

Math 121 - Fundamentals of Algebra

Evangeline P. Bautista

2008

Chapter 1

Introduction

1.1 Integers

We will use \mathbb{N} to denote the set of positive integers and \mathbb{Z} to denote the set of integers. The properties of \mathbb{Z} that will be of major concern to us are given in this section.

The Well Ordering Principle. Any nonempty set of non-negative integers has a smallest element.

Remarks 1.1 The Well Ordering Principle, in effect, states that given any set A of nonnegative integers, there is an $n_0 \in A$ such that $n_0 \leq n$ for all $n \in A$.

Theorem 1.1 (Euclid's Algorithm) If m and n are integers with $n > 0$, then there exist integers q and r with $0 \leq r < n$, such that

$$m = qn + r.$$

Proof: Let

$$W = \{m - tn \mid t \in \mathbb{Z}\}.$$

Now, let

$$W^* = \{v \in W \mid v > 0\}.$$

Observe that W^* is not empty since we can always select t to be a negative number large enough so that $m - tn > 0$. Now, by the Well Ordering

Principle, W^* has a smallest element which we shall call r . That is, $r > 0$ and there is a q such that

$$r = m - qn.$$

If $r \geq n$, then $r - n \geq 0$ and

$$r - n = m - qn - n = m - (q + 1)n \geq 0$$

thereby contradicting our assumption that r is the smallest element of W^* . Thus, $0 < r < n$ and the theorem is proven. \square

Definition 1.1 Given integers $m \neq 0$ and n , we say that m **divides** n , written as $m|n$ if $n = cm$ for some integer c .

Theorem 1.2 The following are true for all integers m, n and q .

1. $1|n$ for all n .
2. If $m|n$ and $n|q$ then $m|q$.
3. If $m|n$ and $m|q$ then $m|an + bq$ for all integers a and b .
4. If $m|1$ then $m = 1$ or $m = -1$.
5. If $m|n$ and $n|m$ then $m = \pm n$.

Proof: Easy

Definition 1.2 Given a, b not both 0, the **greatest common divisor** of a and b , denoted as (a, b) is the number c where

1. $c > 0$;
2. $c|a$ and $c|b$; and
3. If $d|a$ and $d|b$ then $d|c$.

Theorem 1.3 If a, b are not both 0, then their greatest common divisor c is unique, and moreover,

$$c = ma + nb$$

for some suitable m and n .

Proof: Let

$$A = \{sa + tb \mid s, t \in \mathbb{Z}\}$$

If $z \in A$, then there exist integers x and y such that

$$z = xa + yb$$

thus,

$$-z = (-x)a + (-y)b$$

implying that $-z \in A$. Thus, A must contain positive elements.

By the Well Ordering Principle, then, A contains a least positive element, say $c = ma + nb$ for some integers m and n . We claim that c is the greatest common divisor of a and b .

Applying Euclid's algorithm on a and c , we know that there exists q and r , where $0 \leq r < c$ such that

$$\begin{aligned} a &= qc + r \\ a &= q(ma + nb) + r \\ (1 - qm)a + (-n)b &= r \end{aligned}$$

so $r \in A$. But $0 \leq r < c$ and c is the minimal positive element of A which implies that $r = 0$. Thus, c must divide a . In a similar manner, c divides b showing that it is a common divisor of a and b . We have already shown that $c > 0$ and that $c|a$ and $c|b$. Now, if $d|a$ and $d|b$, then by Theorem 1.2 $d|ma + nb = c$ and we are done showing that $c = (a, b)$.

To show uniqueness, we let t satisfy the three properties of the definition of the greatest common divisor. Then $t|c$ and $c|t$ showing that $t = c$. \square

Definition 1.3 The integers a and b are **relatively prime** if and only if $(a, b) = 1$.

Corollary 1.1 The integers a and b are relatively prime if and only if $1 = ma + nb$ for suitable integers m and n .

Theorem 1.4 If a and b are relatively prime and $a|bc$ then $a|c$.

Proof: By the previous corollary, there exist integers m and n such that

$$ma + nb = 1.$$

Hence,

$$\begin{aligned}(ma + nb)c &= c \\ mac + nbc &= c\end{aligned}$$

Now we know that $a|mac$ and that $a|bc$. Thus, a divides $mac + nbc = c$ and we are done. \square

Corollary 1.2 If b and c are both relatively prime to a , then bc is also relatively prime to a .

