H = K$, and hence $H \trianglelefteq G$.

Exercises on Page 121

1. Let $G = \{1, a, b, c\}$ be the Klein 4-group.

(a) We label $\{1, a, b, c\}$ as $\{1, 2, 4, 3\}$. We consider the left regular representation π of this group. The elements are mapped as

$$\begin{aligned}\pi(1) &= 1\\ \pi(a) &= (1\ 2)(3\ 4)\\ \pi(b) &= (1\ 4)(2\ 3)\\ \pi(c) &= (1\ 3)(2\ 4)\end{aligned}$$

(b) We relabel the group as $\{1, 4, 2, 3\}$. Then, the elements are mapped as

$$\begin{aligned}\pi(1) &= 1\\ \pi(a) &= (1\ 4)(2\ 3)\\ \pi(b) &= (1\ 2)(3\ 4)\\ \pi(c) &= (1\ 3)(2\ 4)\end{aligned}$$

Clearly, the image or the representation is the same as in part **(a)**, even though the representations are different.

4. Consider the left regular representation of Q_8, which we denote by π. If we label the points $\{1, -1, i, -i, j, -j, k, -k\}$ as $\{1, 2, 3, 4, 5, 6, 7, 8\}$, we get that

$$\begin{aligned}\pi(1) &= 1\\ \pi(-1) &= (1\ 2)(3\ 4)(5\ 6)(7\ 8)\\ \pi(i) &= (1\ 3\ 2\ 4)(5\ 7\ 6\ 8)\\ \pi(-i) &= (1\ 4\ 2\ 3)(5\ 8\ 6\ 7)\\ \pi(j) &= (1\ 5\ 2\ 6)(3\ 8\ 4\ 7)\\ \pi(-j) &= (1\ 6\ 2\ 5)(3\ 7\ 4\ 8)\\ \pi(k) &= (1\ 7\ 2\ 8)(3\ 5\ 4\ 6)\\ \pi(-k) &= (1\ 8\ 2\ 7)(3\ 6\ 4\ 5)\end{aligned}$$

So, the subgroup $\langle \pi(i), \pi(j) \rangle$ of S_8 is isomorphic to Q_8.

7. **(a)** By Cayley's theorem, Q_8 is isomorphic to a subgroup of S_8.

(b) Here, we will show that Q_8 is not isomorphic to a subgroup of S_n, for any $n \leq 7$.

For the sake of contradiction, suppose Q_8 *is* isomorphic to some subgroup of S_7, say I. Let I act on a set with 7 elements in the usual way, and hence we get an action of Q_8 on the set. The corresponding permutation representation $\pi : Q_8 \to I$ is a surjective map. Now, we will show that $\langle -1 \rangle \leq \ker\pi$.

8. Suppose $H \leq G$ has finite index n. We will show that there is a normal subgroup $K \leq G$ with $K \leq H$ and $|G : K| \leq n!$.

Consider the action of G on the left cosets of H. Let π be the corresponding permutation representation of this action. Then, $\pi : G \to S_n$, because there are n left cosets of H. Consider $\ker\pi$, which is a normal subgroup of G. Clearly, $\ker\pi \leq H$, and observe that $G/\ker\pi$ is isomorphic to some subgroup of S_n, which implies that

$$\frac{|G|}{|\ker\pi|} \leq n!$$

and hence $\ker\pi$ is the required subgroup.

9. Suppose G is a group of order p^α. Then, p is the smallest prime dividing $|G|$. So, any subgroup of order p must be normal. Now, any group of order p^2 contains a group of order p, and hence this subgroup must be normal.

10. Let G be a non-abelian group of order 6. We will show that G has a non-normal subgroup of order 2.

Next, we will consider another important type of group action, called *conjugation*. Let G be a group. Then, the action of G on itself via conjugation, i.e

$$g \cdot a = gag^{-1}$$

defines another action. The orbits under this action are also called *conjugacy classes*. Note that these actions are *not transitive* unless $|G| = 1$, because the orbit of 1 is just $\{1\}$.

We again generalise the action by conjugation to subsets of G. For any $S \subset G$, define

$$g \cdot S = gSg^{-1}$$

Let's now prove a combinatorial result related to this action:

Theorem 24.4. The number of conjugates of a set S in G is equal to $|G : G_s|$, and since $G_s = N_G(S)$, this is equal to $|G : N_G(S)|$. In particular, the number of conjugates of an element s of G is equal to $|G : C_G(s)|$

The conjugation group action and the previous result give the *Class equation*:

Theorem 24.5. *The Class Equation*: Let G be a finite group, and let $g_1, ..., g_k$ be the representatives of distint conjugacy classes of G, such that no g_i is in the $Z(G)$. Then, we have

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

Proof: We know that distinct conjugacy classes partition the group. Let $g_1, ..., g_k$ be representatives of distinct conjugacy classes of G, such that no g_i is in $Z(G)$, and let the conjugacy classes be $K_1, ..., K_k$. Observe that every element in $Z(G)$ has a conjugacy class consisting of itself. So, let $1, z_1, z_2, ..., z_r$ be the elements of $Z(G)$. So, a partition of G is

$$\{1\}, \{z_1\}, ..., \{z_r\}, K_1, ..., K_k$$

so we get

$$|G| = |Z(G)| + \sum_{i=1}^{k} |K_i|$$
$$= |Z(G)| + \sum_{i=1}^{k} |G : C_G(g_i)|$$

and hence we are done.

The class equation has a very important consequence on the groups of prime power order:

Theorem 24.6. Suppose G is a group such that $|G| = p^\alpha$, where p is a prime and $\alpha > 0$. Then, $Z(G)$ is non-trivial.

Proof: By the class equation, we have

$$|G| = |Z(G)| + \sum_{k=1}^{r} |G : C_G(g_k)|$$

where $g_1, ..., g_r$ are representatives of distinct conjugacy classes, and are not in the center. It follows that $C_G(g_k) \neq G$ for any k, and hence $|G : C_G(g_k)|$ is a power of p. Also, we know that p divides $|G|$, and so it implies that p divides $|Z(G)|$. So, $Z(G)$ is non-trivial.

This leads to an interesting corollary:

Theorem 24.7. Suppose G is a group of order p^2. Then G is abelian.

Proof: By the previous theorem, we know that the center is non-trivial. So, it follows that $G/Z(G)$ is cylic, which means that G is abelian.

We can actually prove a stronger statement: G is isomorphic to one of the groups Z_{p^2} or $Z_p \times Z_p$. If G has an element of order p^2, then it is isomorphic to Z_{p^2}. So, suppose G does not have any element of order p^2. Take any element x of order p, and take any element $y \notin \langle x \rangle$, so that y also has order p. Since $\langle x, y \rangle$ has order greater than p, it must be true that $P = \langle x, y \rangle$. Also, the product $\langle x \rangle \times \langle y \rangle$ has p^2 elements. The isomorphism between P and $\langle x \rangle \times \langle y \rangle$ is given by

$$(x^a, y^b) \mapsto x^a y^b$$

and hence it follows that $P \cong Z_p \times Z_p$.

Next, we will look at conjugation in S_n:

Theorem 24.8. Suppose σ is a permutation in S_n such that

$$\sigma = (a_1\ a_2\ ...)(b_1\ b_2\ ,)...$$

Let $\tau \in S_n$. The cycle decomposition of $\tau\sigma\tau^{-1}$ is

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

Proof: Suppose $\sigma(i) = j$. Then, we have

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

Hence, the proof is complete.

Using this theorem, we can see how conjugacy works in S_n. We define the notion of *cycle type* in S_n. Given a cycle σ in S_n consisting of k disjoint cycles (including the fixed elements), the *cycle type* of σ is defined as the sequence of integers $n_1 \leq n_2 \leq ... \leq n_k$, where n_i is the length of the i^{th} cycle in the decomposition.

Theorem 24.9. Two elements of S_n are conjugate if and only if they have the same cycle types. The number of conjugacy classes of S_n is equal to the number of partitions of n.

Note: Before proving the theorem, I will mention an interpretation of this, which makes it much more natural. As in linear algebra, two matrices are conjugates of each other, if they represent the same linear mapping, just the chosen basis are different. A very similar thing occurs in permutations. Suppose I have 4 objects, namely A, B, C and D. I label the objects in two ways: $\{1, 2, 3, 4\}$ and $\{1, 4, 2, 3\}$. Consider the permutation which swaps the first two objects. In the first labelling, this permutation is

$$(1\ 2)(3\ 4)$$

and in the second labelling, this permutation is

$$(1\ 4)(2\ 3)$$

These permutations as objects of S_4 are different, but the underlying permutation is the same. So, these must be conjugates of each other, and in fact this is true. We will now formally prove this idea:

Proof: Let σ and ϕ be two permutations in S_n having the same cycle types. Let the cycle type be $n_1 \leq n_2 \leq ... \leq n_k$. Write the product decomposition of both σ and ϕ in the order of the cycle type.

Now, we consider $\tau \in S_n$ defined as follows: for any element $i \in \{1, ..., n\}$, find the cycle in which it is located in the decomposition of σ. Suppose it is in the p^{th} cycle, and suppose within the cycle, it is located at the q^{th} position. We map i to the element present in the p^{th} cycle in the decomposition of ϕ located at the q^{th} position. It is hence clear that τ is a bijection, hence a permutation.

Also, by our construction, we have

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

and hence ϕ and σ are conjugates of each other.

To prove the second part of the theorem, observe that every cycle-type is a partition of n. So, it follows that the number of conjugacy classes of S_n is equal to the number of partitions of n.

The previous theorem gives us a very powerful to compute the order of the centralizers of various permutations (and not just the order, infact the whole centralizer). We prove this in the next theorem:

Theorem 24.10. Suppose σ is an m-cycle in S_n. Then, we have

$$|C_{S_n}(\sigma)| = m(n-m)!$$

In fact, we have

$$C_{S_n}(\sigma) = P = \{\sigma^i\tau |\ 0 \leq i \leq m-1,\ \tau \in S_{n-m}\}$$

Proof: Observe that the number of elements in the conjugacy class of σ is equal to the number of m-cycles, which is $\frac{n!}{m(n-m)!}$. So, we have that

$$|C_{S_n}(\sigma)| = \frac{|S|m(n-m)!}{n!} = m(n-m)!$$

Now, we know that $\{1, \sigma, ..., \sigma^{m-1}\}$ is a subset of $C_{S_n}(\sigma)$. Also, any permutation of S_n that is disjoint from σ commutes with it. Now, the total number of permutations

that are disjoint from σ are $(n-m)!$. So, we have

$$|P| = m(n-m)!$$

and hence it follows that $C_{S_n}(\sigma) = P$.

25. Exercises on Page 130

1. Suppose G has a left action on a set A, denoted by $g \cdot a$, and let $a \cdot g$ be the corresponding right action. We will show that the equivalence classes under both the actions are the same.

So, suppose $a = g \cdot b$ for some $g \in G$. Then, we have

$$g^{-1} \cdot a = b$$

which means that

$$a \cdot g = b$$

and hence a is related to b under the left action if and only if it is related to b under the right action.

2. In this exercise, we will find the conjugacy classes and their sizes in each of the groups:

(a) D_8: The center of the group is $\{1, r^2\}$. For an element x not in the center, we know that the size of the conjugacy class is $|D_8 : C_{D_8}(x)|$. Now, $\{1, r^2\} \leq C_{D_8}(x)$, and it is easy to see that $x \in C_{D_8}(x)$, so that for every such x, we have

$$|C_{D_8}(x)| = 4$$

So, the class equation of D_8 is

$$8 = 2 + 2 + 2 + 2$$

So, the conjugacy classes are:

$$\{1\}, \{r^2\}, \{r, r^3\}, \{s, sr^2\}, \{sr, sr^3\}$$

(b) Q_8 : The center of the group is $\langle -1 \rangle$. As before, it is easy to see that the order of the centralizer of every element not in the center is 4. So, the class equation is

$$8 = 2 + 2 + 2 + 2$$

The conjugacy classes are

$$\{1\}, \{-1\}, \{i, -i\}, \{j, -j\}, \{k, -k\}$$

(c) A_4: First, we note that the center of A_4 is trivial. Now, any element of A_4 is either a 3-cycle, or product of two 2-cycles. Clearly, a permutation is only conjugate to permutations of the same cycle-type. It can be then seen that the conjugacy classes are

$$\{1\}, \{(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}, \{(1\ 2\ 3), (1\ 3\ 4), (1\ 4\ 2), (2\ 4\ 3)\},$$
$$\{(1\ 3\ 2), (1\ 4\ 3), (1\ 2\ 4), (2\ 3\ 4)\}$$

3. First, we make some general remarks. Let A and B be groups, and let $A \times B$ be their direct product. Now, (x_1, y_1) and (x_2, y_2) are in the same conjugacy class in $A \times B$ if and only of x_1, x_2 are in the same conjugacy class in A and y_1, y_2 are in the same conjugacy class in B.

(a) $Z_2 \times S_3$: Since Z_2 is abelian, each element has a singleton conjugacy class. So, there are 12 singleton conjugacy classes of $Z_2 \times S_3$.

Similarly, given a direct product, the conjugacy classes can be determined from the conjugacy classes of the individual groups.

5. Suppose $Z(G)$ has index n. We know that if $x \in G$, the size of the conjugacy class is $C_G(x)$. But, $Z(G) \leq C_G(x)$, and hence $|C_G(x)| \geq |Z(G)|$. This means that

$$n = |G : Z(G)| \geq |G : C_G(x)|$$

so that the conjugacy class of x has atmost n elements.

6. Suppose G is a non-abelian group of order 15. Then, $|Z(G)|$ has order either $1, 3$ or 5. Clearly, $Z(G)$ cannot have order 3 or 5, because that would imply that $G/Z(G)$ is cyclic, which would imply that G is abelian. Hence, $|Z(G)| = 1$.

Now, let x be any non-identity element. Now, the conjugacy class of x must have order 3 or 5. So, we need to write 14 as a sum of $3s$ and $5s$. The only possible way this is true is

$$14 = 3 + 3 + 3 + 5$$

and so the class equation must be

$$15 = 1 + 3 + 3 + 3 + 5$$

8. Here, we will show that $Z(S_n) = 1$ for all $n \geq 3$. Suppose there is some permutation which commutes with all permutations of S_n. Let σ be the permutation. Assume that there some i which is not fixed, and let $\sigma(i) = j$, so that $j \neq i$. There are two possible cases:

(1) In this first case, $\sigma(j) = i$. Now, take any k distinct from i and j. Let β be a permutation which has $(i\ j\ k)$ as one of its cycles in its cycle decomposition. Observe that

$$\sigma\beta(i) = i$$

and

$$\beta\sigma(i) = k$$

so that $\sigma\beta \neq \beta\sigma$

(2) In the second case, suppose $\sigma(j) = k$, where k is distinct from i and j. Let β be a permutation that swaps i and j. So, we have

$$\sigma\beta(i) = k$$

and $\beta\sigma(i) = i$ and again $\sigma\beta \neq \beta\sigma$

So, this means that all elements must be fixed, and hence $Z(S_n) = 1$.

9. Let us show that

$$|C_{S_n}((1\ 2)(3\ 4))| = 8(n-4)!$$

where $n \geq 4$. We know that $|S_n : C_{S_n}(x)|$ is the size of the conjugacy class of x in S_n. If $x = (1\ 2)(3\ 4)$, then we know that the elements in its conjugacy class have the same cycle type. There are $\frac{1}{2}\binom{n}{4}\binom{4}{2}$ permutations having the cycle type $(2,2)$. So, it follows that

$$|C_{S_n}((1\ 2)(3\ 4))| = \frac{2n!}{\binom{n}{4}\binom{4}{2}} = 8(n-4)!$$

10. Suppose $\sigma = (1\ 2\ 3\ 4\ 5)$ is the 5-cycle in S_5. We will explicitly find the required $\tau \in S_5$.

(a) $\tau\sigma\tau^{-1} = \sigma^2$, and one possible τ is $\tau = (2\ 3\ 5\ 4)$
(b) $\tau\sigma\tau^{-1} = \sigma^2$, and one possible τ is $\tau = (2\ 5)(3\ 4)$
(c) $\tau\sigma\tau^{-1} = \sigma^{-2}$, and one possible τ is $\tau = (2\ 4\ 5\ 3)$

13. Here, we will find all finite groups having exactly two conjugacy classes. Observe that 1 is always in $Z(G)$, and hence it is in its own conjugacy class. Let x be any non-identity element. It follows that

$$\frac{|G|}{|C_G(x)|} = |G| - 1$$

which is only possible if $|G| - 1 = 1$, i.e when $|G| = 2$. So, such a group must be isomorphic to Z_2.

17. Suppose A is any non-empty set. Let

$$D = \{\sigma \in S_A \,|\, |M(\sigma)| < \infty\}$$

We will show that D is a normal subgroup of S_A. First, let us show that it is a subgroup of S_A.

If σ moves finitely many points of A, then it is easy to see that σ^{-1} also moves finitely many points of A, and hence $\sigma^{-1} \in D$. Next, suppose $\sigma_1, \sigma_2 \in D$. If x is a point moved by $\sigma_1\sigma_2$, then $\sigma_2(x)$ can only assume finitely many values (because σ_1 moves only finitely many points). Therefore, x can only assume finitely many values, because σ_2 is a bijection, and hence $\sigma_1\sigma_2$ moves only finitely many values. Hence, D is a subgroup of S_A.

Now, let us show that D is a normal subgroup. So, let $\sigma \in D$ and let $\tau \in S_A$. We will show that $\tau\sigma\tau^{-1}$ moves only finitely many points. If $x \in A$ and if $\tau^{-1}(x)$ is a point fixed by σ, then

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

and hence $\tau\sigma\tau^{-1}$ also fixes x. So, for $\tau\sigma\tau$ inverse to move x, $\tau^{-1}(x)$ can only assume finitely many values, and hence x can only assume finitely many values. This means $\tau\sigma\tau^{-1} \in D$, and hence D is a normal subgroup of S_A.

19. Suppose H is a normal subgroup of G, and suppose K is a conjugacy class of G contained in H and let $x \in K$. We will show that K is a union of k conjugacy classes of equal size in H, where $k = |G : HC_G(x)|$.

Now, observe that the size of the conjugacy class of x in H is $|H : C_H(x)|$, and we know that $C_H(x) = C_G(x) \cap H$. By the second isomorphism theorem, we have

$$\frac{|HC_G(x)|}{|H|} = \frac{|C_G(x)|}{|C_H(x)|}$$

and hence

$$|H : C_H(x)| = \frac{|HC_G(x)|}{|C_G(x)|} = \frac{|K|}{|G : HC_G(x)|} = \frac{|K|}{k}$$

So, it follows that the size of the conjugacy class of x in H is $\frac{K}{k}$. So, there are k conjugacy classes of equal size.

Now, consider a conjugacy class K in S_n consisting of even permutations. We know that $K \subseteq A_n$, and that A_n is a normal subgroup of S_n. So, by what we just proved, K will be a union of k equally-sized conjugacy classes in A_n, where

$$k = |S_n : A_n C_{S_n}(x)|$$

and $x \in K$. Now, observe that $A_n C_{S_n}(x)$ is a subgroup of S_n, which has order $\geq \frac{n!}{2}$. So, either the order is $\frac{n!}{2}$, or the order is $n!$. So, either K is a single conjugacy class, or it is a union of two conjugacy classes.

20. Suppose $\sigma \in A_n$. First, suppose all elements in the conjugacy class of σ in S_n are also conjugate in A_n. By the previous exercises, it follows that

$$k = |S_n : A_n C_{S_n}(\sigma)| = 1$$

which means that

$$|A_n C_{S_n}(\sigma)| = n!$$

and therefore, it means that σ commutes with an odd permutation.

Conversely, if σ commutes with an odd permutation, then $|A_n C_{S_n}(\sigma)| > \frac{n!}{2}$, which means that $|A_n C_{S_n}(\sigma)| = n!$, and hence there is only one conjugacy class in A_n.

21. In this exercise, we will formulate a criterion to check when conjugacy classes in S_n are preserved in A_n, and when they are splitted.

Let K be a conjugacy class in S_n and suppose $K \subseteq A_n$. We show that if $\sigma \in S_n$, then σ *does not* commute with any odd permutation if and only if the cycle type of σ consists of distinct odd integers.

