Math 3GR3 - Abstract Algebra

Sang Woo Park

September 21, 2017

Course Outline

- Office hours: Monday 9:30-10:20 and Wednesday 2:30-3:20 (HH 419)

Contents

1 Set theory **2**

1.1 Reveiew 2

1.2 Equivalence relation 3

1.3 Well ordering principle and division algorithm 6

2 Groups and rings **11**

2.1 Group theory 11

2.2 Subgroups 16

1 Set theory

1.1 Reveiew

Definition 1.1. *Set is a collection of distinct objects.*

Here are some properties of a set:

- $\{\text{apple}, 2, \{3\}\}$ is a set.
- If x is in A, we write $x \in A$. If not, we write $x \notin A$.
- $\varnothing$ is an empty set.
- Note that order or repeated elements are not important: $\{1, 2, 3\} = \{3, 1, 2\}$ and $\{1, 1, 1, 2, 2, 3\} = \{1, 2, 3\}$.

Definition 1.2. *Let A and B be sets. B is a subset of A if for all $x \in B$, $x \in A$ and we write $B \subseteq A$. B is a proper subset of A if B is a subset of A but $B \neq A$ and we write $B \subset A$.*

Theorem 1.1. *A and B are equal if and only if $B \subseteq A$ and $B \subseteq A$.*

Example 1.1.1.

- $\mathbb{N}$ is a set of natural numbers: $\{0, 1, 2, 3, \dots\}$.
- $\mathbb{Z}$ is a set of integers: $\{\dots, -2, -1, 0, 1, 2, \dots\}$.
- $\mathbb{Q}$ is a set of rational numbers.
- $\mathbb{R}$ is a set of real numbers.
- $\mathbb{C}$ is a set of complex numbers.

Definition 1.3. *Universal set U contains all elements.*

Let A and B be sets. Then, we can define the following:

Definition 1.4 (Intersection)**.** $A \cap B = \{x \mid x \in A \textit{ and } x \in B\}$.

Definition 1.5 (Union)**.** $A \cup B = \{x \mid x \in A \textit{ or } x \in B\}$.

Definition 1.6 (Complement)**.** $A' = \{x \mid x \in U \textit{ and } x \notin A\}$.

Definition 1.7 (Set difference)**.** $A - B = \{x \mid x \in A \textit{ but } x \notin B\}$.

Definition 1.8 (Cartesian product)**.** $A \times B = \{(a, b) \mid a \in A, b \in B\}$.

Example 1.1.2. Let $A = \{0, 1\}$ and $B = \{\text{dog}, \text{cat}\}$. Then,

$$A \times B = \{(0, \text{dog}), (0, \text{cat}), (1, \text{dog}), (1, \text{cat})\}$$

Theorem 1.2 (DeMorgan's Laws)**.** *Let A and B be sets. Then,*

- $(A \cup B)' = A' \cap B'$.
- $(A \cap B)' = A' \cup B'$.

Proof. To show that $(A \cap B)' = A' \cup B'$, we want to show that $(A \cap B)' \subseteq A' \cup B'$ and $A' \cup B' \subseteq (A \cap B)'$.

First, let $x \in (A \cap B)'$. Then, $X \notin (A \cap B)$. So either $x \notin A$ or $x \notin B$. If $x \notin A$, then $x \in A'$. Since $A' \subset A' \cup B'$, $x \in A' \cup B'$. If $x \in B$, then $x \in B' \subset A' \cup B'$. Therefore, $x \in A' \cup B'$.

Now, we want to prove the opposite direction. Take $x \in A' \cup B'$. So $x \in A'$ or $x \in B'$. Thus, $x \notin A$ or $x \notin B$. In either case, $x \notin (A \cap B)$. Therefore, $x \in (A \cap B)'$. □

1.2 Equivalence relation

Definition 1.9. *Let A and B be sets. Then, a* relation *is any subset $S \subseteq A \times B$*

Example 1.2.1. Let $A = \{0, 1\}$ and $B = \{\text{dog}, \text{cat}\}$. Then,

$$S = \{(1, \text{dog}), (2, \text{cat})\} \subseteq A \times B$$

Functions can give you relations:

Example 1.2.2. Let $f : \mathbb{R} \to \mathbb{R}$ where $f(x) = x^2$. Then, the following is a relation:

$$\{(x, f(x)) \,|\, x \in \mathbb{R}\} \subseteq \mathbb{R} \times \mathbb{R}$$

Example 1.2.3. Let X be a set of all McMaster students. Then,

$$R = \{(x, y) \,|\, x \text{ has same height as y}\} \subseteq X \times X$$

Definition 1.10. *Let X be a set. An* equivalance relation *on X is a set $R \subseteq X \times X$ such that*

- $(x, x) \in R$ *for all* $x \in X$ (reflexive)
- *If* $(x, y) \in R$ *and* $(y, x) \in R$ (symmetric)
- *If* $(x, y) \in R$ *and* $(y, z) \in R$*, then* $(x, z) \in R$ (transitive)

Example 1.2.4. Example 1.2.1 is not an equivalence relation since $A \neq B$.

Example 1.2.5. Example 1.2.2 is not an equivalence relation since $(2, 2) \notin \{(x, x^2) \,|\, x \in \mathbb{R}\}$.

Example 1.2.6. Example 1.2.3 is an equivalence relation.

- (refective) For any student $xinX$, x has the same height as x, so $(x, x) \in R$.
- (symmetric) Suppose $(x, y) \in R$ so x and y have the same height. But y and x have the same height so $(y, x) \in R$.

- (transitive) if $(x, y) \in R$ and $(y, z) \in R$, then x and y have the same height and y and z have the same height. So x and z have the same height, i.e. $x, z \in R$.

Remark. Sometimes, we write $x \sim y$ to mean $(x, y) \in R$.

Example 1.2.7. Prove that the following is an equivalence relation:a

$$R = \{(x, y) \,|\, x = y\} \subseteq \mathbb{Z} \times \mathbb{Z}$$

Proof.

- (reflective) For any $x \in \mathbb{Z}$, $x = x$ and $(x, x) \in R$.
- (symmetric) If $x \sim y$ then $x = y$ so $y = x$, and $y \sim x$.
- (transitive) If $x \sim y$ and $y \sim z$, then $x = y = z$, so $x \sim z$.

□

Definition 1.11. *Fix a positive integer $n > 0$. We say r is congruent to s modulo n if n divides $r - s$, i.e. $(r - s) = nl$ for some integer l. We write*

$$r \equiv s \mod n$$

Example 1.2.8. Let $n = 7$. Then, $22 \equiv 8 \mod 7$ since 7 divides $22 - 8$. However, $22 \not\equiv 10 \mod 7$ since 7 does not divide $23 - 10 = 13$.

Example 1.2.9. Congruent definition is an equivalence relation on $\mathbb{Z}$:

$$R = \{(r, s) \,|\, r \equiv s \mod n\} \subseteq \mathbb{Z} \times \mathbb{Z}$$

Proof.

- (reflexive) For all $r \in \mathbb{Z}$, n divides $r - r = 0$. So $r \equiv r \mod n$ for all r. So $(r, r) \in R$.
- (symmetric) Suppose $(r, s) \in R$ so $r - s = nl$ for some l. We multiply both sides by (-1) to obtain

  $$(s - r) = (-1)(r - s) = (-1)(nl) = n(-l).$$

  So n divides $s - r$ and $(s, r) \in R$.
- (transitive) If $(r, s) \in R$ and $(s, t) \in R$, then $r - s = nl$ and $s - t = nk$. But then

  $$(r - t) = (r - s) + (s - t) = nl + nk = n(l + k),$$

  so $(r, t) \in R$.

□

Definition 1.12. *If R is an equivalence relation on X, and $x \in X$, the equivalence class of x is*

$$[x] = \{y \,|\, (x, y) \in R\}$$

Example 1.2.10. Consider

$$R = \{(x, y) \,|\, x \text{ and } y \text{ have the same height}\}.$$

Then,

$$[\text{Abby}] = \{\text{all people who have same height as Abby}\}.$$

Example 1.2.11. Consider

$$R = \{(x, y) \,|\, x = y\} \subseteq \mathbb{Z} \times \mathbb{Z}.$$

Then,

$$[42] = \{42\}.$$

Example 1.2.12. Consider

$$R = \{(r, s) \,|\, r \equiv s \mod 5\} \subseteq \mathbb{Z} \times \mathbb{Z}.$$

Then,

$$[3] = \{\dots, -7, -2, 3, 8, 13, 18, \dots\}.$$

Definition 1.13. *A* partition *P of set X is a collection of sets, $X_0, X_1, X_2, \dots$ such that*

$$X = \bigcup_i X_i$$

and $X_i \cap X_j = \varnothing$ for all $i \neq j$.

Example 1.2.13. In Example 1.2.12, we have

$$\mathbb{Z} = [0] \cup [1] \cup [2] \cup [3] \cup [4]$$

Theorem 1.3. *If R is an equivalence relation on X, then the distinct equivalence classes form a partition of X.*

Proof. For any $x \in X$, $x \sim x$ so $x \in [x]$. Thus,

$$X = \bigcup_{x \in X} [x].$$

Given $x, y \in X$, we want to show that $[x] = [y]$ or $[x] \cap [y] = \varnothing$. Suppose that $[x] \cap [y] \neq \varnothing$. Let $z \in [x] \cap [y]$. So $x \sim z$ and $y \sim z$. Let $a \in [x]$. Then, $x \sim a$ so $a \sim x$, and $x \sim z$ and $z \sim y$. So $a \sim y$. Thus $y \sim a$, and thus $a \in [y]$. So $[x] \subseteq [y]$.

Same argument shows $[y] \subseteq [x]$. So have $[x] \cap [y] = \varnothing$ or $[x] = [y]$. So considering only distinct classes, we have a partition:

$$X = [x_0] \cup [x_1] \cup \cdots ,$$

□

1.3 Well ordering principle and division algorithm

Theorem 1.4. *(First principle of mathematical induction) Set $S(n)$ be a statement about integer $n \in \mathbb{N}$ and supposed $S(n)$ is true for some $n_0 \geq 1$. If for all integers $k \geq 0$, if $S(k)$ is true implies $S(k+1)$ is true, then $S(n)$ is true for all $n \geq n_0$.*

Theorem 1.5 (Second principle of mathematical induction)**.** *Let $S(n)$ be a statement foor integers $n \in \mathbb{N}$ and assume $S(n_0)$ is true. If $S(n_0), S(n_0+1), \ldots, S(k)$ imply that $S(k+1)$ is true, then $S(n)$ is true for all $n \geq n_0$.*

Definition 1.14 (Well ordering property)**.** *Every nonempty set of positive integers has a smallest element.*

Remark. Well ordering property becomes false once you include negative values.

Lemma 1.1. *Principle of mathematical induction implies 1 is the smallest integer.*

Theorem 1.6. *Principle of mathematical induction implies well ordering property.*

Proof. Let S be a nonempty set of positive integers. If $1 \in S$, then by above lemma, the set S has a smallest element. Assume that if S is a set that containes $1 \leq k \leq n$, then S satisfies the well ordering property. Let S be any set that contains an integer $1 \leq k \leq n+1$. If S does not contain any elements smaller than $n+1$, $n+1$ is the smallest element. If S does contain an integer $k < n+1$, then by induction step, we have already shown that S has well ordering perperty. By induction, all S satisfy well ordering property. $\square$

Remark. Induction and well ordering property are equivalent.

Recall long division. If we divide 304 with 14, we get $304 = 14(21) + 10$. Here, we call 304 a dividend, 14 a divisor, 21 a quotient, and 10 a remainder. Now, we want to know whether this process stops and whether the answer is unique:

Theorem 1.7 (Division algorithm)**.** *Let A and B be integers with $b > 0$. Then, there exists unique integers q and r such that*

$$a = bq + r \text{ with } 0 \leq r < b$$

Proof. To prove that the above theorem is true, we have to show (1) existence and (2) uniqueness.

First, let $S = \{a - bk \mid a - bk \geq 0\}$. If $0 \in S$, then there is a k such that $a - bk = 0 \iff a = bk$. Then, we can let $q = k$ and $r = 0$. If $0 \notin S$, we want to use the well ordering principle. We need to check that $S \neq \varnothing$.

- If $a < 0$, then $a - ba = a(1-b) > 0$, since $b > 0$. So $S \neq \varnothing$.
- If $a = 0$, then $0 - b(-1) > 0$, so $S \neq \varnothing$.

- If $a > 0$, then $a - b(0) > 0$, so $S \neq \varnothing$.

By the well ordering property, there exists a smallest element say r in S, i.e. there is a q such that $a - bq = r$.

We claim that we also have $0 \leq r < b$. If $r \geq b$,

$$r - b = (a - bq) - b = a - b(q+1) \geq 0.$$

So $r - b \in S$ and $r - b$ is smaller than r, the smallest element of S. So we must have $0 \leq r < b$.

Now, suppose there was q, r, q', r' such that

$$\begin{cases} a = bq + r,\ 0 \leq r < b \\ a = bq' + r',\ 0 \leq r < b \end{cases}$$

So $bq + r = bq' + r' \implies bq - bq' = r' - r$. Note that

$$-b < -r < r' - r < r' < b.$$

Thus,

$$-b < bq - bq' < b.$$

If we divide both sides by b, we get $-1 < q - q' < 1$. So we find that $q - q' = 0$. $\square$

Definition 1.15. *a divides b if there exists m such that $b = am$. We write $a|b$.*

Example 1.3.1. $3|12$ since $12 = 3\dot{4}$.

Definition 1.16. *d is a common divisor of a and b if $d|a$ and $d|b$.*

Example 1.3.2. 2 is a common divisor of 12 and 18.

Definition 1.17. *d is the greatest common divisor of a and b if (1) d is a common divisor of a and b and (2) if $d'|a$ and $d'|b$, then $d'|d$. We write $d = \gcd(a, b)$.*

Example 1.3.3. $6 = \gcd(12, 18)$.

Definition 1.18. *a and b are relatively prime if $\gcd(a, b) = 1$.*

Remark. For any integer b, $b|0$ since $0 = b \cdot 0$. Furthermore, $\gcd(b, 0) = |b|$.

Theorem 1.8. *Let a and b be non-zero integers. Then, there exists r and s such that $\gcd(a, b) = ra + sb$.*

Example 1.3.4. $6 = \gcd(12, 18) = 12(-1) + 18 \cdot 1$

Proof. Let $S = \{am + bn \mid m, n \in \mathbb{Z}, am + bn > 0\}$. If $a < 0$, then $a(-1) + b(0) > 0$, so $S \neq \varnothing$. If $a > 0$, then $a(1) + b(0) > 0$ so $S \neq \varnothing$. By the well ordering property, there exists a smallest element in S, say d. So $d = am + bn$ for some $m + n$.

Now, we want to prove that $d = \gcd(a, b)$. First, by the division algorithm, there exists q and r such that $a = dq + r$ with $0 \leq r < d$. If $r > 0$, then,

$$\begin{aligned} r = a - dq &= a - (am + bn)q \\ &= a - amq - bnq \\ &= a(1 - mq) + b(-nq) > 0. \end{aligned}$$

Then $r \in S$ and $r < d$ but d is the smallest element of S. So $r = 0$, i.e. $a = dq + 0$. So $d|a$. Sampe proof shows $d|b$.

Now, suppose that $d'|a$ and $d'|b$. So $a = d'a'$ and $b = d'b'$. But then

$$\begin{aligned} d &= am + bn \\ &= d'a'm + d'b'n \\ &= d'(a'm + b'n) \end{aligned}$$

So $d'|d$. Hence, $\gcd(a, b) = d$. □

Remark. If $\gcd(a, b) = 1$, then $1 = as + br$ for some s and r.

Lemma 1.2. *Suppose a, b, q and r such that $a = bq + r$. Then,* $\gcd(a, b) = \gcd(b, r)$.

Proof. Let $d = \gcd(a, b)$ and $e = \gcd(b, r)$. Now, $d|a$ and $d|b$, so $a = da'$ and $b = db'$. Since $r = a - bq$, we have $r = da' - db'q = d(a' - b'q)$. So $d|r$ and $d|b$, so $d \leq \gcd(b, r) = e$.

Now, $e|b$ and $e|r$. So $b = eb^*$ and $r = er^*$. So $a = bq + r = eb^*q + er^* = e(b^*q + r^*)$. So $e|b$ and $e|a$. So $e \leq d$. Hence $d \leq e \leq d$, i.e. $e = d$. □

Now, we introduce the *Euclidean algorithm* to find the greatest common divisors of two integers: To compute $\gcd(a, b)$, repeatedly apply divison algorithm:

$$\begin{aligned} a &= bq_1 + r_1 \\ b &= r_1q_1 + r_2 \\ r_1 &= r_2q_3 + r_3 \\ &\vdots \\ r_{n-2} &= r_{n-1}q_n + r_n \\ r_{n-1} &= r_nq_{n+1} + 0 \end{aligned}$$

Then, the last non-zero remainder, r_n is the greatest common divisor.

Remark. This algorithm is guaranteed to stop because r_n is a monotonically decreasing sequence, i.e. $b > r_1 > r_2 > r_3 > \cdots \geq 0$. At some point, we must reach $r_{n+1} = 0$ for some n.

Example 1.3.5. We want to find $\gcd(234, 96)$. Note $234 = 96 \cdot +42$. Note that $\gcd(234, 96) = \gcd(96, 42)$. Then, since $96 = 42 \cdot 2 + 12$, we have $\gcd(96, 42) = \gcd(42), 12$. Likewise, we can continue to obtain $\gcd(234, 96) = 6$.

Remark. We can reverse this algorithm to find s and t such that $\gcd(0, b) = sa + bt$. Notice that

$$\begin{aligned}
234 &= 96(2) + 42 \\
96 &= 42(2) + 12 \\
42 &= 12(3) + 6 \\
42 &= 234 + 96(-2) \; 12 \quad = 96 + 42(-2) \\
6 &= 42 + 12(-3)
\end{aligned}$$

So

$$\begin{aligned}
6 &= 42 + [96 + 42(-2)](-3) \\
&= 42(7) + 96(-3)
\end{aligned}$$

Then,

$$\begin{aligned}
6 &= [234 + 96(-2)](7) + 96(-3) \\
&= (234)(7) + 96(-3) + 96(-3) \\
&= 234(7) + 96(-17)
\end{aligned}$$

Definition 1.19. *A positive integer $p > 1$ is prime if its only divisions are 1 and p. Otherwise, a number is composite.*

Example 1.3.6. 7 is a prime.

Lemma 1.3. *Let a and b be integers and p a prime. If $p|ab$, then $p|a$ or $p|b$. This statement is false when p is not a prime.*

Proof. If $p \nmid a$, we want to show that $p|b$. If $p \nmid a$, then $\gcd(a, p) = 1$. So there exists s and t such that $1 = as + pt$. Then, we have $b = abs + pbt$. Since $p|ab$, we have $ab = pk$. So,

$$b = pks + pbt = p(ks + bt).$$

Therefore, $p|b$. $\square$

Theorem 1.9 (Fundamental theorem of arithmetic)**.** *Let $n > 1$ be any integer.*

$$n = p_1 p_2 \cdots p_k,$$

where p_i is a prime (not necessarily distinct). Furthermore, this decomposition is unique in the following sense. If $n = q_1 \cdots q_l$ is another production of primes, then $k = l$ and after relabelling, $p_i = q_i$.

Existence. Let

$$S = \{a \in \mathbb{Z} \mid a > 1 \text{ and } a \text{ does not have a primary decomposition}\}.$$

If $S \neq \varnothing$, then by the well ordering principle, there is a smallest $a \in S$. Note a is not a prime because if a is prime then $a = a$ is a factorization. So a is composite and $a = bc$ with $1 < b, c < a$. However, $b, c \notin S$ so they have a factorization:

$$b = p_1 \cdots p_l$$
$$c = q_1 \cdots q_k$$

But then $a = p_1 \cdots p_l q_1 \cdots q_k$. So $a \notin S$, This is a contradiction and $S = \varnothing$.

Now, we want to prove the uniqueness. Suppos

$$n = p_1 \cdots p_k = q_1 \cdots q_l$$

Since $p_1 | n$, $p_1 | q_1 \cdots q_l$. So $p_1 | q_i$ for some i by the Lemma. Since q_i is prime and $p_1 > 1$, then $p_1 = q_i$. Then, we do a relabelling so that q_i is q_1. So we have

$$\begin{aligned} p_1 p_2 \cdots p_k &= q_1 q_2 \cdots q_l \\ \implies p_2 \cdots p_k &= q_2 \cdots q_l \end{aligned}$$

We repeat the process. If $k > 1$, we would end with

$$p_{l+1} p_{l+2} \cdots p_k = 1.$$

Likewise, we would end with a similar equation if $k < l$. Both cases are impossible because $p_i, q_i > 1$. So $k = l$ and $p_i = q_i$ for all i. $\square$

Theorem 1.10. *There exists an infinite number of primes.*

Proof. Suppose only primes are $p_1, p_2, \cdots, p_n$. Let

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

Since $P > p_1, \cdots, p_n$, P is not a prime. So P is a composite number by FTA, some p_i must divide P. Since $P - p_1 p_2 \cdots p_n = 1$, then $p_i | 1$, yielding contradiction. So there must be infinite number of primes. $\square$

Example 1.3.7. Prove that if $\gcd(a, b) = 1$ and $a | bc$, then $a | c$.

Proof. Beacuse $\gcd(a, b) = 1$, there exists integers s and t such that $as + bt = 1$. This follows from theorem 2.10. If we multiply both sides by c, we get

$$acs + bct = c$$

Since $a | bc$, $bc = ak$ for some integer k. After substitution, we have

$$c = acs + akt.$$

But this means

$$c = a(cs + kt).$$

So $a | c$, as desired. $\square$

2 Groups and rings

2.1 Group theory

Before we begin, we're going to look at sets with *extra structure*.

Example 2.1.1 (Integer equivalence classes)**.** Let $n = 6$. Consider the distinct equivalence classes modulo 6:

$$R = \{(a, b) \,|\, a \equiv b \mod 6\} \subseteq \mathbb{Z} \times \mathbb{Z}$$

Then,

$$\begin{aligned}
[0] &= \{\dots, -6, 0, 6, \dots\} \\
[1] &= \{\dots, -5, 1, 7, \dots\} \\
[2] &= \{\dots, -4, 2, 8, \dots\} \\
[3] &= \{\dots, -3, 3, 9, \dots\} \\
[4] &= \{\dots, -2, 4, 10, \dots\} \\
[5] &= \{\dots, -1, 5, 11, \dots\}
\end{aligned}$$

We denote the six disctinct equivalence classes by

$$\mathbb{Z}_6 = \{[0], [1], [2], [3], [4], [5]\}.$$

Usually, we write

$$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}.$$

In general, for any $n > 1$, let

$$\mathbb{Z}_n = \{0, 1, 2, \dots, n - 1\}.$$

Then, we can add and multiply elements of $\mathbb{Z}_n$:

$$\begin{aligned}
a + b &= (a + b) \mod n \\
ab &= (ab) \mod 6
\end{aligned}$$

In fact, for any $a \in \mathbb{Z}$ and $n > 1$, if $a = nq + r$ with $0 \leq r < n$, then $[a] = [r]$. Equivalently, $a = r \mod n$ and $a = r$ in $\mathbb{Z}_n$.

We can look at some other properties of addition and multiplication in $\mathbb{Z}_n$:

- Addition and multiplication commute
- Addition and multiplication are associative
- There are additive and multiplicative identities
- For every element in $\mathbb{Z}_n$, there exists an additive inverse.
- Multiplication is distributive over additon
- If $\gcd(a, n) = 1$, then there exists an integer b such that $ab = 1 \mod n$.

Consider a square cut in the plane. We can flip it, rotate it, and but not stretch it, and then put it back in the original spot. Then, we have 8 operations.

Let R_0 be rotating $0°$, R_{90} rotating $90°$, R_{180} rotating $180°$, and R_{270} rotating $270°$. Then, H will be a flip on the horizontal axis, V on the vertical axis, D_1 on the main-diagonal, and D_2 on the anti-diagonal. Note that you can perform one operation, then followed by another, and end back up with another known operation. For example H, R_{270} is equivalent to D_1. Note that order is important.

We want to think of these as functions, i.e., each function maps a square to itself. Let

$$D_4 = \{R_0, R_{90}, R_{180}, R_{270}, V, H, D_1, D_2\}.$$

We call is a dihedral group and it has the following properties:

- Operations of composition is closed.
- R_0 is an identity element.
- Each element $A \in D_4$ has an inverse, i.e., we can reverse it to R_0.
- The operation is associative.

In fact, D_4 forms a group and those are the four properties that all groups must have.

Now, we want to formally define a group.

Definition 2.1. *Given any set G, a* binary operation $\circ$ *is any function*

$$\circ : G \times G \to G$$

that maps a pair $(a, b) \in G \times G$ to an element $a \circ b$.

Example 2.1.2. $+$ on $\mathbb{Z}$ is a binary operation

$$+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$$

. Likewise, multiplication is also a binary operation.

Example 2.1.3. Composition of functions on D_4 is a binary operation:

$$\circ D_4 \times D_4 \to D_4$$

Definition 2.2. *A* group $(G, \circ)$ *is a set G with a binary operation $\circ$ such that*

- *(associative) $a \circ (b \circ c) = (a \circ b) \circ c$.*
- *(identity) there exists an $e \in G$ such that $a \circ e = e \circ a = a$ for all $a \in G$.*
- *(inverse) for all $a \in G$ exists $a^{-1} \in G$ such that $a \circ a^{-1} = a^{-1} \circ a = e$.*

Definition 2.3. *If a group G satisfies commutativity,*

$$a \circ b = b \circ a, \forall a, b \in G,$$

then G is called abelian.

Example 2.1.4. D_4 is a group where the binary operation is composition of functions. D_4 is not abelian since

$$D_1 \circ H \neq H \circ D_1$$

Example 2.1.5. Consider

$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}.$$

There are two operations on $\mathbb{Z}$: addition and multiplication. $\mathbb{Z}$ with addition is an abelian group with identity 0. However, $\mathbb{Z}$ with multiplication is not a group because it doesn't have an inverse.

Example 2.1.6. Rationals, real numbers, and complex numbers are all groups with operation of $+$.

Example 2.1.7 (Trivial group)**.** $G = \{e\}$.

Example 2.1.8. Fix $n > 1$. Then, $\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$ is a group under addition. However, it's not a group under multiplication.

Example 2.1.9. $\mathbb{R}$ is not a group under multiplication. It satisfies associativity and existence of identity but 0 does not have a multipllicative inverse. However,

$$\mathbb{R}^* = \mathbb{R} \setminus \{0\}$$

is a group under multiplication. Likewise, $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ and $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ are groupsunder multiplication.

Example 2.1.10. Let $n > 1$ and

$$u(n) = \{a \,|\, 1 \leq a \leq n-1, \gcd(a, n) = 1\}.$$

For example,

$$\begin{array}{ll} u(3) = \{1, 2\} & u(5) = \{1, 2, 3, 4\} \\ u(4) = \{1, 3\} & u(8) = \{1, 3, 5, 7\} \end{array}$$

For all $n > 1$, $u(n)$ is a group under multiplication modulo n.

Example 2.1.11. Consider

$$M_2(\mathbb{R}) = \{\text{all } 2 \times 2 \text{ matrices with entries in } \mathbb{R}\}.$$

This set is a group under addition.

Example 2.1.12. All vector spaces are groups under addition.

Example 2.1.13 (General linear group)**.**

$$\begin{aligned} GL_2(\mathbb{R}) &= \{\text{all } 2\times 2 \text{ matrices that are invertible}\} \\ &= \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \,\middle|\, ad - cb \neq 0 \right\} \end{aligned}$$

This is a group under matrixmultiplication.

We want to make new groups from existing groups. Let G and H be groups and that let $\Box$ and $*$ denote their binary operations. Then,

$$G \times H = \{(g,h) \,|\, g \in G, h \in H\}.$$

This is also a group where

$$(g_1, h_1) \circ (g_2, h_2) = (g_1 \Box g_2, h_1 * h_2).$$

Example 2.1.14. Consider

$$G = \mathbb{Z}_3 = \{0,1,2\}, H \quad = \mathbb{R}^* = \mathbb{R} \setminus \{0\}$$

Then,

$$(2,4) \circ (2,6) = (2+2, 4\times 6) = (1, 24) \in G \times H.$$

In this case, the identity of $\mathbb{Z}_3 \times \mathbb{R}^*$ is $(0,1)$.

Definition 2.4. *The order of G refers to number of elements in G and is denoted by $|G|$. G is finite if $|G| < \infty$. Otherwise, it is infinite.*

There are many different binary operations used to define groups. Normally, we will use the mutliplicative notation. The only exception is when we are proving something about an additive group.

From now on, we will be using the following notations:

$$a^n = \begin{cases} a \cdot a \cdot \cdots \cdot a & \text{(n times) if } n > 0 \\ 1 & n = 0 \\ (a^{-1} \cdots (a^{-1}) & n < 0 \end{cases}$$

$$na = \begin{cases} a + a + \cdots + a & \text{(n times) if } n > 0 \\ 0 & n = 0 \\ (-a) + (-a) + \cdots + (-a) & n < 0 \end{cases}$$

Theorem 2.1. *For every group G, identity is unique.*

Proof. Suppose e and e' are identities of G. So for any $a \in G$, (1) $ae = a$ and (2) $e'a = a$. If $a = e'$, (1) implies $e'e = e'$. If $a = e$, (2) implies $e'e = e$. So

$$e' = e'e = e,$$

and $e' = e$. $\Box$

Theorem 2.2. *If $g \in G$, then inverse of g is unique.*

Proof. Suppose that g' and g'' are inverses of g. So $g'g = gg' = e$ and $g''g = gg'' = e$. So

$$gg' = gg'' = e.$$

If we multiply both sides by g',

$$\begin{aligned} g'(gg') &= g'(gg'') \\ \implies (g'g)g' &= (g'g)g'' \\ \implies eg' = g' &= g'' = eg''. \end{aligned}$$

□

Theorem 2.3 (Sicks-shoes property)**.** $(ab)^{-1} = b^{-1}a^{-1}$.

Proof. By definition, $(ab)^{-1}$ is the inverse of (ab), i.e.,

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

But we also have

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

So $b^{-1}a^{-1}$ is also n inverse of (ab). Since inverses are unique, we have

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

□

Theorem 2.4. *If G, cancellation works, i.e. if $ab = bc$, then $a = c$.*

Proof. Suppose that $ab = ac$. Then, $a^{-1} \in G$. So we multiply both sides by a^{-1} on the left

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

So $b = c$. □

Remark. As a consequence, each row and column in a Cayley table (group operation table) has a distinct element. In other words, if $ab_i = ab_j$ then $b_i = b_j$

Theorem 2.5. *For any $a, b \in G$, there exists unique x and y such that $ax = b$ and $ya = b$.*

Proof. One solution is $x = a^{-1}b$ since

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

This is unique because if $ax_1 = b = ax_2$, by cancellation $x_1 = x_2$. □

2.2 Subgroups

Definition 2.5. *A subset H of a group G is a goup if it is a group under the same operation of H.*

Example 2.2.1. If $G \neq \{e\}$, the G has at leaset two subrgoups:

- $\{e\} \subseteq G$,
- G itself.

These are trivial groups but we want $\{e\} \subset H \subset G$.

Example 2.2.2. Consider $G = \mathbb{Z}$. Then,

$$E = \{n \in G \,|\, n \text{ is even}\} = \{-4, -2, 0, 2, 4\}$$

is a subgroup because

- because it is closed under addition.
- $0 \in E$.
- addition is associative.
- for any $a \in E$, $-a \in E$ so every element in E has an inverse.

Example 2.2.3. The set of odd integers is not a subgroup because it is not closed under addition and 0 is not an element.

Example 2.2.4. $m\mathbb{Z} = \{mn \,|\, n \in \mathbb{Z}\}$ is a subgroup.

Example 2.2.5. Consider D_4. Let $H = \{R_0, R_{90}, R_{180}, R_{270}\}$. Note D_4 is not abelian but H is.

Example 2.2.6. consider $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$, a group under multiplication. Then,

$$H = \{1, -1, i, -i\}$$

is a finite subgroup of $\mathbb{C}^*$:

	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

Example 2.2.7. Show that if $a^2 = e$ for all $a \in G$ then G is abelian.

Proof. Given any $a, b \in G$, we want to show $ab = ba$. Given that $aa = e$, since inverses are unqiue, $a = a^{-1}$. Now, consider $(ab)^2$. Since $ab \in G$,

$$(ab^2) = (ab)(ab) = e.$$

Now, we multiply $(ab)(ab) = e$ on the left by a and on the right by b:

$$\begin{aligned} a(ab)(ab)b &= aeb \\ (aa)(ba)(bb) &= ab \\ ba &= ab \end{aligned}$$

So G is abelian. $\square$