Proof: As in the previous theorem, we have

$$mac + nbc = c.$$

Now, if $d = (a, bc)$, then $d|c$. But d also divides a and a and c are relatively prime so we must have $1 = d = (a, bc)$. \square

Definition 1.4 A **prime number** is an integer $p > 1$ such that for any integer a , either $p|a$ or $(p, a) = 1$.

Theorem 1.5 If p is a prime and $p|a_1a_2 \cdots a_n$ then $p|a_i$ for some i with $1 \leq i \leq n$.

Proof: If $p|a_1$ then we are done. If $p \nmid a_1$, then by definition of a prime number, $(p, a_1) = 1$ and by Theorem 1.4, $p|a_2a_3 \cdots a_n$. We can then repeat the process. That is, if $p|a_2$ then we are done, else $p|a_3a_4 \cdots a_n$. Continue the process until we find an a_i divisible by p and we know that this is going to exist by Theorem 1.4. \square

Theorem 1.6 If n is an integer greater than 1, then either n is a prime or n is a product of primes.

Proof: Suppose the theorem is false. Then, there is a set of positive integers S which are neither primes nor product of primes. Thus, by the Well Ordering Principle, this set must have a least positive element, say, a . Since a is not a prime, then there must exist two positive integers b and c less than a and greater than 1 such that $a = bc$. Now, since b and c are less than a , $b, c \notin S$. Thus, either b and c are primes or they are products of primes. This implies that a must be a product of primes contradicting our initial assumption. \square

Theorem 1.7 Given $n > 1$, then there is one and only one way of writing n in the form

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$$

where $p_1 < p_2 < \cdots < p_k$ are primes and the exponents a_1, a_2, \cdots, a_k are all positive.

Proof: Suppose there is a set of positive numbers not satisfying the theorem. Then, there is a number $m > 1$ such that m has two distinct factorizations:

$$m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} = q_1^{b_1} q_2^{b_2} \cdots q_l^{b_l}$$

where $p_1 < p_2 < \cdots < p_k$ and $q_1 < q_2 < \cdots < q_l$ are primes and a_1, a_2, \cdots, a_l and b_1, b_2, \cdots, b_l are all positive.

Since

$$p_1 | p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} = q_1^{b_1} q_2^{b_2} \cdots q_l^{b_l}$$

it follows that p_1 divides q_i for some i . But since p_1 and q_i are primes, then $p_1 = q_i$. Similarly, we must have $q_1 = p_j$ for some j . But,

$$p_1 \leq p_j = q_1 \leq q_i$$

implying that $p_1 = q_1$.

Now, since $m/p_1 < m$, then

$$m/p_1 = p_1^{a_1-1} p_2^{a_2} \cdots p_k^{a_k}$$

has the unique factorization property. And since m/p_1 can only be factored in one way, then

$$m/p_1 = p_1^{a_1-1} p_2^{a_2} \cdots p_k^{a_k} = p_1^{b_1-1} q_2^{b_2} \cdots q_l^{b_l}$$

implies easily that $k = l$, $p_i = q_i$ and $a_i = b_i$ thus showing that the factorization of m is also unique. \square

Theorem 1.8 The number of primes is infinite.

Proof: Suppose the number of primes is finite. Then, we can list all the primes as $p_1, p_2 \cdots p_n$ for some number n . Consider the number

$$P = p_1 p_2 \cdots p_n + 1.$$

Since $P > p_i$ for all i , then by our assumption, P is not a prime. It is then a product of primes. But P is not divisible by any of our primes. Thus, we have a contradiction. \square

1.2 Mappings

Definition 1.5 Let S and T be sets. A **function** or a **mapping** f from S to T , denoted by $f : S \rightarrow T$ is a rule that assigns to each element $s \in S$ a unique element $t \in T$. In this case, we say that t is the **image** of s under the function f or that s is the **pre-image** of t and we write $f(s) = t$.

Remarks 1.2 Observe that in our definition, the sets S and T are not necessarily subsets of \mathbb{R} . Thus, in defining a function, it is necessary to define S and T .

Definition 1.6 The mapping $f : S \rightarrow T$ is **onto** or **surjective** if every $t \in T$ is the image of some $s \in S$ under f . That is, given $t \in T$, there exists $s \in S$ such that $f(s) = t$.

Definition 1.7 The mapping $f : S \rightarrow T$ is **one to one** or **injective** if for $s_1 \neq s_2$ in S , $f(s_1) \neq f(s_2)$ in T . Equivalently, $f(s_1) = f(s_2)$ implies that $s_1 = s_2$.

Definition 1.8 The mapping $f : S \rightarrow T$ is a **bijection** if it is both one to one and onto.

Definition 1.9 If $g : S \rightarrow T$ and $f : T \rightarrow U$ are given mappings, then the **composition** or **product** of f g and f is the mapping $f \circ g : S \rightarrow U$ defined by $(f \circ g)(s) = f(g(s))$ for every $s \in S$.

Theorem 1.9 If $h : S \rightarrow T$, $g : T \rightarrow U$, and $f : U \rightarrow V$, then $f \circ (g \circ h) = (f \circ g) \circ h$.

Proof: To show that two mappings are equal, we must check that the images of each element under both mappings are equal. In our case, we must then show that for every $s \in S$, $f \circ (g \circ h)(s) = (f \circ g) \circ h(s)$.

By definition of composition, we have

$$(f \circ (g \circ h))(s) = f((g \circ h)(s)) = f(g(h(s)))$$

and

$$((f \circ g) \circ h)(s) = (f \circ g)(h(s)) = f(g(h(s))).$$

Since this is true for all $s \in S$, conclusion follows. \square

Theorem 1.10 If $g : S \rightarrow T$ and $f : T \rightarrow U$ are both one to one, then $f \circ g : S \rightarrow U$ is also one to one.

Proof: Suppose $f \circ g(s_1) = f \circ g(s_2)$. Then we have $f(g(s_1)) = f(g(s_2))$. But f is one to one so it follows that $g(s_1) = g(s_2)$. Likewise, g is one to one so $s_1 = s_2$ and we are done. \square

Theorem 1.11 If $g : S \rightarrow T$ and $f : T \rightarrow U$ are both onto, then $f \circ g : S \rightarrow U$ is also onto.

Proof: Let $u \in U$. Since f is onto, there exists $t \in T$ such that $f(t) = u$. Also, since g is onto, there is an $s \in S$ such that $g(s) = t$. Thus, for all $u \in U$, there is an $s \in S$ such that

$$f \circ g(s) = f(g(s)) = f(t) = u.$$

\square

Corollary 1.3 If $g : S \rightarrow T$ and $f : T \rightarrow U$ are bijections, then $f \circ g : S \rightarrow U$ is also a bijection.

Remarks 1.3 If $f : S \rightarrow T$ is a bijection, then there is a mapping $f^{-1} : T \rightarrow S$ called the inverse of f such that

$$f \circ f^{-1} = i_T$$

and

$$f^{-1} \circ f = i_S$$

where i_T and i_S are the identity mappings defined on T and S respectively. That is, $i_T : T \rightarrow T$ where $i_T(t) = t$ for all $t \in T$. i_S is similarly defined.

Theorem 1.12 If $f : S \longrightarrow T$ and i_S and i_T are the identity maps defined in the preceding remark, then

$$i_T \circ f = f \circ i_S = f.$$

Proof: Easy.

Chapter 2

Groups and Subgroups

2.1 Groups

Definition 2.1 Given a set S , a **binary operation** $*$ on S is a mapping $S \times S \rightarrow S$. If $a, b \in S$, we usually write $*(a, b)$ as $a * b$ or, if there is no problem of ambiguity, simply as ab .

Example 2.1

1. Addition is a binary operation on the set of real numbers, the set of integers, the set of complex numbers and the set of positive numbers.
2. Subtraction is a binary operation on \mathbb{Z} but it is not a binary operation on \mathbb{N} .
3. Division is not a binary operation on \mathbb{R} since we cannot divide by 0 but it is a binary operation on $\mathbb{R} \setminus \{0\}$.
4. If M is the set of all matrices with real entries, then addition of matrices is not a binary operation on M since not all matrices may be added.

Remarks 2.1 Let $*$ be a binary operation on a set S and let $H \subseteq S$. The subset H is said to be closed under $*$ if $*$ is also a binary operation on H . That is, $a * b \in H$ whenever $a, b \in H$. In this case, we say that the binary operation on H is the **induced operation** of $*$ on H .

Definition 2.2 Given a binary definition $*$ defined on a set S , we say that $*$ is **commutative** if $a * b = b * a$ for every $a, b \in S$.

Definition 2.3 Given a binary definition $*$ defined on a set S , we say that $*$ is **associative** if $(a * b) * c = a * (b * c)$ for every $a, b, c \in S$.

Definition 2.4 A group $\langle G, * \rangle$ is a set G together with a binary operation defined on G such that

i $*$ is associative. That is

$$a * (b * c) = (a * b) * c$$

for all $a, b, c \in G$.

ii There exists $e \in G$ such that

$$a * e = e * a = a$$

for all $a \in G$. e is called the identity of the group.

iii For all $a \in G$, there exists $a^{-1} \in G$ such that

$$a * a^{-1} = a^{-1} * a = e.$$

We may also say that G is a group under the operation $*$.

If, in addition to the three properties above, the group has the property

iv $ab = ba$ for all $a, b \in G$.

the group is said to be Abelian.

Example 2.2 The set of integers \mathbb{Z} under addition is a group. The identity of the group is 0 and the inverse of each $n \in \mathbb{Z}$ is $-n$. The set of real numbers \mathbb{R} and the set of rational numbers \mathbb{Q} are also groups under addition.

Example 2.3 The set \mathbb{R}^* of real numbers without 0 and the set \mathbb{Q}^* of real numbers without 0 are groups under multiplication. The identity is 1 and the inverse of any real (rational) number x in the set is $1/x$.

Example 2.4 The set $\mathbb{Z}_n = \{0, 1, 2, \dots, n\}$ under addition modulo n is a group. The identity is 0 and the inverse of $m \in \mathbb{Z}_n$ is $-m = n - m \pmod{n}$.

Example 2.5 The set of all non-singular 2×2 matrices under multiplication is a group, the identity being the identity matrix and the inverse is just the usual matrix inverse.

Example 2.6 If n is a positive integer, the set $U(n)$ = the set of all positive integers less than n and relatively prime to n is a group under multiplication modulo n .

Theorem 2.1 The identity e of a group G is unique.

Proof: Suppose G has two identities e and e' . Then we know that for all $a \in G$,

$$a = ae = ea$$

and

$$a = ae' = e'a.$$

If we replace a by e' in the first statement and a by e in the second statement, we get

$$e' = e'e = ee' = e$$

showing that $e = e'$. □

Theorem 2.2 In a group G , $ab = ac$ implies that $b = c$ and $ba = ca$ also implies that $b = c$.

Proof: We prove the first statement:

$$\begin{aligned} ab &= ac \\ a^{-1}(ab) &= a^{-1}(ac) \\ (a^{-1}a)b &= (a^{-1}a)c \\ eb &= ec \\ b &= c \end{aligned}$$

□

Theorem 2.3 The inverse of a group G is unique.

Proof: Given $a \in G$, we suppose that a has two inverses: a' and a'' . Then, by definition of the inverse, we have

$$a'a = e \text{ and } a''a = e$$

implying that

$$a'a = a''a.$$

By the cancelation property, we then have

$$a' = a''$$

showing that the inverse is unique. □.

Theorem 2.4 If a and b are elements of a group G , then

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

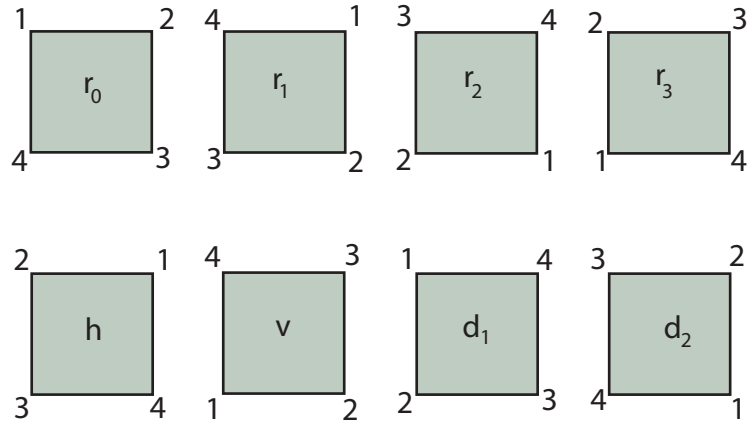
Proof: Since we have already proven that the inverse is unique, showing that an element is the inverse of a given element simply means showing that the product of the two elements is the identity. That is, to show that $(ab)^{-1} = b^{-1}a^{-1}$, we need only show that

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

This is easily done as follows:

$$\begin{aligned} (ab)(b^{-1}a^{-1}) &= a(bb^{-1})a^{-1} \\ &= aea^{-1} \\ &= aa^{-1} \\ &= e \end{aligned}$$

Example 2.7 (The Dihedral Group of Order 8) Consider the symmetries of a square as shown in the figure below:



If we consider each symmetry as a motion and define the product of the motion AB as the motion A followed by motion B , we may then construct the following multiplication table:

	r_0	r_1	r_2	r_3	h	v	d_1	d_2
r_0	r_0	r_1	r_2	r_3	h	v	d_1	d_2
r_1	r_1	r_2	r_3	r_0	d_1	d_2	v	h
r_2	r_2	r_3	r_0	r_1	v	h	d_2	d_1
r_3	r_3	r_0	r_1	r_2	d_2	d_1	h	v
h	h	d_2	v	d_1	r_0	r_2	r_3	r_1
v	v	d_1	h	d_2	r_2	r_0	r_1	r_3
d_1	d_1	h	d_2	v	r_1	r_3	r_0	r_2
d_2	d_2	v	d_1	h	r_3	r_1	r_2	r_0

The multiplication shows that the operation is actually a binary operation whose identity is r_0 . It is easy enough to check that the operation is associative and that we actually have a group which is not abelian. This group is known as the dihedral group of order 8 and is denoted by D_4 .

Remarks 2.2 The multiplication table of a group is a Latin Square. That is, each element of the group must occur in each column and each row exactly once. This can help us in constructing groups. For example, if we are to construct a group of order 4, we can always work with a group table and assign the first element as the identity. It is not too difficult to show that we

can only construct two groups of order 4 and that the two groups have the following multiplication tables:

	e	a	b	c		e	a	b	c
e	e	a	b	c	e	e	a	b	c
a	a	b	c	e	a	a	e	c	b
b	b	c	e	a	b	b	c	e	a
c	c	e	a	b	c	c	b	a	e

The group table on the left is actually the same group table for \mathbb{Z}_4 while the group table on the right is a group known as the Klein 3 group.

Exercise 2.1

1. Prove that a group G is abelian if and only if $(ab)^{-1} = a^{-1}b^{-1}$.
2. Prove that if $(ab)^2 = a^2b^2$ is a group G , then $ab = ba$.
3. Let G be a group and let $g \in G$. Define the function $\phi_g : G \rightarrow G$ by $\phi_g(x) = g^{-1}xg$ for all $x \in G$. Show that ϕ_g is one to one and onto.
4. Prove that if G is a group with the property that the square of every element is the identity, then G is abelian.

2.2 Subgroups

Definition 2.5 The **order** of a group G , denoted by $|G|$ is the number of elements of G .

Definition 2.6 The **order** of an element g in a group G is the smallest positive number n such that $g^n = e$. (Note: in additive notation, we write $ng = 0$.) If no such integer exists, we say that g is of infinite order. The order of $g \in G$ is denoted by $|g|$.

Example 2.8

1. The group \mathbb{Z}_8 has order 8. The orders of its elements are as follows: $|0| = 1$, $|1| = 8$, $|2| = 4$, $|3| = 8$, $|4| = 2$, $|5| = 8$, $|6| = 4$, $|7| = 8$.

2. The group D_4 also has order 8. The orders of its elements are: $|r_0| = 1$, $|r_1| = 4$, $|r_2| = 2$, $|r_3| = 4$, $|h| = |v| = |d_1| = |d_2| = 2$.
3. In \mathbb{Z} , every element except 0 has infinite order.

Exercise 2.2

1. Prove that in a group G , an element and its inverse have the same order.
2. Let x be an element of a group G . If $x^2 \neq e$ while $x^6 = e$, prove that $x^4 \neq e$ and that $x^5 \neq e$. What can you say about the order of e ?
3. Find a group that contains elements a and b such that $|a| = |b| = 2$ while
 - (a) $|ab| = 3$
 - (b) $|ab| = 4$
 - (c) $|ab| = 5$
4. Suppose that a group contains elements a and b such that $|a| = 4$, $|b| = 2$, and $a^3b = ba$. Find ab .

Definition 2.7 If a nonempty subset H of a group G is itself a group under the operation of G , we say that H is a **subgroup** of G and write $H \leq G$.

Example 2.9

1. The set H of all even numbers is a subgroup of \mathbb{Z} .
2. In Z_8 , one can easily check that the set $\{0, 2, 4, 6\}$ is a subgroup.
3. The set $\{r_0, h\}$ is a subgroup of D_4 .

Theorem 2.5 (One-Step Subgroup Test) Let G be a group and H a nonempty subset of G . Then, H is a subgroup of G if $ab^{-1} \in H$ whenever a and b are in H .

Proof: Since the operation of H is the same as that of G , associativity follows immediately. Thus, we only need to show that 1) $e \in H$, 2) the inverse of each element of H is also in H and 3) that G is closed under the operation of G .

To show that e is in H , we choose any $a \in H$. By our hypothesis, aa^{-1} is also in H . But, $aa^{-1} = e$, thus, $e \in H$.

Now, we show that $a^{-1} \in H$ whenever $a \in H$. Since we have already shown that $e \in H$, then, if $a \in H$, it again follows from our hypothesis that $ea^{-1} = a^{-1}$ is in H .

Finally, consider $a, b \in H$. Since we have already shown that the inverse of every element in H is also in H , then $a, b^{-1} \in H$. Thus, $a(b^{-1})^{-1} = ab \in H$ and we are done. \square

Example 2.10 Let G be an abelian group. Define

$$H = \{x \in G \mid x^2 = e\}.$$

Show that $H \leq G$.

Since $e^2 = e$, we know that $e \in H$ so H is not empty. Now, we let $a, b \in H$. We have

$$\begin{aligned} (ab^{-1})^2 &= ab^{-1}ab^{-1} \\ &= a^2(b^{-1})^{-1} \text{ since } G \text{ is abelian} \\ &= ee^{-1} \\ &= e \end{aligned}$$

Thus, $(ab^{-1})^2 = e$ implying that $(ab^{-1})^2 \in H$. Therefore, by the one-step subgroup test, $H \leq G$.

Theorem 2.6 (Two-Step Subgroup Test) Let G be a group and H a nonempty subset of G . Then H is a subgroup of G if $ab \in H$ whenever $a, b \in H$, and $a^{-1} \in H$ whenever $a \in H$. (That is H is a subgroup of G if H is closed under the operation of G and every element of H has its inverse in H .)

Proof: Suppose $a, b \in H$, then, $a, b^{-1} \in H$. Thus, $ab^{-1} \in H$ whenever a and b are in H and by Theorem 2.5, it follows that $H \leq G$. \square

Theorem 2.7 (Finite Subgroup Test) Let H be a nonempty finite subset of a group G . Then, H is a subgroup of G if G is closed under the operation of G .

Proof: Using Theorem 2.6, we need only prove that $a^{-1} \in H$ whenever $a \in H$. We then let $a \in H$. If $a = e$, then $a^{-1} = e \in H$. If $a \neq e$, then by the closure property, $a^n \in H$ for every positive integer n . Now, since H is finite, not all the powers of a are distinct. That is, there exists integers i and j with $i > j$ such that

$$a^i = a^j.$$

It then follows that

$$a^{i-j} = e$$

with $i - j > 1$ since $a \neq e$. Thus,

$$aa^{i-j-1} = e$$

where $i - j - 1 > 0$. This tells us that

$$a^{-1} = a^{i-j-1} \in H$$

and we are done. □

Exercise 2.3

1. Let G be a group and let $a \in G$. Show that

$$\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$$

is a subgroup of G . This group is known as the cyclic subgroup of G generated by a .

2. Let G be a group and let $a \in G$. Show that the group

$$C(a) = \{g \in G \mid ag = ga\}$$

is a subgroup of G . This subgroup is known as the centralizer of a in G .

3. Let G be a group and let

$$Z(G) = \{g \in G \mid gh = hg \text{ for all } h \in G\}.$$

Show that $Z(G)$ is a subgroup of G . This subgroup is known as the center of G .

4. If H and K are subgroups of a group G , show that $H \cap K \leq G$.
5. Suppose that G is a group that has exactly 8 elements of order 3, how many subgroups of order 3 does G have?
6. Let $a \in G$, G a group, and $|a| = 5$. Prove that $C(a) = C(a^3)$. Find an element a from some group such that $|a| = 6$ and $C(a) \neq C(a^3)$.

Bibliography

- [1] Fraleigh, D. Hill *A First Course in Abstract Algebra, 6th ed.* Pearson Education Asia, Singapore, 2002.
- [2] Herstein, I.N. *Abstract Algebra, 3rd ed.* Prentice Hall, USA 1996.
- [3] Dummit, D.M., R.S. Foote *Abstract Algebra* John Wiley and Sons, New York, 1999.
- [4] Hungerford, T.W. *Algebra* Springer Verlag, New York, 1974.