So, suppose $\sigma \in S_n$ does not commute with an odd permutation. Clearly, σ cannot be an odd permutation. Now, let the cycle decomposition of σ be

$$\sigma = \sigma_1 ... \sigma_k$$

where each σ_i is a cycle. If σ_i is an even length cycle for some i, then σ_i is an odd permutation, and clearly σ commutes with σ_i. Hence, σ_i cannot be an even length cycle for any i, and hence the cycle type of σ consists of only odd integers. Now, we show that the cycle type cannot have two equal odd integers. For the sake of contradiction, suppose σ_i and σ_j have the same odd length. Let $\sigma_i = (a_1\ a_2\ ...\ a_k)$ and $\sigma_j = (b_1\ b_2\ ...\ b_k)$. Consider the product of k transpositions given by

$$\tau = (a_1\ b_1)(a_2\ b_2)...(a_k\ b_k)$$

We will show that τ commutes with $\sigma_i \sigma_j$, and hence τ will commute with σ, which will be a contradiction. Observe that

22. Let n be an odd integer, and let us consider the set of all n-cycles, which form a conjugacy class in the symmetric group. Let σ be an n-cycle. So, it is an even permutation, and its cycle type consists of distinct odd integers. So, it doesn't commute with any odd permutation, and hence this conjugacy class splits into two conjugacy classes in A_n.

23. Let M be a maximal subgroup of a group G. Observe that $M \leq N_G(M)$, and hence either $N_G(M) = M$ or $N_G(M) = G$.

Now, let M be subgroup of G that is not normal in G. We will show that the number of non-identity elements of G that are contained in conjugates of M is at most $(|M| - 1)|G : M|$. Consider the action of G on all subgroups of G by conjugation. Under this action, the size of the orbit of M is

$$|G : N_G(M)| = |G : M|$$

because M is not normal. Also, the number of non-identity elements in any conjugate of M is $|M| - 1$. The bound is then obvious.

29. Let p be a prime, and suppose G is a group of order p^α. We will show that G contains a subgroup of order p^β, for every $1 \leq \beta \leq \alpha$. We will do so by induction on α.

Clearly, the statement is trivial for $\alpha = 1$. So, let $\alpha > 1$, and assume that the statement is true for all integers less than α. We know that G has a non-trivial center, and hence let

$$|Z(G)| = p^\beta$$

where $1 \leq \beta \leq \alpha$.

We will consider two cases: first, suppose $Z(G) = G$. In that case, apply Cauchy's theorem to G (since G is abelian, we are using the abelian version of Cauchy) and hence we get a subgroup of order p. Let it be N (clearly it is normal). Now, consider the group G/N of order $p^{\alpha-1}$. By induction, G/N contains a subgroup of order p^k, for every $1 \leq k \leq \alpha - 1$. Take a subgroup K/N of G/N of order p^k. Then, clearly, K is a subgroup of G of order p^{1+k}, where $1 \leq k \leq \alpha - 1$. So, the claim follows.

In the second case, suppose $|Z(G)| = p^\beta$, where $\beta < \alpha$. Then, by induction, $Z(G)$ contains subgroups of order p^k, for every $1 \leq k \leq \beta$. Now, consider the group $G/Z(G)$ of order $\alpha - \beta$. Again, by induction, this group contains a subgroup $K/Z(G)$ of order p^k, for every $1 \leq k \leq \alpha - \beta$, and hence K is a subgroup of G of order $p^{k+\beta}$. Again, the claim follows.

31. Consider D_{2n}, where n is even. We will show that the conjugacy classes of D_{2n} are:

$$\{1\}, \{r^k\}, \{r^{\pm 1}\}, ..., \{r^{\pm(k-1)}\}, \{sr^{2b} | b = 1, ..., k\}\{sr^{2b-1} | b = 1, ..., k\}$$

where $n = 2k$. From here, it will follows that the class equation for D_{2n} is

$$2n = 2 + 2 + ... + 2 + k + k$$

where in the above equation, there are k twos.

First, observe that the center is $\{1, r^k\}$, and that explains the first two equivalence classes. Now, let consider any element of the form r^{k_1}, where $1 \leq k_1 \leq n - 1$, and $k_1 \neq k$. Conjugating r^{k_1} by any power of r will give k_1. Now, if sr^{k_2} is any reflection,

then

$$\begin{aligned} sr^{k_2}r^{k_1}(sr^{k_2})^{-1} &= sr^{k_2}r^{k_1}r^{-k_2}s \\ &= sr^{k_2}s \\ &= r^{-k_2} \end{aligned}$$

and that explains the rest of the conjugacy classes of powers of r.

Now, let sr^{k_1} be any reflection. Conjugating this reflection by a rotation r^{k_2}, we get

$$r^{k_2}sr^{k_1}r^{-k_2} = sr^{k_1-2k_2}$$

and so sr^{k_1} is conjugate to all reflections sr^{k_3}, where the parity of k_3 is the same as that of k_1. This explains the last two conjugacy classes.

26. Automorphisms

In this section, we revisit *automorphisms*. We know that if G is a group, then the set of automorphisms of G, denoted by $\mathrm{Aut}(G)$, also forms a group. Observe that automorphisms are permutations of G, and hence they are a subgroup of S_G. Specifically, they are structure preserving permutations.

We now introduce the idea of an *inner automorphism*:

Theorem 26.1. Let G be a group, and let $H \trianglelefteq G$. Let G act on H by conjugation, and let π be the permutation representation. Then, for every $g \in G$, $\pi(g)$ is an automorphism of H. In particular, π is a homomorphism from G to $\mathrm{Aut}(H)$. The kernel of π is $C_G(H)$. So, $G/C_G(H)$ is isomorphic to some subgroup of $\mathrm{Aut}(H)$.

Proof: First, for $g \in G$, us show that the map $\pi(g)$ is in Aut(H). Clearly, $\pi(g)$ is a permutation of H. It remains to show that it is a homomorphism as well. But, observe that for $h_1, h_2 \in H$, we have

$$\pi(g)(h_1h_2) = g(h_1h_2)g^{-1} = \pi(g)(h_1)\pi(g)(h_2)$$

and hence the first part of the claim is proven.

Now, let $g \in G$ such that $\pi(g) = 1$, where 1 is the identity automorphism. Then, we have that

$$ghg^{-1} = h$$

for all $h \in H$, and hence $g \in C_G(H)$. So, it follows that $\mathrm{Ker}(\pi) = C_G(H)$, and hence by the first isomorphism theorem, $G/C_G(H)$ is isomorphic to some subgroup of $\mathrm{Aut}(H)$.

Respecting this theorem, if we let $H = G$, then we observe that $\pi(g)$ is an automorphism of G. This kind of an automorphism is called an *inner automorphism* of G, and the set of inner automorphisms forms a subgroup of $\mathrm{Aut}(G)$.

This theorem leads to an important result:

Theorem 26.2. Suppose H is a subgroup of a group G. Consider the subgroup $N_G(H)$ of H. Then, $N_G(H)/C_G(H)$ is isomorphic to some subgroup of $\mathrm{Aut}(H)$.

Proof: We know that H is a normal subgroup of $N_G(H)$. By the previous theorem, if we let $N_G(H)$ act on H via conjugation, then we see that $N_G(H)/C_G(H)$ is isomorphic to some subgroup of $\mathrm{Aut}(H)$.

If we put $H = G$ above, then we see that

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

Now, we define the notion of *characteristic subgroups.* If $H \leq G$, we say that H is characteristic in G, if every automorphism of G maps H to itself. We will prove some properties of charateristic subgroups in the coming exercises.

Let's look at the automorphism group of the cyclic group:

Theorem 26.3. $\mathrm{Aut}(Z_n)$ is isomorphic to the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$, which has order $\phi(n)$.

Proof: Let $\sigma \in \mathrm{Aut}(Z_n)$, where $Z_n = \langle x \rangle$. We then know that $\sigma(x) = x^a$, where $(a, n) = 1$. So, consider the map

$$\sigma \mapsto a$$

and we will show that this is an isomorphism. Clearly, this is a one-one and onto map. To see that it is a homomorphism, observe that if $\sigma_1(x) = x^{a_1}$ and $\sigma_2(x) = x^{a_2}$, then we have $\sigma_1\sigma_2(x) = x^{a_1 a_2}$, which means that

$$\sigma_1\sigma_2 \mapsto a_1 a_2$$

and hence it is a homomorphism. This completes the proof.

Exercises on Page 137

1. In this exercise, we will show that for any group G, $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$. So suppose $\sigma \in \mathrm{Inn}(G)$ and suppose $\tau \in \mathrm{Aut}(G)$. So, we know that for any $x \in G$, we have

$$\sigma(x) = gxg^{-1}$$

for some $g \in G$. Now, we have

$$\tau\sigma\tau^{-1}(x) = \tau(g\tau^{-1}(x)g^{-1}) = \tau(g)x[\tau(g)]^{-1}$$

and hence $\tau\sigma\tau^{-1} \in \mathrm{Inn}(G)$, showing that $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$. The quotient $\mathrm{Aut}(G)/\mathrm{Inn}(G)$ is called the *outer automorphism group* of G

2. Suppose G is an abelian group of order pq, where p and q are distinct primes. We will show that G is cyclic. By Cauchy's theorem, there are elements g_1, g_2 of order p and q respectively. Because G is abelian, it follows that $(g_1g_2)^{pq} = 1$. We claim that $|g_1g_2| = pq$. Clearly, $|g_1g_2|$ cannot be 1, and the only other possibilities are p, q and pq. If the order is p, then we will have $g_2^p = 1$, which would imply that $p|q$, which is a contradiction. Similarly, the order cannot be q. Hence, the order is pq, and the group is cyclic.

3. Consider an automorphism of D_8. Since r has order 4, the only possible images of r are r and r^3. Similarly, the element s has atmost 4 possible images, which are s, sr, sr^2 and sr^4. It thus follows that

$$|D_8| \leq 2 \cdot 4 = 8$$

4. We will show that $|\mathrm{Aut}(Q_8)| \leq 24$. We know that Q_8 is generated by elements i and j. So, under an automorphism, i and j must be mapped to a pair of generators. There 12 pairs of generators. Hence, it follows that $|\mathrm{Aut}(D_8)| \leq 2 \cdot 12 = 24$.

6. Let H be a characteristic subgroup of G. Let $g \in G$. Then, then map $\sigma_g : G \to G$ given by

$$\sigma_g(x) = gxg^{-1}$$

is an inner automorphism of G. Since H is characteristic, it follows that for any $h \in H$, $ghg^{-1} \in H$. Since g was arbitrary, it follows that $H \trianglelefteq G$.

Now, we give an example of a normal subgroup that is not characteristic. Consider $V_4 = \{1, a, b, c\}$, and the automorphism σ sending $1 \to 1$, $a \to b$, $b \to c$ and $c \to a$. Consider the normal subgroup $\{1, a\}$. It is easy to see that this subgroup is not characteristic.

7. Suppose H is the unique subgroup of a given order in a group G. Let σ be any automorphism of G. Then, $\sigma(H)$ is also a subgroup of G of the same order. But, this means that $\sigma(H) = H$, and hence H is characteristic.

8. Let G be a group with subgroups H and K with $H \leq K$.

(a) Suppose H char K and $K \trianglelefteq G$. We will show that $H \trianglelefteq G$. This is a kind of "transitivity" property of normal groups.

Let $g \in G$. Since K is normal in G, let G act on K by conjugation. Let π be the permutation representation. Then, for any $g \in G$, $\pi(g)$ is in Aut(K). Since H char K, it follows that $\pi(g)(H) = H$, and hence for any $h \in H$, $ghg^{-1} \in H$. Since g was arbitrary, it follows that $H \trianglelefteq G$.

(b) Suppose H char K and K char G. We will show that H char G. Let $\phi \in$ Aut(G). Then, we know that $\phi(K) = K$. So, ϕ restricted to K is an automorphism of K. Since H is characteristic in K, we then have $\phi(H) = H$. This shows that H char G. So, being characteristic is a transitive property of groups.

Now, it is easy to see that V_4 is characterisitc in A_4, because any automorphism of A_4 must map elements of order 2 to elements of order 2. Also, A_4 is characteristic in S_4, because even permutations must be mapped to even permutations under automorphisms. Hence, it follows that V_4 is characteristic in S_4.

9. Here, we will show that every subgroup of $\langle r \rangle$ is normal in D_{2n}. Let ϕ be any automorphism of D_{2n}. Then, r must be mapped to a generator of $\langle r \rangle$, and hence it clearly follows that $\langle r \rangle$ is characteristic in D_{2n}. Now, any subgroup of $\langle r \rangle$ is normal in $\langle r \rangle$, because this group is abelian. Hence, it follows that any subgroup of $\langle r \rangle$ is normal in D_{2n}.

12. Let G be a group of order 3825, and let H be a normal subgroup of order 17.

Consider the action of G on H by conjugation, and let π be the permutation representation. Then, $\pi : G \to$ Aut(H), and since $|H| = 17$, we see that Aut$(H) \cong (\mathbb{Z}/17\mathbb{Z})^\times$. Now, observe that $\ker\pi = C_G(H)$, and hence $G/C_G(H)$ is isomorphic to some subgroup of $(\mathbb{Z}/17\mathbb{Z})^\times$. The latter group has order 16, and the only choice is $G/C_G(H) \cong 1$, and hence $C_G(H) = G$, implying that $H \leq Z(G)$.

13. Let G be a group of order 203, and suppose H is a normal subgroup of order 7. By a similar argument as in the previous problem, we see that $G/C_G(H)$ is isomorphic to some subgroup of $(\mathbb{Z}/7\mathbb{Z})^\times$, and since the latter group has order 6, it follows that $C_G(H) = G$, showing that $H \leq Z(G)$.

Now, $G/H \cong Z_{29}$, and since $H \leq Z(G)$, it follows that G is abelian (very similar to the fact that if $G/Z(G)$ is cyclic, then G is abelian).

27. Sylow's Theorems

In this section, we will prove and use **Sylow's theorems**, which are arguably some of the most important theorems in group theory. Let's begin with some definitions.

A group G of order p^a, for some $a \in \mathbb{N}$, is called a *p-group*. Subgroups of G which are p-groups are called *p-subgroups*.

If $|G| = p^\alpha m$, where p does not divide m, then a subgroup Q of G of order p^α is called a *Sylow p-subgroup* of G. The set of Sylow p subgroups is denoted by $Syl_p(G)$, and the number of Sylow p-subgroups of G is denoted by $n_p(G)$.

Let's now state the Sylow theorems:

Theorem 27.1. Let G be a finite group of order $p^\alpha m$, where p does not divide m.

(1) Sylow p-subgroups of G exist, i.e the set $Syl_p(G)$ is non-empty.
(2) Let $P \in Syl_p(G)$. If Q is any p-subgroup of G, then Q is contained inside some conjugate of P, i.e $Q \leq gPg^{-1}$ for some $g \in G$. Hence, all Sylow p-subgroups are conjugates of each other.
(3) If n_p is the cardinality of $Syl_p(G)$, then we have that

$$n_p = 1 (\text{mod } p)$$

Further, n_p is the index of the normalizer $N_G(P)$, and hence it follows that

$$n | m$$

Proof: We will prove (1) by induction on the order of G. If $|G| = 1$, then the statement is trivial. So, let $|G| = p^\alpha m$, where p does not divide m, and assume that the statement is true for all groups of order less than $|G|$.

We consider two cases: first, suppose p divides $|Z(G)|$. Since $Z(G)$ is abelian, we apply Cauchy's theorem for abelian groups to $Z(G)$, and hence $Z(G)$ has a subgroup of order p. Let this subgroup be N. Clearly, N is a normal subgroup of G. Consider the quotient group G/N, which has order $p^{\alpha-1}m$. By induction, this quotient group has a subgroup, say P/N, of order $p^{\alpha-1}$. It follows that $N \leq P \leq G$ is a subgroup of order p^α, and hence it is a Sylow-p subgroup of G.

In the second case, assume that p does not divide $Z(G)$. Let the class equation of G be

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

where $\{g_1, ..., g_n\}$ are the representatives of distinct conjugacy classes, none of which is in $Z(G)$. So, it must be true that p does not divide atleast one of $|G : C_G(g_j)|$. Let $H = C_G(g_j)$. It follows that $|H| = p^\alpha k$, where p does not divide k. Clearly, $H < G$, and by induction, H has a subgroup of order p^α. So, G also has a subgroup of order p^α, and this proves (1).

Now, let P be a Sylow-p subgroup of G, and let $S = \{P_1, ..., P_r\}$ be the set of all conjugates of P. Let Q be a p-subgroup of G. Then, Q acts on S via conjugation. Let

$$S = O_1 \cup ... \cup O_s$$

be the orbits of S under this action. Let $P_1, ..., P_s$ be the representatives of these orbits. Then, we have that

$$|O_i| = |Q : N_Q(P_i)| = |Q : Q \cap N_G(P_i)| = |Q : Q \cap P_i|$$

where we used the fact that $Q \cap N_G(P_i) = Q \cap P_i$, which we will prove after the proof of this theorem.

Now, we will show that $r = 1(\text{mod } p)$. To prove this, put $Q = P_1$. Then,

$$|O_1| = 1$$

and for $2 \leq i \leq s$, we have

$$|O_i| = |P_1 : P_1 \cap P_i|$$

Moreover, observe that $P_i \neq P_1$ for $2 \leq i \leq s$, and hence it follows that p divides $|O_i|$ (because each P_i is a p subgroup) for $2 \leq i \leq s$. So,

$$r = |O_1| + ... + |O_s| = 1(\text{mod } p)$$

Now, let us prove (2). Let Q be a p-subgroup of G. Suppose, for the sake of contradiction, $Q \nleq gPg^{-1}$ for any $g \in G$. We have that $|O_i| = |Q : Q \cap P_i|$, and since Q is not contained in any P_i, it follows that p divides $|O_i|$. However, this would imply that $r = 0(\text{mod } p)$, which is a contradiction. Hence, $Q \leq gPg^{-1}$, for some $g \in G$.

Finally, (2) shows that all Sylow p-subgroups are conjugates of each other. This means that the action of G on S creates one orbit. So, it follows that

$$n_p = |G : N_G(P)|$$

for any $P \in Syl_p(G)$. Since $(n_p, p) = 1$, it follows that $n_p | m$.

We now prove the lemma that we used:

Lemma: If $P \in Syl_p(G)$ and Q is any p-subgroup of G, then $Q \cap N_G(P) = Q \cap P$.
Proof: One inclusion is clear. So, we prove that $Q \cap N_G(P) \subseteq Q \cap P$. Let $H = Q \cap N_G(P)$. Consider the group PH (it is a group because $H \leq N_G(P)$). The order of this group is

$$|PH| = \frac{|P||H|}{|P \cap H|}$$

which means the order of the group is a power of p. Also, $P \leq PH$, implying that $|PH| \geq p^\alpha$. But, α is the largest possible power of a p-group, and hence we see that $|PH| = p^\alpha$. So, $PH = P$, and hence $H \leq P$, implying that $H \leq Q \cap P$. This completes the proof.

A useful corollary follows from this:

Theorem 27.2. Let P be a Sylow-p subgroup of G. The following are equivalent:

(1) P is the unique Sylow-p subgroup of G.
(2) P is normal in G.
(3) P is characteristic in G.
(4) All subgroups generated by elements of p-power order are p-groups.

Proof: First, if (1) holds, then it clearly follows that $P \trianglelefteq G$, because for any $g \in G$, $gPg^{-1} \in Syl_p(G)$. (1) follows from (2) in a similar way. If (3) holds, then (2) holds. If (2) holds, then (1) holds, and clearly it will follow that (3) also holds.

Now, suppose (1) holds. Let X be the set of all elements of p-power order. For any $x \in X$, observe that $\langle x \rangle$ is a p-subgroup, and hence $\langle x \rangle$ is contained in some conjugate of P, and hence $\langle x \rangle$ is contained in P. So, $\langle X \rangle \leq P$, and hence $\langle X \rangle$ is a p-group, and hence (4) follows. The converse can be easily proven.

Let's now do some applications of Sylow's theorems, which help us to restrict the structure of some groups to a great extent:

Groups of order pq, where $p < q$ and p does not divide $q - 1$: Let G be such a group. Let Q be a Sylow-q subgroup. Then, n_q divides p, and $n_q = 1(\text{mod } q)$. So, the only choice is $n_q = 1$, and hence Q is normal. Now, let P be a Sylow-p subgroup, and again $n_p = 1\text{mod } p$. By the given condition, the only choice is $n_p = 1$, so that P is also normal. Let $P = \langle x \rangle$ and let $Q = \langle y \rangle$. The idea is to show that x and y commute, and hence it will follows that $|xy| = pq$, proving that $G \cong Z_{pq}$.

Consider $C_G(P)$. Since $P \trianglelefteq G$, we know that $G/C_G(P)$ is isomorphic to a subgroup of $\text{Aut}(P)$, and $|\text{Aut}(P)| = p-1$. So, it follows that the only possible order of $G/C_G(P)$ is 1, and hence $C_G(P) = G$, showing that $xy = yx$. Hence, the proof is complete.

Groups of order 12: Here, consider n_3. We know that $n_3 = 1 \text{ mod } 3$, and also $n_3|4$. So, either $n_3 = 1$ or $n_3 = 4$. Here, we show that if $n_3 = 4$ (i.e no Sylow-3 subgroup is normal), then $G \cong A_4$.

Let G act on the set of Sylow-3 subgroups by conjugation. Since there are four of them, we see that the permutation representation is $\pi : G \to S_4$. The kernel K of π is the intersection

$$\text{Ker}\pi = \bigcap_{P \in Syl_3(G)} N_G(P)$$

Now, since n_3 is the index $|G : N_G(P)|$ for any $P \in Syl_3(G)$, we see that $|N_G(P)| = 3$ for all $P \in Syl_3(G)$. However, since $|P| = 3$ for any such P, it follows that $P = N_G(P)$ for all $P \in Syl_3(G)$. So,

$$\text{Ker}\pi = \bigcap_{P \in Syl_3(G)} N_G(P) = \bigcap_{P \in Syl_3(G)} P = 1$$

because distinct 3-subgroups must intersect trivially. So, G is isomorphic to some subgroup of S_4.

Now each $P \in Syl_3(G)$ contains two elements of order 3, and hence G contains $4 \times 2 = 8$ elements of order 3. Consider $\pi(G)$, to which G is isomorphic. Now, $\pi(G)$ contains 8 elements of order 3, and we know that all these elements are contained in A_4. So, $\pi(G)$ intersects with A_4 on atleast 8 elements. Since $|\pi(G)| = |A_4| = 12$, it follows that $\pi(G) = A_4$, and hence $G \cong A_4$.

Groups of order p^2q, where p and q are distinct primes: Let G be such a group. We consider two cases.

First, suppose $p > q$. Then, $n_p = 1$, and hence if $P \in Syl_p(G)$, then $P \trianglelefteq G$.

Next, suppose $p < q$. Then, $n_q = 1(\text{ mod } q)$ and $n_q|p^2$. If $n_q = 1$, then $Q \trianglelefteq G$, where $Q \in Syl_q(G)$. The only other choice is $n_q = p^2$. In that case, we see that $q|p^2 - 1$, and hence the only choice is $q = p - 1$, which forces $p = 2$ and $q = 3$, and so $|G| = 12$.

28. Exercises on Page 146

4. First consider D_{12}. Any Sylow-2 subgroup is either cyclic or isomorphic to V_4. Clearly, D_{12} does not contain any element of order 4, and hence the only Sylow-2 subgroups are isomorphic to V_4. It is easy to see that one such group is $\{1, r^3, s, sr^3\}$. All other Sylow-2 subgroups are conjugates of this. Moreover, observe that any Sylow-2 subgroup cannot be normal because D_{2n} is not abelian, and hence $n_2 = 3$. So, all

Sylow-2 subgroups are:

$$\{1, r^3, s, sr^3\}$$
$$\{1, r^3, sr^4, sr\}$$
$$\{1, r^3, sr^2, sr^5\}$$

Now, any Sylow-3 subgroup must be cyclic. Hence, the only Sylow-3 subgroup is

$$\{1, r^2, r^4\}$$

5. Consider D_{2n}, and let p be an odd prime. Let $P \in Syl_p(D_{2n})$. We will show that P is cyclic and normal.

Suppose $P \in Syl_p(D_{2n})$. Observe that P cannot contain any reflection, because reflections have order 2, and p is an odd prime. So, it follows that $P \leq \langle r \rangle$. So, P is cyclic. Moreover, observe that $\langle r \rangle$ has a unique subgroup of order p^α, where p^α is the largest power of p dividing n, and hence by this uniqueness, P must be normal.

9. It is easy to see that $|\mathrm{SL}_2(\mathbb{F}_3)| = 24$, and hence any Sylow-3 subgroup must be cyclic. Also, n_3 (the number of Sylow-3 subgroups) can only be 1 or 4. Observe that the following matrix has order 3:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

and hence this is one Sylow-3 subgroup. Explicitly, it is

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \right\}$$

Similarly, observe that the following matrix also has order 3:

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

and hence its corresponding Sylow-3 subgroup is

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \right\}$$

and it follows that $n_4 = 4$. It is not hard to see that the other Sylow-3 subgroups are:

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 2 & 2 \end{pmatrix} \begin{pmatrix} 2 & 2 \\ 1 & 0 \end{pmatrix} \right\}$$

and

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 2 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 2 & 0 \end{pmatrix} \right\}$$

and these are all the Sylow-3 subgroups.

10. Consider the subgroup G of $\mathrm{SL}_2(\mathbb{F}_3)$ given by

$$G = \left\langle \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \right\rangle$$

Also, we know that $n_2 \in \{1, 3\}$.

11. Suppose $G = \mathrm{SL}_2(\mathbb{F}_3)$. Here, we will find $Z(G)$, and show that $G/Z(G) \cong A_4$.

First, we have that $|\mathrm{GL}_2(\mathbb{F}_3)| = (3^2-1)(3^2-3) = 8 \cdot 6 = 48$ and also we have

$$|\mathrm{GL}_2(\mathbb{F}_3) : \mathrm{SL}_2(\mathbb{F}_{\not 3})| = 2$$

and hence $|\mathrm{SL}_2(\mathbb{F}_3)| = 24$. Now, by a previous exercise, we know that

$$\mathrm{SL}_2(\mathbb{F}_3) = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\rangle$$

Now it is easy to see that $x \in Z(G)$ if and only if it commutes with the two matrices

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

Now, suppose $x \in Z(G)$ such that

$$x = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

So, we have the two equations

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

and the above two equations imply that $b = c = 0$ and $a = d$, and hence x is of the form

$$x = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$$

where $a \neq 0$. So, it follows that

$$Z(G) = \left\langle \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \right\rangle$$

We will now show that $G/Z(G) \cong A_4$. To show this, we will show that any Sylow-3 subgroup of $G/Z(G)$ is not normal, and by facts about groups of order 12, this will prove that $G/Z(G) \cong A_4$. To show that any Sylow-3 subgroup of $G/Z(G)$ is not normal, it is enough to show that there are atleast two Sylow-3 subgroups. Now, subgroups of $G/Z(G)$ are in bijection with subgroups of G containing $Z(G)$. So, it is enough to show that there are atleast two subgroups of order 6 in G which contain $Z(G)$ (it will then follow that there are atleast two Sylow-3 subgroups in $G/Z(G)$).

Now, consider the following subgroups of G:

$$H_1 = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \right\}$$
$$H_2 = \left\langle \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\rangle = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \right\}$$

Since $Z(G)$ is normal in G, consider the subgroups $H_1Z(G)$ and $H_2Z(G)$ (these are groups because $Z(G)$ is normal). Also, it is easy to see that the order of both of these

groups is 6. We will show that $H_1Z(G) \neq H_2Z(G)$. To show this, we have

$$H_1Z(G) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 2 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix} \right\}$$

$$H_2Z(G) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 2 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 1 & 2 \end{pmatrix} \right\}$$

and obviously these are two distinct subgroups of order 6 containing $Z(G)$.

So, this proves that $G/Z(G) \cong A_4$.

13. Let G be a group of order 56.

29. Direct Products and the Structure Theorem

Let $G_1, ..., G_n$ be arbitrary groups. We define the *direct product* of these groups as

$$G_1 \times G_2 \times ... \times G_n$$

where the operation of the group is done componentwise. This definition may also be extended to any collection of groups (see exercises).

A simple fact follows from the definition:

$$|G_1 \times G_2 \times ... \times G_n| = |G_1||G_2|...|G_n|$$

and if one of the groups is infinite, so is the direct product.

Next, we will prove how direct products have copies of each group occuring in the product:

Theorem 29.1. Let $G = G_1 \times ... \times G_n$.

(1) Let $1 \leq i \leq n$. Then,

$$G_i \cong \{(1, 1, ..., g_i, 1, ..., 1) |\, g_i \in G_i\}$$

So, G has a copy that is isomorphic to G_i. If we denote this subgroup of G by G_i, then $G_i \trianglelefteq G$, and

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

(2) For each i, we define the *projection* map $\pi_i : G \to G_i$ as

$$\pi_i[(g_1, ..., g_i, ..., g_n)] = g_i$$

π_i is a surjective homomorphism and

$$\text{Ker}(\phi) \cong G/G_i$$

(3) If $x \in G_i$ and $y \in G_j$ for some $i \neq j$, then

$$xy = yx$$

Proof: It is clear that G_i is isomorphic to $\{(1, 1, ..., g_i, 1, ..., 1) |\, g_i \in G_i\}$, and from now on let us denote this isomorphic copy as G_i. Let us now show that $G_i \trianglelefteq G$. Consider the map $(g_1, ..., g_i, ..., g_n) \mapsto (g_1, ..., g_{i-1}, g_{i+1}, ..., g_n)$. This map is clearly a surjective homomorphism. Its kernel is G_i, and hence $G_i \trianglelefteq G$. By the first isomorphism theorem, we have

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

Proving (2) is very similar. It is easy to see that the projection map is a surjective homomorphism. The kernel of the map is the set $\{(g_1, ..., g_{i-1}, 1, g_{i+1}, ..., g_n)\}$, and this is clearly isomorphic to G/G_i.

Statement (3) is trivial.

Let's look at the following examples:

(1) Suppose V is a group such that $v^p = 1$ for all $v \in V$, where p is a prime. If $|V| = p^n$, for some $n \in \mathbb{N}$, then V is called the *elementary abelian group* of order p^n. Observe that, if p is a prime, then
$$G = Z_p \times Z_p \times ... \times Z_p$$
is an elementary abelian group of order n (there are n factors in the product).

