திருவள்ளுவர் பல்கலைக்கழகம்
THIRUVALLUVAR UNIVERSITY
(State University Accredited with "B" Grade by NAAC)
Serkkadu, Vellore - 632 115, Tamil Nadu, India.

TVU E- Recourse Centre

Subject: MATHEMATICS **Paper:** Algebra

Topic/Module: Group theory - I

Faculty Name: Dr. G. KALAIMURUGAN

Faculty Address: Assistant Professor,

Department of Mathematics,

Thiruvalluvar University, Vellore.

Contents

0.1 Set Theory

Definition 0.1.1. *A set is a collection of objects, which are called elements . The order of the elements does not matter, and each element may occur no more than once.*

Note 0.1.2. *For example,* $\{1, 2, 5\}$ *denotes a set with three elements:* 1*,* 2*, and* 5*.* $\{2, 5, 1\}$ *is the same set, since the order of the elements does not matter.* $\{2, 2, 2\}$ *is not a valid set, because the element* 2 *occurs more than once. Note that the elements of a set do not have to be numbers; they could be any sort of object, like people, types of cheese, triangles, binary operations, or even other sets.*

Notations

set notation As seen above, one way to describe a set is to literally list its elements and place them in curly braces, like this: $\{1, 3, 69\}$.

special sets: $\emptyset$*,* $\mathbb{N}$*,* $\mathbb{Z}$*,* $\mathbb{Q}$*,* $\mathbb{R}$*,* $\mathbb{C}$ There are also some important sets which have special notation. Here are a few:

- $\emptyset$ denotes the empty set—the unique set which contains no elements. Sometimes it is also written $\{\}$.
- $\mathbb{N}$ stands for the set of all natural numbers, that is, $\mathbb{N} = \{0, 1, 2, 3, \dots\}$.
- $\mathbb{Z}$ stands for the set of all integers, that is, $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$.

- $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ stand for the set of all rational numbers, all real numbers, and all complex numbers, respectively.

0.2 Introduction to Groups

Modern algebra is largely concerned with the study of abstract set with one or more binary operations.In this section the basic algebraic structure are introduced and some example are given.

Definition 0.2.1. *1. A binary operation $\star$ on a set G is a function $\star : G \times G \longrightarrow G$. For any $a, b \in G$ we shall write $a \star b$ for $\star(a, b)$*

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

3. If $\star$ is a binary operation on a set G we say elements a and b of G commute if $a \star b = b \star a$. We say $\star(orG)$ is commutative if for all $a, b \in G, a \star b = b \star a$.

Example 0.2.2.
- *Usual addition $(+)$ and Usual multiplication (X) are commutative binary operation on $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$.*
- *Usual subration $(-)$ is non commutative binary operation on $\mathbb{Z}$ but not on $\mathbb{Z}^+, \mathbb{Q}^+$ and $\mathbb{R}^+$.*

Definition 0.2.3. 1. A group is an ordered pair $(G, \star)$ where G is a set and $\star$ is a binary operation on G satisfying the following axioms:

- $(a \star b) \star c = a \star (b \star c)$, for all $a, b, c \in G$, i.e., $\star$ is associative,
- there exists an element e in G, called an identity of G, such that for all $a \in G$ we have $a \star e = e \star a = a$,
- for each $a \in G$ there is an element a^{-1} of G, called an inverse of a, such that $a \star a^{-1} = a^{-1} \star a = e$

2. The group $(G, \star)$ i s called abelian (or commutative) if $a \star b = b \star a$ for all $a, b \in G$.

Example 0.2.4.
- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ *and* $\mathbb{C}$ *are abelian group under usual addition.*
- $\mathbb{Q} - 0, \mathbb{R} - 0, \mathbb{C} - 0, \mathbb{Q}^+, \mathbb{R}^+$ *are group under usual multiplication.*
- *The set of all $2X2$ matrices entries from $\mathbb{R}$ are group under matrix addition.*
- $\mathbb{N}$ *is not a group under usual addition.*
- $\mathbb{Q}^+$ *is a group under usual multiplication.*
- $\mathbb{Z}$ *is not a group under usual multiplication.*
- $G = \{1, i, -1, -i\}$ *is a group under usual multiplication.*

- *The set of all n^{th} root of unity are form a group under usual multiplication.*
- *$(\mathbb{Z}_n, \bigoplus)$ is a group.*

Proposition 0.2.5. *If G is a group under the operation $\star$, then*

1. *the identity of G is unique*
2. *for each $a \in G, a^{-1}$ is uniquely determined*
3. *$(a^{-1})^{-1} = a$ for all $a \in G$*
4. *$(a \star b)^{-1} = (b^{-1}) \star (a^{-1})$*
5. *for any $a_1, a_2, \ldots, a_n \in G$ the value of $a_1 \star a_2 \star \ldots \star a_n$ is independent of how the expression is bracketed (this is called the generalized associative law).*

Theorem 0.2.6. *Let G be a group and $a, b \in G$ Then the equation $ax = b$ and $ya = b$ have unique solution for x and y in G.*

Theorem 0.2.7. *Reversal law Let G be a group. $a, b \in G$ then $(ab^{-1}) = b - 1a^{-1}$.*

Problem 0.2.8. *Let G be a group. $a \in G$ with $a^2 = a$ iff $a = e$.*

Solution. Let $a = e$ to prove that $a^2 = a$. $a^2 = aa = ee = e = a$.
Conversely, Let $a^2 = a$ Then $aa = ae$. Hence by cancelation law $a = e$. □

Problem 0.2.9. *Let G be a group with $a^2 = e$ for all $a \in G$. Then G is abelian.*

Problem 0.2.10. *Let G be a group with $(ab)^m = a^m b^m$ for three consecutive integer and for all $a, b \in G$. Then G is abelian.*

0.3 Dihedral Group

Dihedral groups are apparent throughout art and nature. For example, dihedral groups are often the basis of decorative designs on floor tilings, buildings, and artwork. Chemists and mineralogists study dihedral groups to classify the structure of molecules and crystals, respectively. These symmetry groups are even used in advertising for many of the world's largest companies.

For each $n \in \mathbb{Z}^+, n \geq 3$ let D_{2n} be the set of symmetries of a regular n-gon, where a symmetry is any rigid motion of the n-gon which can be effected by taking a copy of the n-gon, moving this copy in any fashion in 3-space and then placing the copy back on the original n-gon so it exactly covers it. A presentation for the dihedral group D_{2n} (using the generators and relations) is then $D_{2n} = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \rangle$.

Remark 0.3.1.
- $1, r, r^2, \ldots, r^{n-1}$ are all distinct and $r^n = 1$, so $|r| = n$

- $|s| = 2$.
- $s \neq r^i$ for any i
- $sr^i \neq sr^j$, for all $0 \leq i, j \leq n-1$ with $i \neq j$, so $D_{2n} = \{1, r, r^2, \ldots, r^{n-1}, s, sr, \ldots, sr^{n-1}\}$
- $r^i s = sr^{-i}$, for all $0 \leq i \leq n$.

Problem 0.3.2. Compute the order of each of the elements in the following groups: (a) D_6 (b) D_8 (c) D_{10}.

Solution. Recall that every element of D_{2n} can be represented uniquely as $s^i r^j$ for some $i = 0, 1$ and $0 \leq j < n$. Moreover, $r^i s = sr^{-i}$ for all $0 \leq i \leq n$. From this we deduce that $(sr^i)(sr^i) = ssr^{-i}r^i = 1$, so that sr^i has order 2 for $0 \leq i \leq n$ (a) $D_6 = \{1, r, r^2, s, sr, sr^2\}$, Let the order of an element α is denoted by $|\alpha|$. Then $|1| = 1, |r| = 3, |r^2| = 3, |s| = |sr| = |sr^2| = 2$. (b)In D_8, $|1| = 1, |r| = 4, |r^2| = 2, |r^3| = 4, |s| = |sr| = |sr^2| = |sr^3| = 2$. (c) In D_{10}, $|1| = 1, |r| = |r^2| = |r^3| = |r^4| = 5, |s| = |sr| = |sr^2| = |sr^3| = |sr^4| = 2$. □

Problem 0.3.3. Use the generators and relations above to show that if x is any element of D_{2n} which is not a power of r, then $rx = xr^{-1}$.

Solution. Every element $x \in D_{2n}$ is of the form $x = s^i r^j$ where $i = 0, 1$ and $0 \leq j < n$. If $i = 0$ we have that x is a power of r; thus $x = sr^j$ for some $0 \leq j < n$. Hence $rx = rsr^j = sr^{-1}r^j = sr^j r^{-1} = xr^{-1}$. □

Problem 0.3.4. Let x and y be elements of order 2 in any group G. Prove that if $t = xy$ then $tx = xt^{-1}$ (so that if $n = |xy| < \infty$ then x, t satisfy the same relations in G as s, r do in D_{2n}).

Solution. We have $xt^{-1} = x(xy)^{-1} = xy^{-1}x^{-1} = xyx = tx$ since x and y have order 2. □

Problem 0.3.5. Find the order of the cyclic subgroup of D_{2n} generated by r.

Solution. We know that $|r| = n$. Thus, the elements of subgroup A are precisely $1, r, r^2, \ldots, r^{n-1}$; thus $|A| = n$ □

0.4 Subgroup

A non empty sub set H of a Group is a subgroup of G, if it satisfies the following conditions

- $a, b \in H \Rightarrow ab \in H$
- $a \in H \Rightarrow a^{-1} \in H$
- $e \in H$

Note 0.4.1. *The identity element of a subgroup is same as the identity element of a Group.*

Note 0.4.2. *The identity element and whole group are two improper subgroup of the group.*

Example 0.4.3. *Let $\mathbb{Z}$ is a group then $2\mathbb{Z}$ is subgroup of $\mathbb{Z}$.*

Example 0.4.4.

1. $\mathbb{Z} \leq \mathbb{Q}$ and $\mathbb{Q} \leq \mathbb{R}$ with the operation of addition.
2. Any group G has two subgroups: $H = G$ and $H = \{1\}$; the latter is called the trivial subgroup and will henceforth be denoted by 1 .
3. If $G = D_{2n}$ is the dihedral group of order $2n$, let H be $\{1, r, r^2, ..., r^{n-1}\}$, the set of all rotations in G. Since the product of two rotations is again a rotation and the inverse of a rotation is also a rotation it follows that H is a subgroup of D_{2n} of order n.

Theorem 0.4.5. *(The Subgroup Criterion) Show that the non-empty subset H of a group G is a subgroup of G if and only if $a, b \in H \Rightarrow ab^{-1} \in H$.*

Proof. $\Rightarrow$ Let H be a subgroup of G. Then clearly H satisfies the condition $a, b \in H \Rightarrow ab^{-1} \in H$. $\Leftarrow$ Let H be a non-empty subset of G satisfying the given condition, To prove that H is a subgroup.
By given condition,

- $a, a \in H \Rightarrow a, a^{-1} \in H \Rightarrow aa^{-1} = e \in H$.
- $e, a \in H \Rightarrow e, a^{-1} \in H \Rightarrow a^{-1} \in H$.
- $a, b \in H \Rightarrow a, b^{-1} \in H \Rightarrow a(b^{-1})^{-1} \in H \Rightarrow ab \in H$.

Hence H is subgroup of G. □

Problem 0.4.6. Show that the following subsets of the dihedral group D_8 are actually subgroups: (a) $\{1, r^2, s, sr^2\}$, (b) $\{1, r^2, sr, sr^3\}$

Solution. (a) We have $r^2r^2 = 1, r^2s = sr^2, r^2sr^2 = s, sr^2 = sr^2, ss = 1, ssr^2 = r^2, sr^2r^2 = s, sr^2s = r^2$, and $sr^2sr^2 = 1$, so that this set is closed under multiplication. Moreover, $(r^2)^{-1} = r^2, s^{-1} = s$, and $(sr^2)^{-1} = sr^2$, so this set is closed under inversion. Thus it is a subgroup.
(b) We have $r^2r^2 = 1, r^2sr = sr^3, r^2sr^3 = sr, srr^2 = sr^3, srsr = 1, srsr^3 = r^2, sr^3r^2 = sr, sr^3sr = r^2$, and $sr^3sr^3 = 1$, so that this set is closed under multiplication. Moreover, $(r^2)^{-1} = r^2, (sr)^{-1} = sr$, and $(sr^3)^{-1} = sr^3$, so this set is closed under inversion. Thus it is a subgroup. □

Problem 0.4.7. Prove that G cannot have a subgroup H with $|H| = n - 1$, where $n = |G| > 2$.

Solution. Under these conditions, there exists a nonidentity element $x \in H$ and an element $y \notin H$. Consider the product xy. If $xy \in H$, then since $x^{-1} \in H$ and H is a subgroup, $y \in H$, a contradiction. If $xy \notin H$, then we have $xy = y$. Thus $x = 1$, a contradiction. Thus no such subgroup exists. □

Problem 0.4.8. Let H and K be subgroups of G. Prove that $H \cup K$ is a subgroup if and only if either $H \subseteq K$ or $K \subseteq H$.

Solution. The ($\Leftarrow$) direction is clear. To see ($\Rightarrow$), suppose that $H \cup K$ is a subgroup of G and that $H \not\subseteq KandK \not\subseteq H$; that is, there exist $x \in H$ with $x \notin K$ and $y \in K$ with $y \notin H$. Now we have $xy \in H \cup K$, so that either $xy \in H$ or $xy \in K$. If $xy \in H$, then we have $x^{-1}xy = y \in H$, a contradiction. Similarly, if $xy \in K$, we have $x \in K$, a contradiction. Then it must be the case that either $H \subseteq K$ or $K \subseteq H$. □

Problem 0.4.9. Let G be a group. (a) Prove that if H and K are subgroups of G, then so is $H \cap K$.
(b) Prove that if $\{H_i\}_{i \in I}$ is a family of subgroups of G then so is $\bigcap_{i \in I} H_i$.(or)Prove that the intersection of an arbitrary nonempty collection of subgroups of G is again a subgroup of G (do not assume the collection is countable)

Solution. (a) Note that $H \cap K$ is not empty since $1 \in H \cap K$. Now suppose $x, y \in H \cap K$. Then since H and K are subgroups, we have $xy^{-1} \in H$ and $xy^{-1} \in K$ by the subgroup criterion; thus $xy^{-1} \in H \cap K$. By the subgroup criterion, $H \cap K$ is a subgroup of G.
(b) Note that $\bigcap_{i \in I} H_i$ is not empty since $1 \in H_i$ for each $i \in I$. Now let $x, y \in \bigcap_{i \in I} H_i$. Then $x, y \in H_i$ for each $i \in I$, and by the subgroup criterion, $xy^{-1} \in H_i$ for each $i \in I$. Thus $xy^{-1} \in \bigcap_{i \in I} H_i$. By the subgroup criterion, $\bigcap_{i \in I} H_i$ is a subgroup of G. □

Note 0.4.10.
- *Intersection of Two subgroups is subgroup.*
- *Union of two subgroups is need not be a subgroup.*

Theorem 0.4.11. *Let H, K be any two subgroup of a group G. Show that HK is a subgroup of G if and only if $HK = KH$.*

Proof. Let as assume that HK is a subgroup of G. We have to show that $HK = KH$. Consider $x \in HK \Rightarrow x^{-1} \in HK$. Let $x^{-1} = hk$ where $h \in H$ and $k \in K$

$$\begin{aligned} (x^{-1})^{-1} &= (hk)^{-1} \\ &= k^{-1}h^{-1} \\ x &\in KH \end{aligned}$$

i.e, $HK \subseteq KH$. Similarly we show that $KH \subseteq HK$. Hence $HK = KH$.
Conversely, Let as assume that $HK = KH$. We prove that HK is subgroup of G. Let $x, y \in HK \Rightarrow x = hk, y = h'k'$ where $h, h' \in H$ and $k, k' \in K$

$$\begin{aligned} xy^{-1} &= hk(h'k')^{-1} \\ &= hk(k'^{-1}h'^{-1}) \\ &= h(kk'^{-1})h'^{-1} \\ &= hk''h'^{-1} \end{aligned}$$

where, $kk'^{-1} = k''$ Let $k''h'^{-1} = h''k'''$ since by our assumption.

$$\begin{aligned} xy^{-1} &= hh''k''' \\ &= h'''k''' \\ xy^{-1} &\in HK \end{aligned}$$

Hence HK is subgroup of G. □

0.5 Centralizers and Normalizer, Stabilizers and Kernels

We now introduce some important families of subgroups of an arbitrary group G which in particular provide many examples of subgroups. Let A be any nonempty subset of G.

