Abstract Algebra Notes

Mario L. Gutierrez Abed

Groups & Subgroups

Definition: A group $\langle G, \ *\rangle$ is a set G, closed under a binary operation $*$, such that the following axioms are satisfied:

- $\mathcal{G}_1$: For all $a, \ b, \ c \in G$, we have
$$(a * b) * c = a * (b * c) \quad \text{(associativity of } *)$$

- $\mathcal{G}_2$: There is an element $e \in G$ such that for all $x \in G$,
$$e * x = x * e = x \quad \text{(identity element } e \text{ for } *)$$

- $\mathcal{G}_3$: Corresponding to each $a \in G$, there is an element $a' \in G$ such that
$$a * a' = a' * a = e \quad \text{(inverse } a' \text{ of } a) \ .$$

Binary algebraic structures with weaker axioms than those of a group have also been studied extensively. Of these weaker structures, the semigroup has perhaps had the most attention.

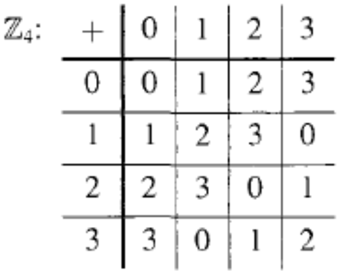
Definition: A semigroup is a set with an associative binary operation. A monoid is a semigroup that has an identity element for the binary operation. Obviously, it follows that every group is both a semigroup and a monoid.

• Theorem:
A subset H of a group G is a subgroup of G iff:
i) H is closed under the binary operation of G,
ii) the identity element e of G is in H,
iii) for all $a \in H$, it is true that $a^{-1} \in H$ also.

Definition: The elements of the set $U_n = \{z \in \mathbb{C} : z^n = 1\}$ are called the n^{th}roots of unity.

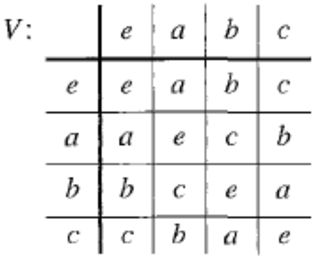
Definition: A partition of a set S is a collection of nonempty subsets of S such that every element of S is in exactly one of the subsets. The subsets are the cells of the partition.

Note: There are two different types of group structures of order 4 (see exercise 20 of section 1.4 on Fraleigh's). We describe them by their group tables (see below):



$\mathbb{Z}_4$:

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



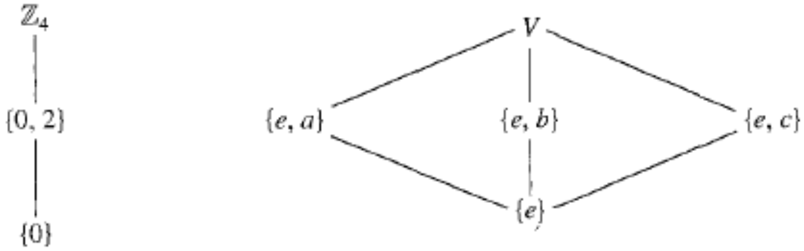
V:

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

The group V is called the Klein-4 group -the notation V comes from the German word *Vier* (four)-. Note that this group has the property $a^2 = b^2 = c^2 = e$. The Klein-4 group is isomorphic to the group $\mathbb{Z}_2 \times \mathbb{Z}_2$, the direct product of two copies of the cyclic group $\mathbb{Z}_2$ of order 2. It is in fact the smallest non-cyclic group and it is also abelian. In addition, the Klein-4 group is isomorphic to D_4(the dihedral group of order 4) and it's also isomorphic to the direct sum $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.

The group $\mathbb{Z}_4$ is isomorphic to the group $U_4 = \{1, i, -1, -i\}$ of fourth roots of unity under multiplication. The only nontrivial proper subgroup of $\mathbb{Z}_4$ is $\{0, 2\}$. Note that $\{0, 3\}$ is not a subgroup of $\mathbb{Z}_4$, since $\{0, 3\}$ is not closed under $+_4$. For example, $3 +_4 3 = 2$, and $2 \notin \{0, 3\}$. However, the group V has three non-trivial proper subgroups, namely $\{e, a\}$, $\{e, b\}$, and $\{e, c\}$. Here $\{e, a, b\}$ is not a subgroup, since $\{e, a, b\}$ is not closed under the operation of V because $a\,b = c$, and $c \notin \{e, a, b\}$.

It is often useful to draw a subgroup diagram of the subgroups of a group. In such a diagram, a line running downward from a group G to a group H means that H is a subgroup of G. Thus the larger group is placed nearer the top of the diagram. The figure below contains the subgroup diagrams for the groups $\mathbb{Z}_4$ and V:



(a) (b)

CYCLIC GROUPS

- Theorem:

Let G be a group and let $a \in G$. Then,

$$H = \{a^n : n \in \mathbb{Z}\}$$

is a subgroup of G and it's in fact the smallest subgroup of G that contains a, i.e. every subgroup containing a contains H.