(2) Let p be a prime. We will show that the elementary abelian group of order p^2, denoted by E_{p^2}, has exactly $p+1$ subgroups of order p. Clearly, a subgroup of order p must be cyclic, i.e it must be generated by some element of E_{p^2}. Clearly, all elements have order p, and hence they generate subgroups of order p. Also, any two subgroups of order p are either equal or intersect trivially. In each such subgroup, there are $p-1$ possible generators. Hence, the p^2-1 elements are partitioned into sets containing $p-1$ elements. So, the total number of subgoups is
$$\frac{p^2-1}{p-1} = p+1$$

30. Exercises on Page 156

1. We will show that
$$Z(G_1 \times ... \times G_n) = Z(G_1) \times ... \times Z(G_n)$$
If $x \in Z(G_1 \times ... \times G_n)$, and if $x = (x_1, ..., x_n)$, then observe that $x_i \in Z(G_i)$ for each i, and hence $x \in Z(G_1) \times ... \times Z(G_n)$. Conversely, if $(x_1, ..., x_n) \in Z(G_1) \times ... \times Z(G_n)$, then it is easy to see that $x = (x_1, ..., x_n) \in Z(G_1 \times ... \times G_n)$. Hence equality follows, and so a direct product is abelian if and only if each factor is abelian.

4. Suppose A and B are finite groups, and let p be a prime. We will show that there is a bijection between $Syl_p(A \times B)$ and the set of all $P \times Q$, where $P \in Syl_p(A)$ and $Q \in Syl_p(B)$. This will prove that
$$n_p(A \times B) = n_p(A) n_p(B)$$
First, if $P \in Syl_p(A)$ and $Q \in Syl_p(B)$, then $P \times Q \in Syl_p(A \times B)$, which is a trivial fact. Conversely, suppose $P' \in Syl_p(A \times B)$. By Sylow's theorem, A contains a Sylow-p subgroup, say P_A, and similarly let P_B be a Sylow-p subgroup of B. Then, $P_A \times P_B \in Syl_p(A \times B)$, and hence P' and $P_A \times P_B$ are conjugates. So,
$$P' = (hP_Ah^{-1}) \times (kP_Bk^{-1})$$
for some $(h, k) \in A \times B$, and hence $P' = P \times Q$. This completes the proof.

This proof easily extends to finite direct product of finite groups.

5. Consider $Q_8 \times Z_4$. Each subgroup of each factor is normal, but still we will exhibit a subgroup which is not normal. Consider the cyclic subgroup $\langle (i, 1) \rangle$, which explicitly is $\langle (i, 1) \rangle = \{(1, 0), (i, 1), (-1, 2), (-i, 3)\}$ Now, we have
$$(j, 1)(i, 1)(j, 1)^{-1} = (jij^{-1}, 1) = (-i, 1)$$
and hence this subgroup is not normal.

6. Here, we will show that all subgroups of $Q_8 \times E_{2^n}$ are normal. Just to be clear, we identify $Q \times E_{2^n}$ with $Q \times Z_2 \times Z_2 \times ... \times Z_2$, where the factor Z_2 appears n times.

7. Suppose $G_1, ..., G_n$ are groups, and let $\pi \in S_n$. Consider the map

$$\phi_\pi : G_1 \times ... \times G_n \to G_{\pi^{-1}(1)} \times ... \times G_{\pi^{-1}(n)}$$

given by

$$\phi_\pi(g_1, ..., g_n) = (g_{\pi^{-1}(1)}, ..., g_{\pi^{-1}(n)})$$

Let us show that ϕ_π is an isomorphism (and hence changing the order of factors is a direct product does not change the isomorphism type).

First, let us show that ϕ_π is a homomorphism. To see this, if $(g_1, ..., g_n)$ and $(h_1, ..., h_n) \in G_1 \times ... \times G_n$, then we have

$$\phi_\pi(g_1h_1, ..., g_nh_n) = (g_{\pi^{-1}(1)}h_{\pi^{-1}(1)}, ..., g_{\pi^{-1}(n)}h_{\pi^{-1}(n)})$$
$$\phi_\pi(g_1, ..., g_n)\phi_\pi(h_1, ..., h_n)$$

Now, it is easy to see that $\mathrm{Ker}\phi_\pi = (1, ..., 1)$, which implies that ϕ_π is one-one. Finally, that ϕ_π is onto is trivial. So, it is an isomorphism.

Remark: Observe that, we used π^{-1} in the indices. There would be no harm to use π either, but this usage will be justified in the next problem. The bottom-line is that we are just reordering factors in the direct product.

8. Suppose $G_1 = G_2 = ... = G_n$, and let $G = G_1 \times ... \times G_n$. Let $\pi \in S_n$, and again consider ϕ_π as in the previous exercise.

Clearly, ϕ_π is an automorphism of G, and hence $\phi_\pi \in \mathrm{Aut}(G)$. Next, consider the map $\pi \mapsto \phi_\pi$ from S_n to $\mathrm{Aut}(G)$. We will show that this is an injective homomorphism.

11. Let p be a prime and let $n \in \mathbb{Z}^+$. Here we will find the number of subgroups of order p in the group E_{p^n}.

Any subgroup of order p must be cyclic. Also, any non-identity element of such a subgroup is a generator of the subgroup. So, the non-identity elements of E_{p^n}, which are $p^n - 1$ in number, are split into classes each of size $p - 1$, which give rise to the same subgroup. So, the total number of subgroups of order p is

$$\frac{p^n - 1}{p - 1}$$

16. In this exercise, we will prove some statements about arbitrary direct products. Let I be any indexing set, and let G_α be a group for every α. Let $\prod G_\alpha$ be the direct product of these groups.

First, we show that the arbitrary direct product contains an isomorphic copy for every index. To show this, let β be fixed, and consider the subset $G_\beta \times \prod_{\alpha \neq \beta}\{1_\alpha\}$, which is evidently a subgroup of the direct product, and the map $g_\beta \mapsto c$, where the map $c \in \prod G_\alpha$ satisfies $c(\beta) = g_\beta$ and $c(\alpha) = 1_\alpha$ for $\alpha \neq \beta$, gives an isomorphism $G_\beta \cong G_\beta \times \prod_{\alpha \neq \beta}\{1_\alpha\}$ (one can say all of this by saying that the projection onto the β^{th} factor is an isomorphism). Also, it is not difficult to see that each factor is infact a normal subgroup, and the isomorphism

$$\prod G_\alpha / G_\beta \cong \prod_{\alpha \neq \beta} G_\alpha$$

holds.

17. Now, we will look at the *restricted direct product*. Again, let I be any indexing set. The *restricted direct product* or *direct sum* of the family of groups is the subset of $\prod G_\alpha$ where all but finitely many coordinates are the identity. It is clear that the direct sum/restricted direct product is a subgroup of the direct product. It is also easy to see that the direct sum is a *normal* subgroup of the direct product.

Fundamental Theorem of Finitely Generated Groups. : We will not prove this theorem here, but we will see its consequences.

Theorem 30.1. Suppose G is a finitely generated abelian group. Then,

$$G \cong Z^r \times Z_{n_1} \times Z_{n_2} \times ... \times Z_{n_s}$$

where $r, n_1, ..., n_s$ are integers satisfying $n_i | n_{i-1}$ for each $2 \leq i \leq s$. Also, this expression is unique.

The integer r above is called the *free rank* of the group G and the integers $n_1, ..., n_s$ are called the *invariant factors* of G. Clearly, a finitely generated abelian group is finite if and only if its free rank is 0. Also, if G is finite, then its order will be the product of its invariant factors.

Now, finite abelian groups are clearly finitely generated. Hence, using this theorem, we can list all finite abelian groups of a given order. So, suppose G is a finite abelian group of order n. Then, if $n_1, ..., n_s$ are its invariant factors, then $n_1...n_s = n$, and since $n_i | n_{i-1}$, it is clear that each prime divisor of n divides n_1. So we have the following theorem:

Theorem 30.2. If n is a product of distinct primes (i.e n is square free), then upto isomorphism the only finite abelian group of order n is Z_n, the cyclic group.

So as we can observe, the decomposition of an abelian group of order n strictly depends on the factorisation of n.

Next, we will state the *Primary Decomposition Theorem* for finite abelian groups, which we will prove later. This theorem is equivalent to the fundamental theorem of finitely generated abelian groups for finite abelian groups. The theorem is as follows:

Theorem 30.3. Suppose G is a finite abelian group of order n, where $n = p_1^{\alpha_1}...p_k^{\alpha_k}$. Then

(1) $G \cong A_1 \times ... \times A_k$ where each $|A_i| = p_i^{\alpha_i}$ (also observe that each A_i(the isomorphic copy) is a Sylow-p_i subgroup of G, so in other words G is the direct product of its Sylow subgroups).
(2) For each $A \in \{A_1, ..., A_k\}$ with $|A| = p^\alpha$, we have
$$A \cong Z_{p^{\beta_1}} \times ... \times Z_{p^{\beta_t}}$$
where t and β_i depend on i.
(3) The decomposition in (1) and (2) is unique.

The numbers p^{β_i} above are called the *elementary divisors* of G. Note that these are different from the invariant factors of G.

So, respecting the above theorem, it is enough to finite all finite abelian groups of prime power order. Suppose $|A| = p^\alpha$, for some α. Then we can easily see that

$$A \cong Z_{p^{\beta_1}} \times ... \times Z_{p^{\beta_t}}$$

where $\beta_1 + ... + \beta_t = \alpha$, and also $\beta_i \geq \beta_{i+1} \geq 1$ for each i. So, finite abelian groups of prime power order are in one-to-one correspondence with partitions of α ordered in descending order.

So, if $n = p_1^{\alpha_1}...p_k^{\alpha_k}$, and q_i is the number of (non-isomorphic) finite abelian groups of order pi^{α_i}, then the number of finite abelian groups of order n is $q_1...q_k$.

In the exercises, we will see how to find elementary divisors from invariant factors and vice-versa. First, let us prove the following simple theorem:

Theorem 30.4. Let $m, n \in \mathbb{Z}^+$.

(1) $Z_m \times Z_n \cong Z_{mn}$ if and only if $(m, n) = 1$.
(2) If $n = p_1^{\alpha_1}...p_k^{\alpha_k}$ then

$$Z_n \cong Z_{p_1^{\alpha_1}} \times ... \times Z_{p_k^{\alpha_k}}$$

Proof: (2) follows from (1) easily by induction. So, we will only prove (1).

First, suppose $Z_{mn} \cong Z_m \times Z_n$. This means that $Z_m \times Z_n$ is cyclic, and let $(x, y) \in Z_m \times Z_n$ be a generator. The order of the element (x, y) is $[m, n]$, where $[m, n]$ is the lcm. This means that $[m, n] = mn$, and hence $(m, n) = 1$.

Conversely, suppose $(m, n) = 1$, and let x be a generator of Z_m and let y be a generator of Z_n. The order of (x, y) is mn, and hence $Z_m \times Z_n \cong Z_{mn}$.

Finally, we have two important definitions. If G is a finite abelian group with invariant factors $(n_1, .., n_t)$, then t is called the *rank* of G. If G is any group, the *exponent* is the smallest positive integer n such that $x^n = 1$ for all $x \in G$ (if no such number exists then exponent is ∞).

31. Exercises on Page 165

1. In this exercise, we will give the number of non-isomorphic abelian groups of the given order. In the following, let G be an abelian group of the given order. Suppose $n = p_1^{\alpha_1}..p_k^{\alpha_k}$. Then, by the primary decomposition theorem, it is easy to see that the number of non-isomorphic groups G is equal to $P(\alpha_1)...P(\alpha_k)$, where $P(t)$ represents the number of partitions of t.

(a) Order 100. We have $100 = 2^2 \cdot 5^2$, and the number of partitions of 2 is 2. So, there are 4 non-isomorphic possibilities for G.

(b) Order 576. We have that $576 = 2^6 \cdot 3^2$. The number of partitions of 6 is 11, and the number of partitions of 2 is 2. So, there are 22 non-isomorphic possibilities for G.

2. and 3. In these two exercises combined, we will see how to find the invariant factors as well as the elementary divisors. Here, we only consider abelian groups, so there is no ambiguity.

(a) Order 270. First, we will find the elementary divisors, because they are easier to find. We have that $270 = 2 \cdot 5 \cdot 3^3$. So, we see that $G \cong Z_2 \times B \times Z_5$, where $|B| = 3^3$. There are three partitions of 3, and hence there are three possibilities for B, which are Z_{27}, $Z_9 \times Z_3$ and $Z_3 \times Z_3 \times Z_3$. So, G has 3 possibilities, which are

$$Z_2 \times Z_{27} \times Z_5$$
$$Z_2 \times Z_9 \times Z_3 \times Z_5$$
$$Z_2 \times Z_3 \times Z_3 \times Z_3 \times Z_5$$

The invariant factors are (210), $(90, 3)$ and $(30, 3, 3)$.

(b) Order 9801. We repeat the method. We have $9801 = 3^4 \times 11^2$. The number of partitions of 4 is 5, and the number of partitions of 2 is 2. So, there are 10 choices of

G, which are

$$Z_{81} \times Z_{121}$$
$$Z_{81} \times Z_{11} \times Z_{11}$$
$$Z_{27} \times Z_3 \times Z_{121}$$
$$Z_{27} \times Z_3 \times Z_{11} \times Z_{11}$$
$$Z_9 \times Z_9 \times Z_{121}$$
$$Z_9 \times Z_9 \times Z_{11} \times Z_{11}$$
$$Z_9 \times Z_3 \times Z_3 \times Z_{121}$$
$$Z_9 \times Z_3 \times Z_3 \times Z_{11} \times Z_{11}$$
$$Z_3 \times Z_3 \times Z_3 \times Z_3 \times Z_{121}$$
$$Z_3 \times Z_3 \times Z_3 \times Z_3 \times Z_{11} \times Z_{11}$$

The corresponding invariant factors are: (9801), $(891, 11)$, $(3267, 3)$, $(297, 33)$, $(1089, 9)$, $(99, 99)$, $(1089, 3, 3)$, $(99, 33, 3)$, $(363, 3, 3, 3)$, $(33, 33, 3, 3)$

Using the Fundamental theorem and Primary Decomposition theorem, we can also find the elementary divisors from invariant factors in a very similar fashion. This shows the power of these two theorems.

4. In this exercise, we will see how to determine whether direct products of cyclic groups are isomorphic. We will do only one part.

Here, $\{a_1, ..., a_n\}$ denotes $Z_{a_1} \times ... \times Z_{a_n}$.

(c) Here, we are given the groups $\{5^2 \cdot 7^2, 3^2 \cdot 5 \cdot 7\}$, $\{3^2 \cdot 5^2 \cdot 7, 5 \cdot 7^2\}$, $\{3 \cdot 5^2, 7^2, 3 \cdot 5 \cdot 7\}$, $\{5^2 \cdot 7, 3^2 \cdot 5, 7^2\}$.

We will use the fact that two finite abelian groups are isomorphic if and only if they have the same set of elementary divisors. The given groups are

$$Z_{5^2 \cdot 7^2} \times Z_{3^2 \cdot 5 \cdot 7} \cong Z_{3^2} \times Z_{5^2} \times Z_5 \times Z_{7^2} \times Z_7$$
$$Z_{3^2 \cdot 5^2 \cdot 7} \times Z_{5 \cdot 7^2} \cong Z_{3^2} \times Z_{5^2} \times Z_5 \times Z_{7^2} \times Z_7$$
$$Z_{3 \cdot 5^2} \times Z_{7^2} \times Z_{3 \cdot 5 \cdot 7} \cong Z_3 \times Z_3 \times Z_{5^2} \times Z_5 \times Z_{7^2} \times Z_7$$
$$Z_{5^2 \cdot 7} \times Z_{3^2 \cdot 5} \times Z_{7^2} \cong Z_{3^2} \times Z_{5^2} \times Z_5 \times Z_{7^2} \times Z_7$$

And hence once easily sees that the first, second and third groups are isomorphic to each other.

The idea here was to split each cyclic group into primes, and look at the elementary divisors.

5. Let G be a finite abelian group of type $(n_1, ..., n_t)$. We will show that G contains an element of order m if and only if $m | n_1$. We write G as

$$G \cong Z_{n_1} \times ... \times Z_{n_t}$$

Let $(a_1, ..., a_t) \in G$. Clearly, the order of this element is the lcm of the orders of a_i in Z_{n_i}. Moreover, each of these orders divide n_1, and hence it follows that if the order of this element is m, then $m | n_1$.

Conversely, if $m | n_1$, then there is an element a_1 of order 1 in Z_{n_1}, and hence the element $(a_1, 1, ..., 1)$ has order m in G. This proves the claim.

From this, it is easy to conclude that the exponent of G is n_1.

9. Let $A = Z_{60} \times Z_{45} \times Z_{12} \times Z_{36}$. We will find the number of elements of order 2 and the number of subgroups of index 2.

First, we rewrite G in terms of its elementary divisors:

$$G \cong Z_{2^2} \times Z_{2^2} \times Z_{2^2} \times \times Z_{3^2} \times Z_{3^2} \times Z_3 \times Z_3 \times Z_5 \times Z_5$$

Now, any subgroup of G may be written in terms of its elementary divisors as well. Any subgroup

Recognition Theorems: Now, we will see how to recognize direct products. Let's begin with some definitions. Let $x, y \in G$. Define

$$[x, y] = x^{-1}y^{-1}xy$$

to be the *commutator* of x and y. Define G' to be the subgroup of G generated by all commutators of elements of G.

Intuitively, the commutator sort of approximates how much the elements x and y commute. This is justified by the following:

Theorem 31.1. Let G be a group, and let $x, y \in G$ and $H \leq G$. Then

(1) $xy = yx[x, y]$
(2) $H \trianglelefteq G$ if and only if $[H, G] \leq H$.
(3) Let $\sigma \in \mathrm{Aut}(G)$. Then, $[\sigma(x), \sigma(y)] = \sigma([x, y])$. G' char G and G/G' is abelian.
(4) G/G' is the largest abelian quotient of G in the sense if $H \trianglelefteq G$ and G/H is abelian, then $G' \leq H$. Conversely, if $G' \leq H$, then H is normal and G/H is abelian.

(1) is immediate from the definition. To prove (2), suppose $H \trianglelefteq G$. Let $x \in H$ and $y \in G$. Then, we see that $[x, y] = x^{-1}y^{-1}xy \in H$, and hence $[H, G] \leq H$. Conversely, if $[H, G] \leq H$, then it follows that for any $y \in G$ and $x \in H$, we have that $x^{-1}y^{-1}xy \in H$, and hence $H \trianglelefteq G$.

Now, suppose σ is an automorphism. Then, we have

$$[\sigma(x), \sigma(y)] = \sigma(x^{-1})\sigma(y^{-1})\sigma(x)\sigma(y) = \sigma(x^{-1}y^{-1}xy) = \sigma[x, y]$$

which proves the formula. Next, we will show that G' is characteristic. To show this, it is enough to show that for any $x, y \in G$, $\sigma[x, y] \in G'$. But this is clear from the fact that $\sigma[x, y] = [\sigma(x), \sigma(y)]$, and this proves the claim.

Next, let us show that G/G' is abelian. Suppose $x, y \in G$. Then, we see that $x^{-1}y^{-1}xy \in G'$, and hence $xyG' = yxG'$, so that G/G' is abelian.

Next, we will prove (4). Suppose $H \trianglelefteq G$ and G/H is abelian. It then follows that $(xy)H = (yx)H$ for all $x, y \in G$, and hence $[x, y] \in H$. This means that $G' \leq H$. Conversely, suppose $G' \leq H$. Now, since G/G' is abelian, it follows that

$$H/G' \trianglelefteq G/G'$$

and hence $H \trianglelefteq G$ by the fourth isomorphism theorem. Moreover, we have

$$(G/G')/(H/G') \cong G/H$$

and hence G/H is abelian.

Next, we have a useful result:

Theorem 31.2. Suppose H, K are subgroups of G. Consider an element of HK. The number of ways of writing this element as a product hk, where $h \in H$ and $k \in K$ is $|H \cap K|$.

Proof: Suppose $x \in HK$. Then, we $x = hk$ for some $h \in H$ and $k \in K$. Now, for every element $y \in H \cap K$, we can write

$$x = hk = (hy^{-1})(yk)$$

so this gives us atleast $|H \cap K|$ ways of writing x as a product. To show that there are exactly $|H \cap K|$ ways, observe that if

$$hk = h_1k_1$$

then $h_1 - 1h = k_1k^{-1} = y$ so that $y \in |H \cap K|$. This proves the claim.

We will now look at the *recognition theorem*:

Theorem 31.3. Suppose G is a group with subgroups H and K such that

(1) H and K are normal.
(2) $H \cap K = 1$

then

$$HK \cong H \times K$$

Proof: Clearly, we know that HK is a subgroup. Consider the map

$$\varphi : HK \to H \times K$$

given by

$$hk \mapsto (h, k)$$

This is clearly an onto map. It is one-one because $H \cap K = 1$, and hence every element can be written in exactly one way as a product. So, this map is a bijection.

Finally, we show that it is a homomorphism. To see this, we first observe that for h_1k_1 and h_2k_2 in HK, we have

$$h_1k_1h_2k_2 = h_1(k_1h_2k_1^{-1})k_1k_2 = h_1h_2(h_2^{-1}k_1h_2)k_2$$

and hence since $H \cap K = 1$, we have $k_1h_2k^{-1} = h_2$, which means that $h_2k_1 = k_1h_2$. So, we have $h_1k_1h_2k_2 = h_1h_2k_1k_2$ and hence

$$\varphi(h_1k_1h_2k_2) = (h_1h_2, k_1k_2)$$

showing that φ is a homomorphism. This completes the proof.

Note: We can infact show that every element of H commutes with every element of K by a similar argument.

For such subgroups H and K, we define HK to be the *internal direct product* and $H \times K$ to be the *external direct product*. The above theorem shows the this is only a matter of notation.

32. Exercises on Page 173

33. Semi-Direct Producst

In the case of direct products, note that H and K were both normal in G, and only then were we able to relate HK to $H \times K$. We can get rid of the requirement that K is normal, and this leads us to the notion of *semi-direct products*.

First, suppose G is a group with $H \trianglelefteq G$ and $K \leq G$ (we don't know about the normality of K), such that $H \cap K = 1$. Then, the there is still a *bijection* between HK and $H \times K$. Also, as we did before, we have

$$h_1k_1h_2k_2 = h_1(k_1h_2k_1^{-1})k_1k_2 = h_1(k_1 \cdot h_2)k_1k_2$$

where K acts on H via conjugation, and hence we have a map $\pi : K \to \text{Aut(H)}$. Note that if we know π *apriori*, then we can drop the reference to G whatsover, and we can just talk in terms of H, K and π. This is the exact idea of as given below:

Theorem 33.1. Let H and K be groups, and let $\pi : K \to \text{Aut}(H)$ be a homomorphism (so it induces a group action of K on H). Let $\cdot$ denote this left action. Define G to be the set of ordered pairs (h, k) with $h \in H$ and $k \in K$, and define multiplication in G by

$$(h_1, k_1)(h_2, k_2) = (h_1 k_1 \cdot h_2, k_1 k_2)$$

Then, the following are true:

(1) G is a group of order $|H||K|$.
(2) G contains isomorphic copies of H and K. Denote the isomorphic copy of H in G by H. Then, $H \trianglelefteq G$.
(3) $H \cap K = 1$, where H and K are the isomorphic copies.

Before proving the claim, we denote the group G by $H \rtimes K$, and call this the *semi-direct product*.

Proof: First, let's prove that G is a group. The identity element is $(1, 1)$, because for any (h, k) we have

$$(1, 1)(h, k) = (\pi(1)(h), k) = (h, k)$$

and also

$$(h, k)(1, 1) = (h\pi(k)(1), k) = (h, k)$$

because $\pi(k)$ is an automorphism of H.

Next, suppose $(h, k) \in G$. Then, we have

$$(h, k)((\pi(k))^{-1}(h^{-1}), k^{-1}) = (1, 1)$$

and hence every element has an inverse. The proof of the associative laws is as follows:

$$\begin{aligned}
[(h_1, k_1)(h_2, k_2)](h_3, k_3) &= (h_1 k_1 \cdot h_2, k_1 k_2)(h_3, k_3) \\
&= (h_1 k_1 \cdot h_2 (k_1 k_2) \cdot h_3, k_1 k_2 k_3) \\
&= (h_1 k_1 \cdot h_2 k_1 \cdot (k_2 \cdot h_3), k_1 k_2 k_3) \\
&= (h_1 k_1 \cdot (h_2 k_2 \cdot h_3), k_1 k_2 k_3) \\
&= (h_1, k_1)[(h_2 k_2 \cdot h_3, k_2 k_3)] \\
&= (h_1, k_1)[(h_2, k_2)(h_3, k_3)]
\end{aligned}$$

where we used that fact that $k_2 \cdot a k_2 \cdot b = k_2 \cdot (ab)$ (this is true because $\pi(k)$ is an automorphism). The order of G is clearly $|H||K|$.

To prove (2), consider the set $H' = \{(h, 1)\}$ and $K' = \{(1, k)\}$. We show that $H' \cong H$ and $K' \cong K$. Consider the map $\varphi : H' \to H$ given by $(h, 1) \mapsto h$. This map is obviously a bijection. It is also a homomorphism because

$$\varphi[(h_1, 1)(h_2, 1)] = \varphi[h_1 h_2, 1] = h_1 h_2$$

and this shows that isomorphism. The proof that $K' \cong K$ is also similar. From now, we will refer to these isomorphic copies as H and K.

Next, we will show that H is normal in G. To show this, let $(h,k) \in G$ and $(x,1) \in H$. So, we have

$$\begin{aligned}(h,k)(x,1)(h,k)^{-1} &= (h,k)(x,1)(k^{-1}\cdot h^{-1}, k^{-1}) \\ &= (hk\cdot x, k)(k^{-1}\cdot h^{-1}, k^{-1}) \\ &= (hk\cdot xh^{-1}, 1) \in H\end{aligned}$$

and hence H is normal.

The fact that H and K intersect trivially is clear. This completes the proof.

Remark: Observe that $H \rtimes K = HK$, where the H and K on the right hand side are isomorphic copies inside $H \rtimes K$.

The notation for the semi-direct product is useful because it reminds us which of the factors is normal, and the other factor need not be normal.

We now see when semi-direct products are the direct products:

Theorem 33.2. Let H and K be groups, and let $\pi : K \to \mathrm{Aut}(H)$ be a homomorphism. Then, the following are equivalent:

(1) The identity map between $H \rtimes K$ and $H \times K$ is a homomorphism (and hence an isomorphism).
(2) π is the trivial homomorphism from K to $\mathrm{Aut}(H)$.
(3) $K \trianglelefteq H \rtimes K$

Proof: First, suppose (1) is true, and hence $\mathrm{id} : H \rtimes K \to H \times K$ is an isomorphism. Now, let (h_1,k_1) and $(h_2,k_2) \in H \rtimes K$. Then, we have

$$\mathrm{id}[(h_1,k_1)(h_2,k_2)] = (h_1h_2, k_1k_2)$$

but we know that

$$\mathrm{id}[(h_1,k_1)(h_2,k_2)] = \mathrm{id}(h_1\pi(k_1)(h_2), k_1k_2) = (h_1\pi(k_1)(h_2), k_1k_2)$$

which means that $\pi(k_1)(h_2) = h_2$, and hence $\pi(k_1)$ is the trivial automorphism of H. So, $\pi : K \to \mathrm{Aut}(H)$ is the trivial homomorphism, and hence (2) follows.

Now, suppose (2) is true. Let $(1,k_0) \in K \leq H \rtimes K$, and let $(h,k) \in H \rtimes K$. First, observe that $(h,k)^{-1} = (k^{-1}\cdot h^{-1}, k^{-1}) = (h^{-1}, k^{-1})$ and hence

$$\begin{aligned}(h,k)(1,k_0)(h,k)^{-1} &= (h,k)(1,k_0)(h^{-1},k^{-1}) \\ &= (h,kk_0)(h^{-1},k^{-1}) \\ &= (1, kk_0k^{-1}) \in K\end{aligned}$$

and hence $K \trianglelefteq H \rtimes K$.

Now, suppose (3) is true, i.e $K \trianglelefteq H \rtimes K$. Let $k_0, k \in K$, and let $h \in H$. Then, we know that

$$(h,k)(1,k^{-1}k_0k)(k^{-1}\cdot h^{-1}, k^{-1}) \in K$$

Upon actual multiplication, we see that

$$\begin{aligned}(h,k)(1,k^{-1}k_0k)(k^{-1}\cdot h^{-1},k^{-1}) &= (hk\cdot 1, k_0k)(k^{-1}\cdot h^{-1}, k^{-1}) \\ &= (hk\cdot 1(k_0k)\cdot(k^{-1}\cdot h^{-1}), k_0) \\ &= (hk_0\cdot h^{-1}, k_0)\end{aligned}$$

and hence this means that $k_0 \cdot h^{-1} = h^{-1}$. Since h was arbitrary, it follows that $\pi(k_0)$ is the trivial automorphism, and hence $\pi : K \to \mathrm{Aut}(H)$ is the trivial homomorphism.

This means that mutiplication in $H \rtimes K$ is the same as that in $H \times K$, and hence the identity map is a homomorphism.

As in the case of direct products, there is a recognition theorem for semi-direct products as well. We now prove it:

Theorem 33.3. Suppose G is a group, and let $H \trianglelefteq G$ and $K \leq G$ with $H \cap K = 1$. Let π be the homomorphism $\pi : K \to \mathrm{Aut}(H)$ that sends k to σ_k, where $\sigma_k(h) = khk^{-1}$ for $h \in H$. Then, $HK \cong H \rtimes K$. In particular if $G = HK$, then $G \cong H \rtimes K$.

Proof: Consider the map $\varphi : HK \to H \rtimes K$ given by

$$\varphi(hk) = (h, k)$$

which is obviously a bijection. To prove that it is a homomorphism, we have

$$\varphi(h_1k_1h_2k_2) = \varphi(h_1k_1 \cdot h_2k_1k_2) = (h_1k_1 \cdot h_2, k_1k_2) = \varphi(h_1k_1)\varphi(h_2, k_2)$$

and hence $HK \cong H \rtimes K$.

Let's make a quick definition: Let $H \leq G$. We say that $K \leq G$ is the *complement* of H if $G = HK$ and $H \cap K = 1$.

Now we look at some examples.

Example 33.4.