Definition 0.5.1. Define $C_G(A) = \{g \in G | gag^{-1} = a \text{ for all } a \in A\}$. This subset of G is called the *centralizer* of A in G. Since $gag^{-1} = a$ if and only if $ga = ag, C_G(A)$ is the set of elements of G which commute with every element of A.

Definition 0.5.2. Define $Z(G) = \{g \in G | gx = xg \text{ for all } x \in G\}$, the set of elements commuting with all the elements of G . This subset of G is called the *center* of G .

Definition 0.5.3. Define $gAg^{-1} = \{gag^{-1} | a \in A\}$. Define the *normalizer* of A in G to be the set $N_G(A) = \{g \in G | gAg^{-1} = A\}$.

Example 0.5.4. If G is abelian then all the elements of G commute, so $Z(G) = G$. Similarly, $C_G(A) = N_G(A) = G$ for any subset A of G since $gag^{-1} = gg^{-1}a = a$ for every $g \in G$ and every $a \in A$.

Definition 0.5.5. if G is a group acting on a set S and s is some fixed element of S, the *stabilizer* of s in G is the set $G_s = \{g \in G | g \cdot s = s\}$.

Problem 0.5.6. Prove that $C_G(A) = \{g \in G | g^{-1}ag = a \text{ for all } a \in A\}$.

Solution. By definition, $C_G(A) = \{g \in G \mid gag^{-1} = a \text{ for all } a \in A\}$.

($\subseteq$) If $g \in C_G(A)$, then $gag^{-1} = a$ for all $a \in A$. Left multiplying by g^{-1} and right multiplying by g, we have that $a = g^{-1}ag$ for all $a \in A$.

($\supseteq$) If $g \in G$ such that $g^{-1}ag = a$ for all $a \in A$, then left multiplying by g and right multiplying by g^{-1} we have that $a = gag^{-1}$ for all $a \in A$. □

Problem 0.5.7. Prove that $C_G(Z(G)) = G$ and deduce that $N_G(Z(G)) = G$

Solution. First we show that $C_G(Z(G)) = G$.

($\subseteq$) is clear. ($\supseteq$) Suppose $g \in G$. Then by definition, for all $a \in Z(G)$, we have $ga = ag$. That is, for all $a \in Z(G)$, we have $a = gag^{-1}$. Thus $g \in C_G(Z(G))$.

Since $C_G(Z(G)) \leq N_G(Z(G))$, we have $N_G(Z(G)) = G$ □

Problem 0.5.8. Prove that if A and B are subsets of G with $A \subseteq B$ then $C_G(B)$ is a subgroup of $C_G(A)$.

Solution. Let $x \in C_G(B)$. Then for all $b \in B, xbx^{-1} = b$. Since $A \subseteq B$, for all $a \in A$ we have $xax^{-1} = a$, so that $x \in C_G(A)$. Thus $C_G(B) \subseteq C_G(A)$, and hence $C_G(B) \leq C_G(A)$ $\square$

Problem 0.5.9. Let H be a subgroup of order 2 in G . Show that $N_G(H) = C_G(H)$. Deduce that if $N_G(H) = G$, then $H \leq Z(G)$.

Solution. Say $H = \{1, h\}$.

We already know that $C_G(H) \subseteq N_G(H)$. Now suppose $x \in N_G(H)$; then $\{x1x^{-1}$, $xhx^{-1}\} = \{1, h\}$. Clearly, then, we have $xhx^{-1} = h$. Thus $x \in C_G(H)$. Hence $N_G(H) = C_G(H)$.

If $N_G(H) = G$, we have $C_G(H) = G$. Then $ghg^{-1} = h$ for all $h \in H$, so that $gh = hg$ for all $h \in H$, and thus $H \leq Z(G)$. $\square$

Problem 0.5.10. Prove that $Z(G) \leq N_G(A)$ for any subset A of G.

Solution. If $A = \emptyset$, the statement is vacuously true since $N_G(A) = G$. If A is not empty, let $x \in Z(G)$. Then $xax^{-1} = a$ for all $a \in A$, so that $xAx^{-1} = A$. Hence $x \in N_G(A)$. $\square$

0.6 Cyclic Groups and Cyclic Subgroups of a Group

Definition 0.6.1. A group H is *cyclic* if H can be generated by a single element, i.e. , there is some element $x \in H$ such that $H = \{x^n | n \in \mathbb{Z}\}$ (where as usual the operation is multiplication).

Remark 0.6.2. In additive notation H is cyclic if $H = \{nx | n \in \mathbb{Z}\}$. In both cases we shall write $H = \langle x \rangle$ and say H is generated by x (and x is a generator of H). A cyclic group may have more than one generator. For example, if $H = \langle x \rangle$, then also $H = \langle x^{-1} \rangle$.

Proposition 0.6.3. If $H = \langle x \rangle$, then $|H| = |x|$(where if one side of this equality is infinite, so is the other). More specifically (1) if $|H| = n < \infty$, then $x^n = 1$ and $1, x, x^2, \ldots, x^{n-1}$ are all the distinct elements of H, and (2) if $|H| = \infty$, then $x^n \neq 1$ for all $n \neq 0$ and $x^a \neq x^b$ for all $a \neq b$ in $\mathbb{Z}$.

Proposition 0.6.4. Let G be an arbitrary group, $x \in G$ and let $m, n \in \mathbb{Z}$. If $x^n = 1$ and $x^m = 1$, then $x^d = 1$, where $d = (m, n)$. In particular, if $x^m = 1$ for some $m \in \mathbb{Z}$, then $|x|$ divides m .

Theorem 0.6.5. Let $H = \langle x \rangle$ be a cyclic group. Then every subgroup H is cyclic. More precisely, if $K \leq H$, then either $K = \{1\}$ or $K = \langle x^d \rangle$, where d is the smallest positive integer such that $x^d \in K$.

Problem 0.6.6. Find all cyclic subgroups of D_8 . Find a proper subgroup of D_8 which is not cyclic.

Solution. We have the following.

(1) $\langle 1\rangle = \{1\}$ (2)$\langle r\rangle = \{1, r, r^2, r^3\}$ (3)$\langle r^2\rangle = \{1, r^2\}$ (4)$\langle r^3\rangle = \{1, r, r^2, r^3\}$ (5)$\langle s\rangle = \{1, s\}$ (6)$\langle sr\rangle = \{1, sr\}$ (7)$\langle sr^2\rangle = \{1, sr^2\}$ (8)$\langle sr^3\rangle = \{1, sr^3\}$. We know that $\{1, r^2, s, r^2s\}$ is a subgroup of D_8, but is not on the above list, hence is not cyclic. □

Problem 0.6.7. Let p be a prime and let n be a positive integer. Show that if x is an element of the group G such that $x^{Pn} = 1$ then $|x| = p^m$ for some $m \leq n$.

Solution. We prove a lemma.

Lemma: Let G be a group and $x \in G$ an element of finite order, say, $|x| = n$. If $x^m = 1$, then n divides m. **Proof:** Suppose to the contrary that n does not divide m; then by the Division Algorithm there exist integers q and r such that $0 < r < |n|$ and $m = qn + r$. Then we have $1 = x^m = x^{qn+r} = (x^n)^q + x^r = x^r$. But recall that by definition n is the least positive integer with this property, so we have a contradiction. Thus n divides m. □

Problem 0.6.8. Let G be a finite group and let $x \in G$.