Definition: Let G be a group and let $a \in G$. Then the subgroup $\{a^n : n \in \mathbb{Z}\}$ of G is called the cyclic subgroup of G generated by a, denoted by $\langle a \rangle$.

Definition: Let G be a group. An element $a \in G$ generates G –and thus is said to be a generator for G– if $\langle a \rangle = G$. A group G is cyclic if there is such element a that generates G.

Example:

▸ Take the groups $\mathbb{Z}_4 = \{0,\ 1,\ 2,\ 3\}$ and $V = \{a,\ b,\ ab,\ e\}$ (the Klein-4 group). Then $\mathbb{Z}_4$ is cyclic and both 1 and 3 are generators, i.e. $\langle 1 \rangle = \langle 3 \rangle = \mathbb{Z}_4$.
However, V is not cyclic. Notice that $\langle a \rangle$, $\langle b \rangle$, and $\langle ab \rangle$ are proper subgroups of two elements, and $\langle e \rangle$ is the trivial subgroup of 1 element. Since no single element generates all of V, we conclude that this is a noncyclic group.

▸ The group $\mathbb{Z}$ under addition is a cyclic group. Both 1 and -1 are generators for this group, and they are the only generators (in fact, since every infinite cyclic group is isomorphic to $\mathbb{Z}$ (we prove this later on), they must all have exactly two generators!).
Also for $n \in \mathbb{Z}^+$, the group $\mathbb{Z}_n$ under addition modulo n is cyclic. If $n > 1$, then both 1 and $n-1$ are generators, but there may be others.

• Theorem:
Every cyclic group is abelian.

Proof:
Let G be a cyclic group and let a be a generator for G so that $G = \langle a \rangle = \{a^n : n \in \mathbb{Z}\}$. If g_1 and g_2 are any two elements of G, there exist integers r and s such that $g_1 = a^r$ and $g_2 = a^s$.
Then,

$$g_1 g_2 = a^r a^s = a^{r+s} = a^{s+r} = a^s a^r = g_2 g_1.$$

Thus we have proven that G is abelian. ■

• Division Algorithm for $\mathbb{Z}$:
If m is a positive integer and n is any integer, then there exist unique $q,\ r \in \mathbb{Z}$ such that $n = mq + r$ and $0 \le r < m$.

Example:

▸ Using the division algorithm, let us find the quotient q and remainder r when 38 is divided by 7. The positive multiples of 7 are 7, 14, 21, 28, 35, 42, … . Choosing the multiple to leave a nonnegative remainder less than 7, we write

$$38 = 35 + 3 = 7\,(5) + 3.$$

Thus the quotient is $q = 5$ and the remainder is $r = 3$.

▸ Using the division algorithm, let us find the quotient q and remainder r when -38 is divided by 7. The negative multiples of 7 are -7, -14, -21, -28, -35, -42, … . Choosing the multiple to leave a nonnegative remainder less than 7, we write

$$-38 = -42 + 4 = 7\,(-6) + 4.$$

Thus the quotient is $q = -6$ and the remainder is $r = 4$. ✡

• Theorem:
A subgroup of a cyclic group is cyclic.

Proof:
(See page 61, Fraleigh's) ■

• Corollary:
The subgroups of $\mathbb{Z}$ under addition are precisely the groups $n\,\mathbb{Z}$ under addition for $n \in \mathbb{Z}$.

This corollary gives us an elegant way to define the greatest common divisor (gcd) of two positive integers r and s:

Definition: Let r and s be two fixed positive integers. The positive generator d of the cyclic group $H = \{nr + ms : n,\ m \in \mathbb{Z}\}$ under addition is the greatest common divisor (gcd) of r and s. We write $d = \gcd(r,\ s)$.

Note from the definition that d is a divisor of both r and s since both $r = 1\,r + 0\,s$ and $s = 0\,r + 1\,s$ are in H. Hence since $d \in H$, we can write

$$d = nr + ms \qquad \text{(for some } n,\ m \in \mathbb{Z}\text{)}.$$

We see that every integer dividing both r and s divides the right hand side of the equation, and hence must be a divisor of d also. Thus d must be the largest number dividing both r and s (hence the name greatest common divisor).

Example:
Find the gcd of 42 and 72.

Solution:
The positive divisors of 42 are

$$1,\ 2,\ 3,\ 6,\ 7,\ 14,\ 21, \text{ and } 42.$$

The positive divisors of 72 are

$$1,\ 2,\ 3,\ 4,\ 6,\ 8,\ 9,\ 12,\ 18,\ 24,\ 36, \text{ and } 72.$$

The greatest common divisor is 6.

Remark: Note that in the previous example we have that $6 = (3)\,72 + (-5)\,42$. There is an algorithm for expressing the greatest common divisor $d = \gcd(r,\ s)$ in the form $d = nr + ms$ (see Exercise set 1, problem #2).

Definition: Two positive integers are relatively prime if their gcd is 1. If r and s are relatively prime and if r divides sm, then r must divide m.
For example, 12 and 25 are relatively prime. Note that they have no prime factors in common.