(1) Prove that if $g \in N_G(\langle x\rangle)$ then $gxg^{-1} = x^a$ for some integer a.
(2) Show conversely that if $gxg^{-1} = x^a$ for some integer a, then $g \in N_G(\langle x\rangle)$. [Hint: Show first that $gx^kg^{-1} = (gkg^{-1})^k = x^{ak}$ for any integer k, so that $g\langle x\rangle g^{-1} \leq \langle x\rangle$. If x has order n, show that the elements gx^ig^{-1} are distinct for $i \in \{0, 1, \ldots, n-1\}$, so that $|g\langle x\rangle g^{-1}| = |\langle x\rangle| = n$ and conclude that $g\langle x\rangle g^{-1} = \langle x\rangle$.]

Solution. (1) Let $g \in N_G(\langle x\rangle)$. By definition, we have $gxg^{-1} \in \langle x\rangle$, so that $gxg^{-1} = x^a$ for some integer a.

(2) We prove some lemmas. **Lemma 1:** Let G be a group and let $x, g \in G$. Then for all integers $k, gx^kg^{-1} = (gxg^{-1})^k$. **Proof:** First we prove the conclusion for nonnegative k by induction on k. If $k = 0$, we have $gx^0g^{-1} = gg^{-1} = 1 = (gxg^{-1})^0$. Now suppose the conclusion holds for some $k \geq 0$; then $gx^{k+1}g^{-1} = gxx^kg^{-1} = gxg^{-1}gx^kg^{-1} = gxg^{-1}(gxg^{-1})^k = (gxg^{-1})^{k+1}$. By induction, the conclusion holds for all nonnegative k. Now suppose $k < 0$; then $gx^kg^{-1} = (gx^{-k}g^{-1})^{-1} = (gxg^{-1})^{-k^{-1}} = (gxg^{-1})^k$. Thus the conclusion holds for all integers k. □

Lemma 2: Let G be a group and let $x, g \in G$ such that $gxg^{-1} = x^a$ for some integer a. Then $g\langle x\rangle g^{-1}$ is a subgroup of $\langle x\rangle$. **Proof:** Let $gx^kg^{-1} \in g\langle x\rangle g^{-1}$; by Lemma 1 we have $gx^kg^{-1} = (gxg^{-1})^k = x^{ak}$, so that $gxg^{-1} \in \langle x\rangle$. Thus $g\langle x\rangle g^{-1} \subseteq \langle x\rangle$. Now let $gx^bg^{-1}, gx^cg^{-1} \in g\langle x\rangle g^{-1}$. Then $gx^bg^{-1}(gx^cg^{-1})^{-1} = gx^bg^{-1}gx^{-c}g^{-1} = gx^{b-c}g^{-1} \in g\langle x\rangle g^{-1}$. By the Subgroup Criterion, then, $g\langle x\rangle g^{-1} \leq \langle x\rangle$. □

Lemma 3: Let G be a group and let $x, g \in G$ such that $gxg^{-1} = x^a$ for some integer a and such that $|x| = n, n \in \mathbb{Z}$. Then $gx^ig^{-1} are distinct for i \in \{0, 1, \ldots, n-1\}$. **Proof:** Choose distinct $i, j \in \{0, 1, \ldots, n-1\}$. By a previous exercise, $x^i \neq x^j$. Suppose now that $gx^ig^{-1} = gx^jg^{-1}$; by cancellation we have $x^i = x^j$, a contradiction. Thus the gx^ig^{-1} are

distinct. □

Now to the main result; suppose $gxg^{-1} = x^a$ for some integer a. Since G has finite order, $|x| = n$ for some n. By Lemma 2, $g\langle x\rangle g^{-1} \leq \langle x\rangle$, and by Lemma 3 we have $|g\langle x\rangle g^{-1}| = |\langle x\rangle|$. Since G is finite, then, we have $g\langle x\rangle g^{-1} = \langle x\rangle$. Thus $g \in N_G(\langle x\rangle)$.

□

0.7 Subgroups Generated by Subsets of a Group

Proposition 0.7.1. If $\mathcal{A}$ is any nonempty collection of subgroups of G, then the intersection of all members of $\mathcal{A}$ is also a subgroup of G.

Proof. This is an easy application of the subgroup criterion (see [**?**]). Let $K = \cap_{H\in\mathcal{A}}H$. Since each $H \in \mathcal{A}$ is a subgroup, $1 \in H$, so $1 \in K$, that is, $K \neq \emptyset$. If $a, b \in K$, then $a, b \in H$, for all $H \in \mathcal{A}$. Since each H is a group, $ab^{-1} \in H$, for all H, hence $ab^{-1} \in K$. Then $K \leq G$. □

Definition 0.7.2. If A is any subset of the group G define $\langle A\rangle = \cap_{A\subseteq H, H\leq G}$. This is called the subgroup of G generated by A.

Problem 0.7.3. Let G be a group. Prove that if $H \leq G$ is a subgroup then $\langle H\rangle = H$.

Solution. That $H \subseteq \langle H\rangle$ is clear. Now suppose $x \in \langle H\rangle$. We can write x as a finite product $h_1h_2\cdots h_n$ of elements of H; since H is a subgroup, then, $x \in H$. □

Problem 0.7.4. Let G be a group, with $A \subseteq B \subseteq G$. Prove that $\langle A\rangle \leq \langle B\rangle$. Give an example where $A \subseteq B$ with $A \neq B$ but $\langle A\rangle = \langle B\rangle$.

Solution. Let $\mathcal{A} = \{H \leq G \mid A \subseteq H\}$ and $\mathcal{B} = \{H \leq G \mid B \subseteq H\}$. Since $A \subseteq B$, we have $A \subseteq H$ whenever $B \subseteq H$; thus $\mathcal{B} \subseteq \mathcal{A}$. By definition, we have $\langle A\rangle = \cap\mathcal{A}$ and $\langle B\rangle = \cap\mathcal{B}$. We know from set theory that $\cap\mathcal{A} \subseteq \cap\mathcal{B}$, so that $\langle A\rangle \subseteq \langle B\rangle$.

Now since $\langle A\rangle$ is itself a subgroup of G, we have $\langle A\rangle \leq \langle B\rangle$.

Now suppose $G = \langle x\rangle$ is cyclic. Then $\{x\} \subsetneq G$, but we have $\langle x\rangle = \langle G\rangle$. □

Problem 0.7.5. Let G be a group and let $H \leq G$ be an abelian subgroup. Show that $\langle H, Z(G)\rangle$ is abelian. Give an explicit example of an abelian subgroup H of a group G such that $\langle H, C_G(H)\rangle$ is not abelian

Solution. We begin with a lemma.

Lemma: Let G be a group, $H \leq G$ an abelian subgroup. Then every element of $\langle H, Z(G)\rangle$ is of the form hz for some $h \in H$ and $z \in Z(G)$. **Proof:** Recall that every element of $\langle H, Z(G)\rangle$ can be written as a (finite) word $a_1a_2\cdots a_k$ for some integer k and $a_i \in H \cup Z(G)$. We proceed by induction on k, the length of a word in $H \cup Z(G)$. If $k = 1$, we have $x = a_1$; if $a_1 \in H$ we have $x = a_1 \cdot 1$, and if $a_1 \in Z(G)$ we have $x = 1 \cdot a_1$.

Now suppose all words of length k can be written in the form hz, and let $x = a_1a_2\cdots a_{k+1}$ be a word of length $k+1$. By the induction hypothesis we have $a_2\cdots a_{k+1} = hz$ for some $h \in H$ and $z \in Z(G)$. Now if $a_1 \in H$, we have $x = (a_1h)\cdot z$, and if $a_1 \in Z(G)$, then $x = h\cdot(a_1z)$. By induction, every element of $\langle H, Z(G)\rangle$ is of the form hz for some $h \in H$ and $z \in Z(G)$.□

Now let $x, y \in \langle H, Z(G)\rangle$. By the lemma we have $x = h_1z_1$ and $y = h_2z_2$ for some $h_1, h_2 \in H$ and $z_1, z_2 \in Z(G)$. Then $xy = h_1z_1h_2z_2 = z_1h_1z_2h_2 = z_1z_2h_1h_2 = z_2z_1h_2h_1 = z_2h_2z_1h_1 = yx$. Hence $\langle H, Z(G)\rangle$ is abelian.

Now to the counterexample; for any group $G, Z(G)$ is an abelian subgroup. By a previous exercise, we know also that $C_G(Z(G)) = G$. Thus if G is any nonabelian group, $\langle Z(G), C_G(Z(G))\rangle = G$ is not abelian. □

Problem 0.7.6. Let G be a group and $H \leq G$. Show that $H = \langle H \setminus \{1\}\rangle$.

Solution. We have $H \setminus \{1\} \subseteq \langle H \setminus \{1\}\rangle$. If $H = 1$, then $\langle H \setminus \{1\}\rangle = \langle\emptyset\rangle = 1 = H$. If $H \neq 1$, there exists some nonidentity $h \in H$. So $h \in H\setminus\{1\}$, so that $hh^{-1} = 1 \in \langle H\setminus\{1\}\rangle$. Thus $H \subseteq \langle H \setminus \{1\}\rangle$.

Now if $x \in \langle H \setminus \{1\}\rangle$, we can write $x = a_1a_2\cdots a_n$ for some integer n and group elements $a_i \in H \setminus \{1\}$; since H is a subgroup, then, $x \in H$. □

0.8 Homomorphisms and Isomorphisms

Definition 0.8.1. Let $(G, \star)$ and $(H, \diamond)$ be groups. A map $\phi : G \to H$ such that $\phi(x \star y) = \phi(x) \diamond \phi(y)$ for all $x, y \in G$, is called a *homomorphism*.

Definition 0.8.2. The map $\varphi : G \to H$ is called an isomorphism and G and H are said to be *isomorphic* or of the same *isomorphism type*, written $G \cong H$, if

1. φ is a homomorphism (i.e.,$\varphi(xy) = \varphi(x)\varphi(y)$), and
2. φ is a bijection.

Let G and H be groups. Solve the following problems.

Problem 0.8.3. Let $\varphi : G \to H$ be a homomorphism. (a) Prove that $\varphi(xn) = \varphi(x)n$ for all $n \in \mathbb{Z}^+$. (b) Do part (a) for $n = -1$ and deduce that $\varphi(xn) = \varphi(x)n$ for all $n \in \mathbb{Z}$.

Solution. (a) We proceed by induction on n. For the base case, $\varphi(x^1) = \varphi(x) = \varphi(x)^1$. Suppose the statement holds for some $n \in \mathbb{Z}^+$; then $\varphi(x^{n+1}) = \varphi(x^nx) = \varphi(x^n)\varphi(x) = \varphi(x)^n\varphi(x) = \varphi(x)^{n+1}$, so the statement holds for n+1. By induction, $\varphi(x^n) = \varphi(x)^n forall n \in \mathbb{Z}^+$.
(b)First, note that $\varphi(x) = \varphi(1_G \cdot x) = \varphi(1_G)\cdot\varphi(x)$. By right cancellation, we have $\varphi(1_G) = 1_H$. Thus $\varphi(x^0) = \varphi(x)^0$. Moreover, $\varphi(x)\varphi(x^{-1}) = \varphi(xx^{-1}) = \varphi(1) = 1$; thus by the uniqueness of inverses, $\varphi(x^{-1}) = \varphi(x)^{-1}$. Now suppose n is a negative integer. Then $\varphi(x^n) = \varphi((x^{-n})^{-1}) = \varphi(x^{-n})^{-1} = (\varphi(x)^{-n})^{-1} = \varphi(x)^n$. Thus $\varphi(x^n) = \varphi(x)^n$ for all $x \in G$ and $n \in \mathbb{Z}$.

□

Problem 0.8.4. If $\varphi : G \to H$ is an isomorphism, prove that G is abelian if and only if H is abelian.

Solution. Let $\varphi : G \to H$ be a group isomorphism.

($\Rightarrow$) Suppose G is abelian, and let $h_1, h_2 \in H$. Since φ is surjective, there exist $g_1, g_2 \in G$ such that $\varphi(g_1) = h_1$ and $\varphi(g_2) = h_2$. Now we have $h_1h_2 = \varphi(g_1)\varphi(g_2) = \varphi(g_1g_2) = \varphi(g_2g_1) = \varphi(g_2)\varphi(g_1) = h_2h_1$. Thus h_1 and h_2 commute; since $h_1, h_2 \in H$ were arbitrary, H is abelian.

($\Leftarrow$) Suppose H is abelian, and let $g_1, g_2 \in G$. Then we have $\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2) = \varphi(g_2)\varphi(g_1) = \varphi(g_2g_1)$. Since φ is injective, we have $g_1g_2 = g_2g_1$. Since $g_1, g_2 \in G$ were arbitrary, G is abelian. □

Problem 0.8.5. Prove that the additive groups $\mathbb{R}$ and $\mathbb{Q}$ are not isomorphic.

Solution. We know that no bijection $\mathbb{Q} \to \mathbb{R}$ exists, so no such isomorphism exists. □

Problem 0.8.6. Define a map $\pi : \mathbb{R}^2 \to \mathbb{R}$ by $\pi((x, y)) = x$. Prove that π is a homomorphism and find the kernel of π.

Solution. To show that π is a homomorphism, let $(x_1, y_1), (x_2, y_2) \in \mathbb{R}^2$. Then $\pi((x_1, y_1) \cdot (x_2, y_2)) = \pi((x_1x_2, y_1y_2)) = x_1x_2 = \pi((x_1, y_1)) \cdot \pi((x_2, y_2))$.

Now we claim that $\ker \pi = 0 \times \mathbb{R}.(\subseteq) If (x, y) \in \ker \pi$ then we have $x = \pi((x, y)) = 0$. Thus $(x, y) \in 0 \times \mathbb{R}.(\supseteq)$ If $(x, y) \in 0 \times \mathbb{R}$, we have $x = 0$ and thus $\pi((x, y)) = 0$. Hence $(x, y) \in \ker \pi$. □

Problem 0.8.7. Let G be any group. Prove that the map from G to itself defined by $g \mapsto g^{-1}$ is a homomorphism if and only if G is abelian.

Solution. ($\Rightarrow$) Suppose G is abelian. Then $\varphi(ab) = (ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1} = \varphi(a)\varphi(b)$, so that φ is a homomorphism.

($\Leftarrow$) Suppose φ is a homomorphism, and let $a, b \in G$. Then $ab = (b^{-1}a^{-1})^{-1} = \varphi(b^{-1}a^{-1}) = \varphi(b^{-1})\varphi(a^{-1}) = (b^{-1})^{-1}(a^{-1})^{-1} = ba$, so that G is abelian. □

Problem 0.8.8. Let G be any group. Prove that the map from G to itself defined by $g \mapsto g^2$ is a homomorphism if and only if G is abelian.

Solution. ($\Leftarrow$) Suppose G is abelian. Then $\varphi(ab) = abab = a^2b^2 = \varphi(a)\varphi(b)$, so that φ is a homomorphism.

($\Rightarrow$) Suppose φ is a homomorphism. Then we have $abab = \varphi(ab) = \varphi(a)\varphi(b) = aabb$, so that $abab = aabb$. Left multiplying by a^{-1} and right multiplying byb^{-1}, we see that $ab = ba$. Thus G is abelian. □

Theorem 0.8.9. *Let $\varphi : G \to H$ be a homomorphism. prove that*

1. *$\varphi(e) = e'$ where e' is identity element of H.*
2. *$\varphi(x^{-1}) = \varphi(x)^{-1}$*

Definition 0.8.10. If φ is a homomorphism $\varphi : G \to H$, the kernel of φ is the set $\{g \in G | \varphi(g) = l\}$ and will be denoted by $ker\varphi$ (here 1 is the identity of H).

Proposition 0.8.11. *Let G and H be groups and let $\varphi : G \to H$ be a homomorphism.*

1. *$\varphi(1_G) = 1_H$, where 1_G and 1_H are the identities of G and H,respectively.*
2. *$\varphi(g^{-1}) = (\varphi(g))^{-1}$ for all $g \in G$.*
3. *$\varphi(g^n) = (\varphi(g))^n$ for all $n \in \mathbb{Z}$.*
4. *$ker\varphi$ is a subgroup of G.*
5. *$im\varphi$, the image of G under φ, is a subgroup of H*

.

Proof. (1) Since $\varphi(1_G) = \varphi(1_G 1_G) = \varphi(1_G)\varphi(1_G)$, the cancellation laws show that (1) holds.
(2) $\varphi(1_G) = \varphi(gg^{-1}) = \varphi(g)\varphi(g^{-1})$ and, by part (1), $\varphi(1_G) = 1_H$, hence $1_H = \varphi(g)\varphi(g^{-1})$. Multiplying both sides on the left by $\varphi(g)^{-1}$ and simplifying gives (2).
(3) This is an easy exercise in induction for $n \in \mathbb{Z}$. By part (2), conclusion (3) holds for negative values of n as well.
(4) Since $1 \in ker\varphi$, the kernel of φ is not empty. Let $x, y \in ker\varphi$, that is $\varphi(x) = \varphi(y) = 1_H$. Then $\varphi(xy^{-1}) = \varphi(x)\varphi(y^{-1}) = \varphi(x)\varphi(y)^{-1} = 1_H 1_H^{-1}$ that is, $xy^{-1} \in ker\varphi$. By the subgroup criterion, $ker\varphi \leq G$.
(5)Since $\varphi(1_G) = 1_H$, the identity of H lies in the image of φ, so $im(\varphi)$ is nonempty. If x and y are in $im(\varphi)$, say $x = \varphi(a), y = \varphi(b)$, then $y^{-1} = \varphi(b^{-1})$ by (2) so that $xy^{-1} = \varphi(a)\varphi(b^{-1}) = \varphi(ab^{-1})$ since φ is a homomorphism. Hence also xy^{-1} is in the image of φ, so $im(\varphi)$ is a subgroup of H by the subgroup criterion □

0.9 Cosets

Definition 0.9.1. For any $N \leq G$ and any $g \in G$ let $gN = \{gn | n \in N\}$ and $Ng = \{ng | n \in N\}$ called respectively a left coset and a right coset of N in G. Any element of a coset is called a representative for the coset.

Definition 0.9.2. Let G and H be groups and Let $\varphi : G \to H$ be a homomorphism with kernel K . The quotient group or factor group, G/K (read G modulo K or simply G mod K) is defined by $G/K = \{gK | g \in G\}$,

Proposition 0.9.3. Let $\varphi : G \to H$ be a homomorphism of groups with kernel K. Let $X \in G/K$ be the fiber above a, i.e., $X = \varphi^{-1}(a)$. Then
(1) For any $u \in X, X = \{uk | k \in K\}$
(2) For any $u \in X, X = \{ku | kEK\}$.

Proof. We prove (1) and leave the proof of (2) as an exercise.
Let $u \in X$ so, by definition of $X, \varphi(u) = a$. Let $uK = \{uk | k \in K\}$. We first prove $uK \subseteq X$. For any $k \in K, \varphi(uk) = \varphi(u)\varphi(k) = \varphi(u)l = a$, (since φ is a homomorphism) (since $k \in ker\varphi$) that is, $uk \in X$. This proves $uK \subseteq X$.
To establish the reverse inclusion suppose $g \in X$ and let $k = u^{-1}g$. Then $\varphi(k) = \varphi(u^{-1})\varphi(g) = \varphi(u)^{-1}\varphi(g) = a^{-1}a = 1$. Thus $k \in ker\varphi$. Since $k = u^{-1}g, g = uk \in uK$, establishing the inclusion $X \subseteq uK$. This proves (1). □

Example 0.9.4. The homomorphism φ from $\mathbb{Z}$ to Z_n, where $n\mathbb{Z}$ is the kernel. $\mathbb{Z}/n\mathbb{Z}$ is the quotient and the elements of the form $a + n\mathbb{Z}$

Proposition 0.9.5. Let N be any subgroup of the group G. The set of left cosets of N in G form a partition of G. Furthermore, for all $u, v \in G, uN = vN$ if and only if $v^{-1}u \in N$ and in particular, $uN = vN$ if and only if u and v are representatives of the same coset.

Proof. First of all note that since N is a subgroup of G, $1 \in N$. Thus $g = g \cdot 1 \in gN$ for all $g \in G$, i.e., $G = \cup_{g \in G}$.
To show that distinct left cosets have empty intersection, suppose $uN \cap vN \neq \emptyset$. We show $uN = vN$. Let $x \in uN \cap vN$.
Write $x = un = vm$, for some $n, m \in N$. In the latter equality multiply both sides on the right by n^{-1} to get $u = vmn^{-1} = vm_1$ where $m_1 = mn^{-1} \in N$. Now for any element ut of $uN(t \in N), ut = (vm_1)t = v(m_1t) \in vN$. This proves $uN \subseteq vN$. By interchanging the roles of u and v one obtains similarly that $vN \subseteq uN$. Thus two cosets with nonempty intersection coincide.
By the first part of the proposition, $uN = vN$ if and only if $u \in vN$ if and only if $u = vn$, for some $n \in N$ if and only if $v^{-1}u \in N$, as claimed.
Finally, $v \in uN$ is equivalent to saying v is a representative for uN, hence $uN = vN$ if and only if u and v are representatives for the same coset (namely the coset $uN = vN$).
□

Definition 0.9.6. The element gng^{-1} is called the conjugate of $n \in N$ by g. The set $gNg^{-1} = \{gng^{-1} | n \in N\}$ is called the conjugate of N by g. The element g is said to normalize N if $gNg^{-1} = N$. A subgroup N of a group G is called *normal* if every element of G normalizes N, i.e., if $gNg^{-1} = N$ for all $g \in G$. If N is a normal subgroup of G we shall write $N \trianglelefteq G$.

Theorem 0.9.7. *Let N be a subgroup of the group G. The following are equivalent:*
(1) $N \trianglelefteq G$
(2) $N_G(N) = G$ (recall $N_G(N)$ is the normalizer in G of N)
(3)$gN = Ng$ for all $g \in G$
(4) $gNg^{-1} \subseteq N$ for allg $\in G$.

Proposition 0.9.8. A subgroup N of the group G is normal if and only if it is the kernel of some homomorphism

Definition 0.9.9. Let $N \trianglelefteq G$. The homomorphism $\pi : G \to G/N$ defined by $\pi(g) = gN$ is called the *natural projection* of G onto G/N. If $\bar{H} \leq G/N$ is a subgroup of G/N, the *complete preimage* of $\bar{H}$ in G is the preimage of $\bar{H}$ under the natural projection homomorphism.

Example 0.9.10. Let G be a group.
(1) The subgroups 1 and G are always normal in $G; G/1 \cong G$ and $G/G \cong 1$.
(2) If G is an abelian group, any subgroup N of G is normal because for all $g \in G$ and all $n \in N, gng^{-1} = gg^{-1}n = n \in N$. Note that it is important that G be abelian, not just that N be abelian.

Problem 0.9.11. Let G be a group and N a normal subgroup of G. Show that for all $g \in G$ and $k \in \mathbb{Z}, (gN)^k = (g^k)N$

Solution. First we show that the conclusion holds for nonnegative k by induction. Note that $(gN)^0 = N = (g^0)N$. Now suppose the conclusion holds for $k \geq 0$; then $(gN)^{k+1} = (gN)(gN)^k = (gN)(g^kN) = (g^{k+1})N$. So the conclusion holds for nonnegative k by induction.

Now suppose $k < 0$. Then $(gN)^k = ((gN)^{-k})^{-1} = (g^{-k}N)^{-1} = (g^k)N$. Thus the conclusion holds for all integers k. □

Problem 0.9.12. Define $\pi : \mathbb{R}^2 \to \mathbb{R}$ by $\pi(x, y) = x + y$. Prove that π is a surjective homomorphism and describe the fibers of π geometrically.

Solution. π is a homomorphism since $\pi((x_1, y_1) + (x_2, y_2)) = \pi((x_1 + x_2, y_1 + y_2)) = x_1 + x_2 + y_1 + y_2 = x_1 + y_1 + x_2 + y_2 = \pi(x_1, y_1) + \pi(x_2, y_2).\pi$ is surjective since for all $c \in \mathbb{R}, \pi(c, 0) = c$. Clearly the fiber of $c \in \mathbb{R}$ is $\{(x, y) \mid x + y = c\}$; that is, the line $x + y = c$ in $\mathbb{R}^2$. □

Problem 0.9.13. Let G be a group. Let H and K are normal subgroups G. Prove that $H \cap N \trianglelefteq G$ is normal.

Problem 0.9.14. Let G be a group, and let $N \trianglelefteq G$ be normal. Prove that if $H \trianglelefteq G$, then $N \cap H \trianglelefteq H$ is normal.

Problem 0.9.15. Let G be a group and let $N \leq G$. Prove that N is normal in G if and only if $gNg^{-1} \subseteq N$ for all $g \in G$.

Solution. Suppose first that N is normal. Then $N_G(N) = G$; thus, for all $g \in G$, we have $gNg^{-1} = N$. In particular, for all $g \in G, gNg^{-1} \subseteq N$. conversely suppose $gNg^{-1} \subseteq N$ for all $g \in G$. Then for all $g \in G$, we have $N = gg^{-1}Ngg^{-1} \subseteq gNg^{-1}$, so that $gNg^{-1} = N$. Hence $N_G(N) = G$. □

Problem 0.9.16. Let G be a group and N a finite subgroup of G. Show that $gNg^{-1} \subseteq N$ if and only if gNg^{-1}. Deduce that $N_G(N) = \{g \in G \mid gNg^{-1} \subseteq N\}$.

Solution. It suffices to show that for all $g \in G, gNg^{-1} \subseteq N$ implies $gNg^{-1} = N$. Let $g \in G$. The mapping $n \mapsto gng^{-1}$ is a bijection $N \to gNg^{-1}$, so that $|gNg^{-1}| = |N|$. Since N is finite, $gNg^{-1} = N$.

The last statement follows trivially. □

Problem 0.9.17. Let G be a group, $g \in G$, and $N \leq G$. Prove that $gN = Ng$ if and only if $g \in N_G(N)$.

Solution. ($\Rightarrow$) Suppose $gN = Ng$. Right multiplying by g^{-1}, we have $gNg^{-1} = Ngg^{-1} = N$, so that $g \in N_G(N)$. ($\Leftarrow$) Suppose $g \in N_G(N)$. Then $gNg^{-1} = N$, and right multiplying by g we have $gN = Ng$. □

Problem 0.9.18. Let G be a group. Prove that if $G/Z(G)$ is cyclic then G is abelian

Solution. Let G be a group and suppose $G/Z(G) = \langle xZ(G)\rangle$ is cyclic.
Note that for all $g \in G$, we have $g \in gZ(G) = x^kZ(G)$ for some integer k. In particular, $g = x^kz$ for some integer k and some $z \in Z(G)$.

Now let $g, h \in G$, where $g = x^az$ and $h = x^bw$ and $z, w \in Z(G)$. We have $gh = x^azx^bw = x^{a+b}zw = x^{b+a}wz = x^bwx^az = hg$. Thus G is abelian. □

Problem 0.9.19. Let G be a group and let $H, K \leq G$ be normal subgroups. Prove that if $H \cap K = 1$ then $hk = kh$ for all $h \in H$ and $k \in K$.

Solution. Lemma: Let G be a group and let $H, K \leq G$ be normal subgroups. Then for all $h \in H$ and $k \in K$ we have $[h, k] \in H \cap K$.
Proof: Note that $h^{-1}k^{-1}h = (h^{-1})k^{-1}(h^{-1})^{-1} \in K$ since K is normal, so that $h^{-1}k^{-1}hk \in K$. Similarly, $h^{-1}k^{-1}hk \in H$.□

Now if $H \cap K = 1$, we have $[h, k] = 1$ for all $h \in H$ and $k \in K$. Thus $h^{-1}k^{-1}hk = 1$, or $hk = kh$. □

0.10 More on Cosets and Lagrange's Theorem

Theorem 0.10.1. *(Lagrange's Theorem)* If G is a finite group and H is a subgroup of G, then the order of H divides the order of G (i.e., $|H| \mid |G|$) and the number of left cosets . $|G|$ of H in G equals $\frac{|G|}{|H|}$.

Definition 0.10.2. If G is a group (possibly infinite) and $H \leq G$, the number of left cosets of H in G is called the *index* of H in G and is denoted by $|G : H|$. In the case of finite groups the index of H in G is $\frac{|G|}{|H|}$. For G an infinite group the quotient $|G|$ does not make sense.

Corollary 0.10.3. If G is a finite group and $x \in G$, then the order of x divides the order of G. In particular $x^{|G|} = 1$ for all x in G.

Corollary 0.10.4. If G is a group of prime order p, then G is cyclic, hence $G \cong \mathbb{Z}_p$.

Definition 0.10.5. Let H and K be subgroups of a group and define $HK = \{hk | h \in H, k \in K\}$.

Proposition 0.10.6. If H and K are finite subgroups of a group then $|HK| = \frac{|H||K|}{|H \cap K|}$.

Proof. Notice that HK is a union of left cosets of K, namely,$HK = \bigcup_{h \in H} hK$.
Since each coset of K has K elements it suffices to find the number of distinct left cosets of the form $hK, h \in H$.
But $h_1K = h_2K$ for $h_1, h_2 \in H$ if and only if $h_2^{-1}h_1 \in K$. Thus
$h_1K = h_2K \Leftrightarrow h_2^{-1}h_1 \in H \cap K \Leftrightarrow h_1(H \cap K) = h_2(H \cap K)$.
Thus the number of distinct cosets of the form hK, for $h \in H$ is the number of distinct cosets $h(H \cap K)$, for $h \in H$. The latter number, by Lagrange's Theorem, equals $\frac{|H|}{|H \cap K|}$.
Thus HK consists of $\frac{|H|}{|H \cap K|}$ distinct cosets of K (each of which has $|K|$ elements) which gives the formula above. □

Problem 0.10.7. Let G be a group and let $H, K \leq G$ be finite subgroups of relatively prime order. Prove that $H \cap K = 1$.

Solution. Let $|H| = p$ and $|K| = q$. We saw in a previous exercise that $H \cap K$ is a subgroup of both H and K; by Lagrange Theorem, then, $|H \cap K|$ divides p and q. Since $\mathsf{gcd}(p, q) = 1$, then, $|H \cap K| = 1$. Thus $H \cap K = 1$. □

Problem 0.10.8. Let G be a group and let $H, K \leq G$ be subgroups of finite index; say $[G : H] = m$ and $[G : K] = n$. Prove that $\mathsf{lcm}(m, n) \leq [G : H \cap K] \leq mn$. Deduce that if m and n are relatively prime, then $[G : H \cap K] = [G : H] \cdot [G : K]$.

Solution. Lemma 1: Let A and B be sets, $\varphi : A \to B$ a map, and Φ an equivalence relation on A. Suppose that if $a_1 \,\Phi\, a_2$ then $\varphi(a_1) = \varphi(a_2)$ for all $a_1, a_2 \in A$. Then $\psi : A/\Phi \to B$ given by $[a]_\Phi \mapsto \varphi(a)$ is a function. Moreover, if φ is surjective, then ψ is surjective, and if $\varphi(a_1) = \varphi(a_2)$ implies $a_1 \,\Phi\, a_2$ for all $a_1, a_2 \in A$, then ψ is injective.
Proof: ψ is clearly well defined. If φ is surjective, then for every $b \in B$ there exists $a \in A$ such that $\varphi(a) = b$. Then $\psi([a]_\Phi) = b$, so that ψ is surjective. If $\psi([a_1]) = \psi([a_2])$, then $\varphi(a_1) = \varphi(a_2)$, so that $a_1 \,\Phi\, a_2$, and we have $[a_1] = [a_2]$.□

First we prove the second inequality.

Lemma 2: Let G be a group and let $H, K \leq G$ be subgroups. Then there exists an injective map $\psi : G/(H \cap K) \to G/H \times G/K$.
Proof: Define $\varphi : G \to G/H \times G/K$ by $\varphi(g) = (gH, gK)$. Now if $g_2^{-1}g_1 \in H \cap K$, then we have $g_2^{-1}g_1 \in H$, so that $g_1H = g_2H$, and $g_2^{-1}g_1 \in K$, so that $g_1K = g_2K$. Thus $\varphi(g_1) = \varphi(g_2)$. Moreover, if $(g_1H, g_2K) = (g_1H, g_2K)$ then we have $g_2^{-1}g_1 \in H \cap K$, so that $g_1(H \cap K) = g_2(H \cap K)$. By Lemma 1, there exists an injective mapping $\psi : G/(H \cap K) \to G/H \times G/K$ given by $\psi(g(H \cap K)) = (gH, gK)$.□

As a consequence, if $[G : H]$ and $[G : K]$ are finite, $[G : H \cap K] \leq [G : H] \cdot [G : K]$.

Now to the first inequality.

Lemma 3: Let G be a group and $K \leq H \leq G$. Let S be a set of coset representatives of G/H. Then the mapping $\psi : S \times H/K \to G/K$ given by $\psi(g, hK) = ghK$ is bijective.
Proof: (Well defined) Suppose $h_2^{-1}h_1 \in K$. Then $h_1K = h_2K$, so that $gh_1K = gh_2K$, and we have $\psi(g, h_1K) = \psi(g, h_2K)$.
(Surjective) Let $gK \in G/K$. Now $g \in \overline{g}H$ for some $\overline{g} \in S$; say $g = \overline{g}h$. Then $\psi(\overline{g}, hK) = gK$, so that ψ is surjective. (Injective) Suppose $\psi(g_1, h_1K) = \psi(g_2, h_2K)$. Then $g_1h_1K = g_2h_2K$; in particular, $g_1h_1 \in g_2h_2K \subseteq g_2H$, so that $g_1 \in g_2H$ and hence $g_2^{-1}g_1 \in H$. So $g_1H = g_2H$, and in fact $g_2 = g_1$. Thus $h_1K = h_2K$, and ψ is injective. □

As a consequence, we have $[G : H] \cdot [H : K] = [G : K]$.

Now in this case we have $H \cap K \leq H \leq G$. Thus m divides $[G : H \cap K]$ and n divides $[G : H \cap K]$, so that $\mathsf{lcm}(m, n)$ divides $[G : H \cap K]$. In particular, since all numbers involved are natural, $\mathsf{lcm}(m, n) \leq [G : H \cap K]$.

Finally, if m and n are relatively prime, then $\mathsf{lcm}(m, n) = mn$, and we have $[G : H \cap K] = mn$. □

Problem 0.10.9. Let G be a group and let $H, N \leq G$ with N normal in G. Prove that if $|H|$ and $[G : N]$ are relatively prime then $H \leq N$.

Solution. First we prove a lemma.
Lemma: Let G be a group, $H \leq G$, and $x \in G$ an element of finite order n. If k is the least positive integer such that $x^k \in H$, then $k|n$.
Proof: If k does not divide n, we have $n = qk + r$ for some $0 < r < k$ by the division algorithm. Now $1 = x^n = x^{qk}x^r \in H$, and $x^{qk} = (x^k)^q \in H$. Thus $x^r \in H$, which contradicts the minimality of k. Thus $k|n$.□

Now to the main result.
Suppose $x \in H$, and let k be the least positive integer such that $x^k \in N$. (k exists since H is finite.) By a previous exercise, as an element of $G/N, |xN| = k$, so that k divides $[G : N]$. Moreover, we have $|x|$ divides $|H|$ by Lagrange, so that (by the lemma) k divides $|x|$ and thus divides $|H|$. Because $|H|$ and $[G : N]$ are relatively prime, then, $k = 1$. But then $|xN| = 1$, so $xN = N$, and we have $x \in N$. So $H \subseteq N$. By a previous exercise $H \leq N$. □

Problem 0.10.10. Let G be a group and $A, B \leq G$ be subgroups such that A is abelian and normal in G. Prove that $A \cap B$ is normal in AB.

Solution. First we prove a lemma.
Lemma: Let G be a group, let $H, K, N \leq G$ be subgroups, and suppose $N \lhd H$. Then $N \cap K \lhd H \cap K$.

Proof: Let $a \in H \cap K$. Then $a(N \cap K) = aN \cap aK = Na \cap Ka = (N \cap K)a$.□

Now $A \cap B \lhd A$ because A is abelian and $A \cap B \lhd B$ by the lemma. Now if $x \in AB, x = ab$ for some $a \in A$ and $b \in B$. Thus $x(A \cap B) = ab(A \cap B) = a(A \cap B)b = (A \cap B)ab = (A \cap B)x$. □

0.11 The Isomorphism Theorems

Theorem 0.11.1. *(The First Isomorphism Theorem)* If $\varphi : G \to H$ is a homomorphism of groups, then $ker\varphi \trianglelefteq G$ and $G/ker\varphi \cong \varphi(G)$.

Corollary 0.11.2. Let $\varphi : G \to H$ be a homomorphism of groups.
(1) φ is injective if and only if $ker\varphi = 1$.
(2) $|G : ker\varphi| = |\varphi(G)|$.

Theorem 0.11.3. *(The Second or Diamond Isomorphism Theorem)* Let G be a group, let A and B be subgroups of G and assume $A \leq N_G(B)$. Then AB is a subgroup of $G, B \trianglelefteq AB, A \cap B \trianglelefteq A$ and $AB/B \cong A/A \cap B$.

Theorem 0.11.4. *(The Third Isomorphism Theorem)* Let G be a group and let H and K be normal subgroups of G with $H \leq K$. Then $K/H \trianglelefteq G/H$ and $(G/H)/(K/H) \cong G/K$. If we denote the quotient by H with a bar, this can be written $\bar{G}/\bar{K} \cong G/K$.

Problem 0.11.5. Let G be a group, $N \leq G$ a normal subgroup of prime index p, and $K \leq G$ a subgroup. Prove that either $K \leq N$ or $G = NK$ and $[K : K \cap N] = p$.

Solution. Suppose $K \setminus N \neq \emptyset$; say $k \in K \setminus N$. Now $G/N \cong \mathbb{Z}/(p)$ is cyclic, and moreover is generated by any nonidentity- in particular by $\overline{k}$.

Now $KN \leq G$ since N is normal. Let $g \in G$. We have $gN = k^a N$ for some integer a. In particular, $g = k^a n$ for some $n \in N$, hence $g \in KN$. We have $[K : K \cap N] = p$ by the Second Isomorphism Theorem. □

Problem 0.11.6. Let p be a prime and let G be a finite group of order $p^a m$, where p does not divide m. Let $P \leq G$ be a subgroup of order p^a and $N \leq G$ a normal subgroup of order $p^b n$ where p does not divide n. Prove that $|P \cap N| = p^b$ and that $|PN/N| = p^{a-b}$.

Solution. By the Second Isomorphism Theorem, we have $PN \leq G, N \leq PN$ normal, $P \cap N \leq P$ normal, and $P/(P \cap N) \cong PN/N$. Now $|PN|$ divides $|G|$ by Lagrange, so that $|PN| = p^k \ell$ for some k where p does not divide ℓ; then $\ell | m$. Because $P \leq PN$, we have $k = a$, and because $N \leq PN, n | \ell$. Thus $|PN/N| = p^{a-b}q$, where p does not divide q. Note that $|P/(P \cap N)| = p^k$ for some k, and we have $p^k = p^{a-b}q$. Thus $q = 1$ and we have $|PN/N| = p^{a-b}$. Finally, we have $|P|/|P \cap N| = p^a/p^b$, so that $|P \cap N| = p^b$. □