- Theorem:

Let G be a cyclic group with generator a. Then,
(i) If the order of G is infinite, then G is isomorphic to $\langle \mathbb{Z},\ +\rangle$.
(ii) If G has finite order, then G is isomorphic to $\langle \mathbb{Z}_n,\ +_n\rangle$.

Proof:
▸ First we prove (i), in which case for all positive integers m, we have $a^m \neq e$. We claim that no two distinct exponents h and k can give equal elements a^h and a^k of G.
Suppose that $a^h = a^k$ and say $h > k$. Then

$$a^h\, a^{-k} = a^{h-k} = e$$

contrary to our assumption that $a^m \neq e$ for all positive integers m. Hence every element of G can be expressed as a^m for a unique $m \in \mathbb{Z}$. This indicates that the map $\phi : G \longrightarrow \mathbb{Z}$ given by $\phi(a^i) = i$ is thus well defined and is bijective.
Also,

$$\phi(a^i\, a^j) = \phi(a^{i+j}) = i + j = \phi(a^i) + \phi(a^j).$$

So the homomorphism property is satisfied and ϕ is an isomorphism. ✓

▸ Now we we prove (ii), in which case $a^m = e$ for some positive integer m. Let n be the smallest positive integer such that $a^n = e$. If $s \in \mathbb{Z}$ and $s = nq + r$ for $0 \leq r < n$, then

$$a^s = a^{nq+r} = (a^n)^q\, a^r = e^q\, a^r = a^r.$$

As in (i), if $0 < k < h < n$ and $a^h = a^k$, then $a^{h-k} = e$ and $0 < h - k < n$, contradicting our choice of n.

Thus the elements

$$a^0 = e,\ a,\ a^2,\ \ldots,\ a^{n-1}$$

are all distinct and comprise all elements of G. This indicates that the map $\psi : G \longrightarrow \mathbb{Z}_n$ given by $\psi(a^i) = i$ for $i = 0,\ 1,\ \ldots,\ n-1$ is thus well defined and bijective. Because $a^n = e$, we see that $a^i\, a^j = a^k$ where $k = i +_n j$. Thus

$$\psi(a^i\, a^j) = i +_n j = \psi(a^i) +_n \psi(a^j).$$

So the homomorphism property is satisfied and ψ is an isomorphism. ✓ ■

• Theorem:

Let G be a cyclic group with n elements generated by a. Let $b \in G$ and let $b = a^s$ for some $s \in \mathbb{Z}$. Then b generates a cyclic subgroup H of G containing n / d elements, where d is the gcd of n and s. Also, $\langle a^s \rangle = \langle a^t \rangle$ iff $\gcd(s,\ n) = \gcd(t,\ n)$.

Proof:

(See page 64, Fraleigh's) ■

Example:

For an example using additive notation, consider $\mathbb{Z}_{12}$ with the generator $a = 1$.
Then,

▸ Since the gcd of 3 and 12 is 3, we have that $3 = 3 \cdot 1$ generates a subgroup of $12 / 3 = 4$ elements, namely $\langle 3 \rangle = \{0,\ 3,\ 6,\ 9\}$.

▸ Since the gcd of 8 and 12 is 4, we have that $8 = 8 \cdot 1$ generates a subgroup of $12 / 4 = 3$ elements, namely $\langle 8 \rangle = \{0,\ 4,\ 8\}$.

▸ Since the gcd of 12 and 5 is 1, we have that $5 = 5 \cdot 1$ generates a subgroup of $12 / 1 = 12$ elements, namely $\langle 5 \rangle = \{0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10,\ 11\} = \mathbb{Z}_{12}$. ✡

The following corollary follows immediately from the above theorem:

• Corollary:

If a is a generator of a finite cyclic group G of order n, then the other generators of G are the elements of the form a^r, where r is reltively prime to n.

Example:

Find all subgroups of $\mathbb{Z}_{18}$ and give their subgroup diagram.

Solution:

All subgroups are cyclic. By the above corollary, the elements 1, 5, 7, 11, 13, and 17 are all generators of $\mathbb{Z}_{18}$.
Starting with 2,

$$\langle 2\rangle = \{0,\ 2,\ 4,\ 6,\ 8,\ 10,\ 12,\ 14,\ 16\}$$

is of order 9 and has as generators elements of the form $2\,h$, where h is relatively prime to 9. Namely, $h = 1,\ 2,\ 4,\ 5,\ 7,$ and 8, so $2\,h = 2,\ 4,\ 8,\ 10,\ 14,$ and 16. The element 6 of $\langle 2\rangle$ generates $\{0,\ 6,\ 12\}$, and 12 also is a generator for this subgroup.
We have thus far found all subgroups generated by 0, 1, 2, 4, 5, 6, 7, 8, 10, 12, 13, 14, 16, and 17. This leaves just 3, 9, and 15 to consider:

$$\langle 3\rangle = \{0,\ 3,\ 6,\ 9,\ 12,\ 15\},$$

and 15 also generates this group of order 6, since $15 = 5\cdot 3$, and the gcd of 5 and 6 is 1.
Finally,

$$\langle 9\rangle = \{0,\ 9\}.$$

The subgroup diagram for these subgroups of $\mathbb{Z}_{18}$ is given by the following figure: