Math 3GR3 - Abstract Algebra

Sang Woo Park

December 11, 2017

Course Outline

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

Contents

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)**.** $A \cap B = \{x \mid x \in A \text{ and } x \in B\}$.

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

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

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

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,

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

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 $x \in X$, 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

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

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*

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

Example 1.2.10. Consider

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

Then,

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

Example 1.2.11. Consider

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

Then,

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

Example 1.2.12. Consider

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

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 suppose $S(n)$ 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. □

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 $S = \{a - bk \,|\, a - bk \geq 0\}$. 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 $q - q' = 0$. □

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 $12 = 3 \cdot 4$.

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:

$$\begin{aligned} a &= bq_1 + r_1 \\ b &= r_1 q_1 + r_2 \\ r_1 &= r_2 q_3 + r_3 \\ &\vdots \\ r_{n-2} &= r_{n-1} q_n + r_n \\ r_{n-1} &= r_n q_{n+1} + 0 \end{aligned}$$

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 $\gcd(a,b) = sa + bt$. 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, $p|b$. □

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, $p_i = q_i$.

Proof. (Existence) Let

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

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 $S = \varnothing$.

(Uniqueness). Suppose

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

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. □

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. □

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. □

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:

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

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

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 $e' = e$. □

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 (Socks-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 G.*

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. □

Theorem 2.6. *A subset H of a group G is a subgroup if*

- $e \in H$.
- $\forall g_1, g_2 \in H, g_1 \circ g_2 \in H$.
- $\forall g \in H, g^{-1} \in H$

Proof. 1 implies that H has an identity, 2 implies that H is closed under operation. 3 implies that every $g \in H$ has an inverse. So we only need to check the associative property.

Let $a, b, c \in H$. Now, $a, b, c \in G$, so

$$(ab)c = a(bc)$$

holds in G. But since the operation is closed, (ab) and (bc) are in H, so

$$(ab)c = a(bc)$$

also holds in H. □

Definition 2.6 (Center of a group)**.** *For any group G, the center of G is defined as*

$$Z(G) = \{a \in G \mid ag = ga, \ \forall g \in G\}.$$

Example 2.2.8. If G is abelian, $G = Z(G)$. If $G = D_3$, $Z(D_4) = \{R_0, R_{180}\}$. For all G, $e \in Z(G)$.

Theorem 2.7. *For all G, $Z(G)$is a subgroup of G.*

Proof. First, $e \in Z(G)$ since for all $g \in G$,

$$eg = g = ge.$$

Let $a, b \in Z(G)$. We want to show that $ab \in Z(G)$. Sofor any $g \in G$, we need to show that $(ab)g = g(ab)$. To prove this, take any $g \in G$. Then,

$$\begin{aligned} (ab)g &= a(bg) && \text{(associativity)} \\ &= a(gb) && \text{(since } b \in Z(G)) \\ &= (ag)b && \text{(associativity)} \\ &= (ga)b && \text{(since } a \in Z(G)) \\ &= g(ab) && \text{(associativity)} \end{aligned}$$

So $ab \in Z(G)$.

Now, let $a \in Z(a)$ and take any $g \in G$. So $g^{-1} \in G$, and since $a \in Z(G)$,

$$ag^{-1} = g^{-1}a.$$

Taking the inverse of both sides gives

$$ga^{-1} = (ag^{-1})^{-1} = (g^{-1}a)^{-1} = a^{-1}g.$$

So for any $a \in Z(G)$ and any $g \in G$,

$$a^{-1}g = ga^{-1},$$

i.e. $a^{-1} \in Z(G)$. □

Example 2.2.9. If every proper subgroup of group G is abelian, is G abelian?

Proof. No. D_4 is not abelian. However, all proper subgroup are abelian.

$$\begin{aligned} &H_1 = \{R_0, R_{90}, R_{180}, R_{270}\} \\ &H_2 = \{R_0, R_{180}\} \\ &H_3 = \{R_0, D_1\} \\ &H_4 = \{R_0, D_2\} \\ &H_5 = \{R_0, V\} \\ &H_6 = \{R_0, H\} \\ &H_7 = \{R_0, D_{1,2}, H, V\} \end{aligned}$$

□

3 Special groups

3.1 Cyclic groups

So how do we find subgroups? Here's one way to construct subgroups:

Definition 3.1. *Fix an $a \in G$. Then, $\langle a \rangle = \{a^m \mid n \in \mathbb{Z}\}$*

Example 3.1.1. Consider $G = D_4$. Then, since $R_{90} \in G_4$,

$$\begin{aligned} \langle R_{90} \rangle &= \{R_{90}^{-1}, R_0, R_{90}, R_{90} \circ R_{90}, \cdots\} \\ &= \{R_0, R_{90}, R_{180}, R_{270}\}. \end{aligned}$$

Example 3.1.2. If $G = \mathbb{Z}_6$ and $2 \in G$, then

$$\begin{aligned} \langle 2 \rangle &= \{2 - 2 - 2, 2 - 2, 2, 2 + 2, 2 + 2 + 2, \dots\} \\ &= \{2, 4, 0\}. \end{aligned}$$

Theorem 3.1. *For any $a \in G$, $\langle a \rangle$ is a subgroup of G and it is the smallest subgroup of G that contains a.*

Proof. First, $e \in \langle a \rangle$ since $e = a^0$. Now, suppose that $g_1, g_2 \in \langle a \rangle$. So $g_1 = a^{n_1}$ and $g_2 = a^{n_2}$. But then,

$$g_1 g_2 = a^{n_1} a^{n_2} = a^{n_1 + n_2} \in \langle a \rangle.$$

Finally, if $a^n \in \langle$m then $(a^n)^{-1} = a^{-n} \in \langle a \rangle$. So $\langle a \rangle$ is a subgroup.

To prove that it is the smallest subgroup, consider a subgroup H with $a \in H$. Then, a^1, a^2, a^3 and a^0, a^{-1}, a^{-2} are also in H. So $\langle a \rangle \subseteq H$. □

Definition 3.2. *If G contains an element a such that $G = \langle a \rangle$, then we say G is cyclic and a is the generator.*

Example 3.1.3. $\mathbb{Z}_6$ is cyclic since $\mathbb{Z}_6 = \langle 5 \rangle$.

Definition 3.3. *If $a \in G$, then the order of a is the smallest positive integer such that $a^n = e$. We write $|a| = n$. If order is not finite, $|a| = \infty$.*

Example 3.1.4. Consider $G = \mathbb{Z}_6$. Then,

- $|3| = 2$ since $3 + 3 = 0$.
- $|5| = 6$ since $5 + 5 + 5 + 5 + 5 + 5 = 0$.

Example 3.1.5. Consider $\mathbb{Z}$ with addition. Then, $|1| = \infty$.

Example 3.1.6. Consider $\mathbb{Z}_n$ with addition. Then, $|1| = n$.

Example 3.1.7. Consider $u(8) = \{1, 3, 5, 7\}$ under multiplication. Observe that

$$\begin{aligned} |1| &= 1 \\ |3| &= 2 \\ |5| &= 2 \\ |7| &= 2 \end{aligned}$$

$u(8)$ is not cyclic because no element with $|a| = |u(8)| = 4$.

Theorem 3.2. *Every cyclic group is abelian.*

Proof. Let $g_1, g_2 \in \langle a \rangle$. So $g_1 = a^{n_1}$ and $g_2 = a^{n_2}$ for some n_1, n_2. Then,

$$g_1 g_2 = a^{n_1} a^{n_2} = a^{n_1+n_2} = a^{n_2+n_1} = a^{n_2} a^{n_1} = g_2 g_1.$$

□

Theorem 3.3. *If G is cyclic, all subgroups are cyclic.*

Proof. Let $H \subseteq G$ be a subgroup of $G = \langle a \rangle$. If $H = \{e\}$ and if $H = G$, then H is cyclic.

So assume that $\{e\} \subset H \subset G$. If $g \in H$, then $g = a^n$ for some $n \in \mathbb{Z}$. Since $g^{-1} = a^{-n}$, we know that at least one of n or $-n$ is positive.

Let M be the smallest positive integer such that $a^m \in H$. We claim that $H = \langle a^m \rangle$. If $a^m \in H$, then $\langle a^m \rangle \subseteq H$. Take $g = a^n \in H$. Then, we can divide n by m using the division algorithm, i.e.,

$$n = mq + r,$$

with $0 \leq r < m$. If $0 < r < m$, then

$$a^n = a^{mq+r} = a^{mq} a^r.$$

Since $a^{mq} \in H$, $a^{-mq} \in H$. So

$$a^n a^{-mq} = a^{n-mq} = a^r \in H.$$

However, this contradicts our assumption that m is the smallest positive exponent in H. Therefore, $r = 0$. Hence, $n = mq$, so $g = a^n = (a^m)^q \in \langle a^m \rangle$. So H is cyclic. □

Recall that the order of $a \in G$, denoted $|a|$, is smallest positive integer n such that $a^n = e$. The order of G, denoted $|G|$, is number of elements in G.

Theorem 3.4. *Let $a \in G$.*

- *If $|a| = \infty$, then $a^i = a^j$ if and only if $i = j$.*
- *If $|a| = n$, then $a^i = a^j$ if and only if $n | (i - j)$.*
- *If $|a| = n$, Then, $\langle a \rangle = \{a^0, a^1, a^2, \ldots, a^{n-1}\}$. Also, $|a| = |\langle a \rangle|$.*

Proof. (1) Because $|a| = \infty$, all elements of $\langle a \rangle$ are distinct. Indeed, if $a^i = a^j$, then $a^i a^{-j} = e$. So $a^{i-j} = e$. But $|a| = \infty$, so $a^{i-j} = e$ iff $i - j = 0$, i.e., $i = j$.

(2) Suppose that $a^i = a^j$. Without loss of generality, we can assume that $i > j$. So $a^i a^{-j} = e$. Now, we can divide $(i - j)$ by n using division algorithm, i.e.,

$$(i - j) = nq + r,$$

with $0 \leq r < n$. If $0 < r < m$, then

$$a^{i-j} = (a^n)^q a^r = a^r = e.$$

This means $a^r = e$ with $r < n$. However, this contradicts the assumption that $|a| = n$. So $r = 0$ and $n|(i-j)$. To prove the other direction, assume that $n|(i-j)$. Then, $(i-j) = nq$ and $i = nq + j$. Then,

$$a^i = a^{nq+j} = (a^n)^q a^j = a^q a^j = a^j.$$

(3) We want to show that $\langle a \rangle = \{a^0, a^1, \ldots, a^{n-1}\}$. Take $a^k \in \langle a \rangle$. Then, we divide k by n using division algorithm:

$$k = nq + r,$$

with $0 \leq r < n$. So

$$a^k = a^{nq+r} = a^r.$$

So $a^k = a^r \in \{a^0, a^1, \ldots, a^{n-1}\}$. □

Example 3.1.8. Consider

$$\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}.$$

This is a cyclic group generated by 1. So $|1| = 5$. Note that $7 \cdot 1 = 2 = 22 \cdot 1$ and $5|(22-7)$.

Corollary 3.1. *For any cyclical group $G = \langle a \rangle$, if $|a| = n$, and $a^k = e$, then $n|k$.*

Proof. Apply (2) with $i = k$ and $j = 0$. □

Theorem 3.5. *If $|a| = n$, then $|a^k| = n/\gcd(n.k)$.*

Example 3.1.9. Consider

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

Then,

$$\langle 1 \rangle = \{1, 1+1, 1+1+1, 1+1+1+1, 1+1+1+1+1, 1+1+1+1+1+1\}.$$

Then, $|1| = 6$. So

$$\langle 1 \rangle = \{1 \cdot 1, 2 \cdot 1, 3 \cdot 1, 4 \cdot 1, 5 \cdot 1, 0 \cdot 1\}.$$

So

$$|2 \cdot 1| = \frac{6}{\gcd(2,6)} = \frac{6}{2} = 3$$
$$|3 \cdot 1| = \frac{6}{\gcd(3,6)} = \frac{6}{3} = 2$$
$$|4 \cdot 1| = \frac{6}{\gcd(4,6)} = \frac{6}{2} = 3$$

Corollary 3.2. *For any $k \in \mathbb{Z}$, $\mathbb{Z}_n = \langle k \rangle$ iff $\gcd(n,k) = 1$.*

Proof. Observe that

$$k = 1 + 1 + 1 + \cdots + 1 = k \cdot 1$$

with $|1| = n$. So

$$|k| = \frac{n}{\gcd(n,k)}.$$

So $\langle k \rangle = \mathbb{Z}_n$ iff $|k| = n$ iff $n = n/\gcd(n,k)$ iff $\gcd(n,k) = 1$. □

Now, recall that $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$, and $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ are multiplicative groups. We are interested in finding finite multiplicative subgroups.

Theorem 3.6. *In $\mathbb{Q}^*$ and $\mathbb{R}^*$, there are only two finite subgroups, which are $\{1\}$ and $\{1, -1\}$.*

Proof. Take any $H \subseteq \mathbb{Q}^*$ be a subgroup with $|H| < \infty$. Let $a \in H$. Then, $a^n = 1$ for some n. So, a satisfies

$$a^n - 1 = 0 = (a-1)(a^{n-1} + a^{n-2} + \cdots + a + 1).$$

If $n = 1$, then $a = 1$. If $n = 2$, then $a^2 = 1$ so $a = \pm 1$.

If $n < 3$, a would have to take a root of

$$x^{n-1} + x^{n-2} + \cdots + x + 1 = 0,$$

or $(x - 1)$. But the former equation does not have real or rational roots. So $a = 1$.

Therefore, $H = \{1\}$ or $H = \{-1, 1\}$. □

Recall the following properties of complex numbers:

- $(a + bi)(c + di) = (ac - bd) + (ad + bc)i$.
- $|a + bi| = \sqrt{a^2 + b^2}$.
- $(a + bi)^{-1} = (a - bi)/(a^2 + b^2)$.

We can represent complex numbers using polar coordinates:

$$a + bi = z = |z|(\cos\theta + i\sin\theta),$$

and we denote it by $r\text{cis}\theta$. It is convenient to use polar coordinates due to the following property:

Theorem 3.7. *If $z_1 = r_1\text{cis}\theta_1$ and $_2 = r_2\text{cis}\theta_2$. Then,*

$$z_1 z_2 = r_1 r_2(\text{cis}(\theta_1 + \theta_2))$$
$$z_1^{-1} = r^{-1}\text{cis}(-\theta)$$

Definition 3.4 (Circle subgroup)**.**

$$\mathbb{T} = \{z \in \mathbb{C}^* \mid |z| = 1\}$$

is a subgroup.

Proof.

- (identity) $1 \in \mathbb{T}$ since $|1| = 1$.
- (closure) Suppose $z_1, z_2 \in \mathbb{T}$. So $z_1 = 1\text{cis}\theta_1$ and $z_2 = 1\cos\theta_2$. So $z_1 z_2 = 1 \cdot 1\text{cis}(\theta_1 + \theta_2) \in \mathbb{T}$.
- (inverse) If $z = 1\text{cis}\theta \in \mathbb{T}$, then $z^{-1} = 1\text{cis}(-\theta) \in \mathbb{T}$.

□

Definition 3.5. *Fix $n \geq 1$. The complex numbers that satisfy $x^n - 1 = 0$ are called n-th root of unity.*

Remark. $x^n - 1$ has n roots (up to multiplicity) in $\mathbb{C}$.

Example 3.1.10. Consider $n = 3$,

$$x^3 - 1 = 0.$$

Roots are $1, w, w^2, \ldots,$ where

$$w = \frac{-1 + \sqrt{3}i}{2}, w^2 = \frac{-1 - \sqrt{3}i}{2}.$$

Theorem 3.8. *The set of n-th root of unity form a cyclic group of order n in $\mathbb{C}^*$. Furthermore, the n-th root of unity are*

$$z = \text{cis}\left(\frac{2k\pi}{n}\right),$$

for $k = 0, 1, 2, \ldots, n-1$.

Definition 3.6. *A generator of the n-th group of units is called a primitive n-th root.*

Example 3.1.11. If $n = 8$, primitive roots are

$$w, w^3, w^5, w^7,$$

and the rest are non-primitive roots.

Example 3.1.12. Find all cyclic subgroups of $\mathbb{Z}_8$.

$$\begin{aligned}
&\langle 0 \rangle = \{0\} \\
&\langle 1 \rangle = \langle 3 \rangle = \langle 5 \rangle = \langle 7 \rangle = \mathbb{Z}_8 \\
&\langle 4 \rangle = \{0, 4\} \\
&\langle 2 \rangle = \langle 6 \rangle = \{0, 2, 4, 6\}
\end{aligned}$$

Example 3.1.13. Find all cyclic subgroups of $u(9)$.

$$\begin{aligned}\langle 1\rangle &= \{1\}\\ \langle 2\rangle &= u(9) = \langle 5\rangle\\ \langle 4\rangle &= \{4,7,1\} = \langle 7\rangle\\ \langle 8\rangle &= \{1,8\}.\end{aligned}$$

Example 3.1.14. Prove that the order of every element in a cyclic group 6 divides $|6|$.

Example 3.1.15. Suppose $|6| = p$, a prime and G cyclic. Show that every nonidentity element has order p.

3.2 Permutation groups

Definition 3.7. *A permutation of a set X is a bijection:*

$$\sigma : X \to X$$

Definition 3.8. *A permutation group of a set X is the set of all permutations of X with binary operation composition of functions.*

Example 3.2.1. Consider

$$X = \{1,2,3,4,5\}$$

Then, given

$$\begin{aligned}\sigma : X &\to X\\ 1 &\to 1\\ 2 &\to 3\\ 3 &\to 4\\ 4 &\to 2\\ 5 &\to 5\end{aligned}$$

and

$$\begin{aligned}\tau : X &\to X\\ 1 &\to 2\\ 2 &\to 3\\ 3 &\to 1\\ 4 &\to 5\\ 5 &\to 4\end{aligned},$$

we have

$$\begin{aligned}\sigma \cdot \tau : X &\to X \\ 1 &\to 3 \\ 2 &\to 4 \\ 3 &\to 1 \\ 4 &\to 5 \\ 5 &\to 2\end{aligned}$$

To avoid writing like this, we introduce a better notation:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 2 & 5 \end{pmatrix}, \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}.$$

Then,

$$\sigma \cdot \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 2 & 5 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix}$$

Likewise,

$$\tau \cdot \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 3 & 4 \end{pmatrix}$$

Note that $\sigma \cdot \tau \neq \tau \cdot \sigma$. In general, a permutation group is not abelian.

Definition 3.9. *Fix an integer $n \geq 1$. The symmetric group on n letters, denoted S_n, is the set of all permuatations of $\{1, 2, 3, \ldots, n\}$.*

Theorem 3.9. *S_n is a non-abelian group (if $n \geq 3$).*

Proof.

- S_n has an identity
$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 1 & 2 & 3 & \cdots & n \end{pmatrix}$$
- Each elment has an inverse (reverse the map the permutation)
- Composition is associative

□

Remark. Note that there are $n!$ permutations.

Example 3.2.2.

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right.$$
$$\left. \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}$$

Now, we introduce a cyclic notation. Consider

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 3 & 6 & 2 & 5 \end{pmatrix}$$

Note that 1 and 3 map to themselves whereas we have

$$2 \to 4 \to 6 \to 5.$$

So we write

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 3 & 6 & 2 & 5 \end{pmatrix} = (2465),$$

which means that

- each element is mapped to the one to right
- the last element is mapped to the front
- elements that do not appear are apped to themselves

Example 3.2.3.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 6 & 5 & 3 \end{pmatrix} = (12)(346)$$

Example 3.2.4.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 2 & 1 & 3 & 5 & 6 \end{pmatrix} = (143) = (314) = (431)$$

Definition 3.10. *A permutation of form $(a_1, a_2, \ldots, a_k)$ is called a k-cycle.*

Theorem 3.10. *If two cycles, σ and τ, are disjoint cycles, (i.e., they don't share any common values), then $\sigma \cdot \tau = \tau \cdot \sigma$.*

Proof. Let $\sigma = (a_1, \ldots, a_k)$ and $\tau = (b_1, \ldots, b_l)$. We know that

$$\sigma \cap \tau = \varnothing.$$

Then,

- if $x \in \{1, 2, \ldots, n\}$ but $x \notin \sigma \cup \tau$, then $\sigma(x) = x$ and $\tau(x) = x$ so $\sigma(\tau(x)) = x = \tau(\sigma(x))$.
- suppose $x \in \sigma$ so $x = a_i$ for some i and $x \notin \tau$. Now, $\sigma(x) = \sigma(a_i) = a_{i+1}$. Also, $\tau(x) = x$ and $\tau(a_{i+1}) = a_{i+1}$. So

  $$\sigma(\tau(a_i)) = \sigma(a_i) = a_{i+1} = \tau(a_{i+1}) = \tau(\sigma(a_i))$$

□

Example 3.2.5.

$$(12)(346) = (346)(12)$$

Remark. Not every permutation can be expressed as a cycle

Theorem 3.11. *Every permutation can be expressed as a product of disjoint cycles.*

We will illustrate this with an example, rather than a proof. Consider

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 7 & 5 & 2 & 1 & 8 & 4 & 6 \end{pmatrix}$$

We start with an element that is not mapped to itself, i.e.,

$$1 \to 3 \to 5 \implies (135)$$

Now, take another element not in previous step and is not mapped to itself

$$2 \to 7 \to 4 \implies (274)$$

We can do the same thing for the rest and get

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 7 & 5 & 2 & 1 & 8 & 4 & 6 \end{pmatrix} = (135)(274)(68)$$

The advantangeof doing this is that it's easy to compute the order of σ.

Theorem 3.12. *Suppose $\sigma = \sigma_1\sigma_2 \dots \sigma_t$ is a product of t disjoint cycles. Then,*

$$|\sigma| = \operatorname{lcm}(|\sigma_1|, |\sigma_2|, \dots, |\sigma_t|)$$

Remark. If $\sigma = (a_1a_2a_3 \cdots a_k)$ is a k-cycle, $|\sigma| = k$.

Proof. Let $d_i = |\sigma_i|$ and $d = \operatorname{lcm}(d_1, \dots, d_t)$. Since the cycles are disjoint,

$$\sigma^d = (\sigma_1 \cdots \sigma_t)^d = \sigma_1^d \sigma_2^d \cdots \sigma_t^d$$

For each i, $d = d_i m_i$ for some m_i. So

$$\begin{aligned} \sigma^d &= \sigma_1^{d_1m_1}\sigma_2^{d_2m_2} \cdots \sigma_t^{d_tm_t} \\ &= \left(\sigma_1^{d_1}\right)^{m_1} \left(\sigma_2^{d_2}\right)^{m_2} \cdots \left(\sigma_t^{d_t}\right)^{m_t} \\ &= e^{m_1}e^{m_2} \cdots e^{m_t} \\ &= e \end{aligned}$$

So $|\sigma| \leq d$.

Now, let $l = |\sigma|$. So

$$e = \sigma^l = (\sigma_1\sigma_2 \cdots \sigma_t)^l = \sigma_1^l \cdots \sigma_t^l$$

Since the cycles are disjoint, this implies that

$$\sigma_i^l = e$$

for each i. Since $|\sigma_i| = d_i$, we have that $d_i|l$ for all i. So l is a common multiple of $d_1, d_2, \ldots, d_t$. So

$$\operatorname{lcm}(d_1, \ldots d_t) \leq l.$$

Thus,

$$|\sigma| \leq d = \operatorname{lcm}(d_1, d_2, \ldots, d_t) \leq l = |\sigma|.$$

Hence, $|\sigma| = \operatorname{lcm}(d_1, \ldots, d_t)$. □

Example 3.2.6. Going back to the example, since

$$\sigma = (135)(274)(68),$$

we get

$$|\sigma| = \operatorname{lcm}(3, 3, 2) = 6.$$

Definition 3.11. *A 2-cycle is called a transposition.*

Example 3.2.7. Consider the cycle (1423). We can write it as a product of transpoistions:

$$(1423) = (13)(12)(14)$$

Theorem 3.13. *Every permutation can be expressed as a product of transpositions.*

Proof. We only need to verify this for cycles. Consider

$$(a_1a_2 \cdots a_k) = (a_1a_k)(a_1a_{k-1})(a_1a_{k-2}) \cdots (a-1a_3)(a_1a_2)$$

□

Example 3.2.8.

$$\begin{aligned} \sigma &= (135)(247)(68) \\ &= (15)(13)(27)(24)(68) \end{aligned}$$

Remark. Factorization in the transposition is not unique.

Example 3.2.9.

$$\begin{aligned} (123) &= (13)(12) \\ &= (13)(23)(12)(13) \\ (1235) &= (15)(13)(12) \\ &= (13)(24)(35)(14)(24) \end{aligned}$$

Observe that (123) is a product of an even number of transpoisitions whereas (1235) is a product of an odd number of transpositions. So we want to make this into a theorem but we need to prove a lemma first:

Lemma 3.1. *If $(id) = e = \sigma_1\sigma_2 \cdots \sigma_t$, then t is even.*

Proof. Since no transposition is the identity, we must have $t > 1$. If $t = 2$, we are done. We can perform induction on t.

e have the following 4 cases for $\sigma_{t-1}\sigma_t$:

	$\sigma_{t-1}\sigma_t$	$=$	$\sigma'_{t-1}\sigma'_t$
1	$(ab)(ab)$		e
2	$(bc)(ab)$		$(ac)(bc)$
3	$(cd)(ab)$		$(ab)(cd)$
4	$(ac)(ab)$		$(ab)(bc)$

In case 1,since $(ab)(ba) = e$, weremove$\sigma_{t-1}\sigma_t$ from $e = \sigma_1 \cdots \sigma_{t-2}$, and byinducting $t-2$ is even, so t is even.

In cases 2, 3 and 4, we can replace $\sigma_{t-1}\sigma_t$ with $\sigma'_{t-1}\sigma'_t$. Inall cases, the last occurence of a moves left by 1.

Now, we look at $\sigma_{t-2}\sigma_{t-1}$.Ifin case 1,remove the pair $\sigma_{t-2}\sigma_{t-1}$ and finish by inducting. Else, use cases 2, 3 and 4 to move left one transpositions.Weeventually get into case 1. If not, we end with

$$(id) = (ab')\sigma_2\sigma_3 \cdots \sigma_t,$$

but the right hand side sends a to b', contraidicting the fact that this is identity. □

Theorem 3.14. *No permutation can be expressed as both of odd number of transpositions and event number of transpositions*

Proof. Suppose

$$\sigma = \sigma_1 \cdots \sigma_t = \tau_1 \cdots \tau_l$$

with t even and l odd. Then,

$$\begin{aligned}(id) = \sigma\left(\sigma^{-1}\right) &= (\sigma_1 \cdots \sigma_t)(\tau_1 \cdots \tau_l)^{-1} \\ &= \sigma_1 \cdots \sigma_t \tau_1^{-1} \cdots \tau_l^{-1} \\ &= \sigma_1 \cdots \sigma_t \tau_1 \cdots \tau_l\end{aligned}$$

So (id) is a product of $t+l$ transpositions. But this is odd, so a contradiction to the lemma. □

Definition 3.12. *A permutation of $\sigma \in S_n$ is even if it can be written as an even number of transpositions and odd if it can be written as an odd number of transpositions.*

3.3 Alternating groups

Definition 3.13. *The alternating group A_n is*

$$A_n = \{\sigma \in S_n \mid \sigma \textit{ is even}\}.$$

Theorem 3.15. *A_n is a group and a subgroup of S_n.*

Proof. To prove closure, let $\sigma, \tau \in A_n$. So

$$\sigma = \sigma_1 \cdots \sigma_t$$

and

$$\tau = \tau_1 \cdots \tau_l$$

with t, l even. But then

$$\sigma\tau = \sigma_1 \cdots \sigma_t \tau_1 \cdots \tau_l \in A_n$$

since $t + l$ is even. Also, $(id) \in A_n$ by the lemma above.

Finally, if $\sigma \in A_n$ and $\sigma = \sigma_1 \cdots \sigma_t$ with t even, then

$$\begin{aligned} \sigma^{-1} &= (\sigma_1 \cdots \sigma_t)^{-1} \\ &= \sigma_t^{-1} \cdots \sigma_1^{-1} \\ &= \sigma_t \cdots \sigma_1 \in A_n \end{aligned}$$

□

3.4 Group of rigid motions

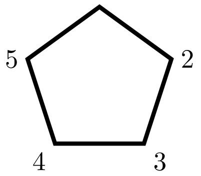
Recall that D_4 is a set of all rigid motions of the square. We can now think of the rotations as permutations

$$\begin{aligned} R_0 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \\ R_{90} &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \\ R_{180} &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \\ &\vdots \\ D &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \end{aligned}$$

In fact, we can apply this for any regular polygons:

Definition 3.14. *D_n is the group of rigid motions of the regular n-gon.*

Note that we are going to write vertices in clockwise fashion:



A rigid motion is determined by 2 pieces of information:

- where 1 is sent to (n choices)
- do the numbers go clockwise or counter clockwise (2 choices)

So the total number of rigid motions is $2n$.

Theorem 3.16. *D_n is a group of order $2n$.*

Proof. We already showed that $|D_n| = 2n$. We want to show that it's actually a group:

- Clearly, $e \in D_n$ since this is the motion where we leave unchanged.
- If $\sigma, \tau \in D_n$, they are both rigid motion, but so it $\sigma\tau \in D_n$.
- If $\sigma \in D_n$ is a rigid motion, we can always reverse the motion to back the original configuration. So $\sigma^{-1} \in D_n$.

□

Remark. D_n is a subgroup of S_n.

Example 3.4.1. $D_3 = S_3$

We saw that D_4 is not cyclic. In general, D_n is not cyclic. However, D_n can be generated by 2 elements.

Theorem 3.17. *For $n \geq 3$, D_n consists of all products of elements r and s such that rotation, r, and reflection, s, satisfy*

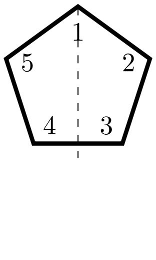
$$r^n = 1 \text{ and } s^n = 1,$$

Proof. Notice that any rigid motion is a rotation and/or a reflection.

Let $r = \frac{2\pi}{n}$. Then, there are n rotations:

$$(id), r, r^2 = 2\left(\frac{2\pi}{n}\right), r^3 = 3\left(\frac{2\pi}{n}\right), \ldots, r^{n-1}(n-1)\left(\frac{2\pi}{n}\right)$$

Likewise, there are n reflections $s_1, s_2, s_3, \ldots, s_n$, where each s_i leaves i fixed. For example, s_1 in D_5 will look like this:



If n is odd, s_i only fixes i, whereas if n is even, s_i fixes two or no elements (e.g., reflection of a square along the vertical axis fix no elements).

Let $s = s_1$. I claim that every element of D_n can be written in terms of r and s. Recall that a rigid motion is determined by (1) where 1 is sent and (2) whether numbers are clockwise or counter clockwise. If 1 is sent to k clockwise, the motion is given by r^{k-1}. If 1 is sent to k in counter clockwise, the motion is given by $r^{k-1}s$. So

$$D_n = \{r^a s^b \mid D \leq a \leq n-1, 0 \leq b \leq 1\}.$$

Finally, consider $rsrs$. Then, $rsrs = 1$ so $r(srs) = 1$ and $r^{-1} = srs$. □

Example 3.4.2. Show D_n is not abelian for all $n \geq 3$.

Proof. Suppose that D_n is abelian. We showed that $rsrs = 1$. Since D_n is abelian, $rs^2r = 1$. But $s^2 = 1$. So $r^2 = 1$. But $n \geq 3$ and $|r| = 3 > 2$. □

Example 3.4.3. Use cycle notation to write out all elements of D_5.

3.5 Lagrange's Theorem

Definition 3.15. *Let G be a group with subgroup $H \subseteq G$. The left coset of H with representative $g \in G$ is the set*

$$gH = \{gh \,|\, h \in H\}.$$

The right coset of H is

$$Hg = \{hg \,|\, h \in H\}.$$

Example 3.5.1. Consider

$$\begin{cases} G = u(8) = \{1, 3, 5, 7\} \\ H = \{1, 5\} \subseteq G \end{cases}$$

Then,

$$\begin{aligned} 1H &= \{1, 5\} \\ 3H &= \{3, 7\} \\ 5H &= \{5, 1\} \\ 7H &= \{7, 3\} \end{aligned}$$

Example 3.5.2. Consider

$$\begin{cases} G = \mathbb{Z}_8 = \{0, 1, 2, 3, \ldots, 7\} \\ H = \{0, 4\} \subseteq G \end{cases}$$

Then,

$$\begin{aligned}
0 + H &= \{0, 4\} \\
1 + H &= \{1, 5\} \\
2 + H &= \{2, 6\} \\
&\vdots \\
7 + H &= \{7, 3\}
\end{aligned}$$

Remark. If G is abelian, then left and right cosets are same, i.e.

$$gH = \{gh \,|\, h \in H\} = \{gh \,|\, h \in H\} = Hg.$$

This is false if G is not abelian.

Example 3.5.3. Consider $G = D_4$ and $T = \{R_0, H\}$, where H is the horizontal flip. Then,

$$R_{90}T = \{R_{90} \circ R_0, R_{90} \circ H\} \neq \{R_0 \circ R_{90}, H \circ R_{90}\} = TR_{90}$$

Lemma 3.2 (Properties of cosets)**.** *Let $H \subseteq G$ be a subgroup. Then,*

- $g \in gH$.
- $gH = H$ *iff* $g \in H$.
- $g_1H = g_2H$ *iff* $g_1 \in g_2H$.
- $g_1H = g_2H$ *or* $g_1H \cap g_2H = \varnothing$.
- $g_1H = g_2H$ *iff* $g_1^{-1}g_2 \in H$.
- $|g_1H| = |g_2H|$.
- $|gH| = |Hg|$

Proof.

(1) Since $e \in H$, $ge = g \in gH$.

(2) ($\Rightarrow$) Suppose $gH = H$. Since $g \in gH$, $g \in H$ because $H = gH$. ($\Leftarrow$) Now we want to show that gH given $g \in H$. Since $g \in H$, and H is a subgroup, $gh \in H$ for all $h \in H$. So $gh \subseteq H$. Now, we take $h \in H$. Because $g \in H$, $g^{-1} \in H$, and so is $g^{-1}h$. But then

$$h = g(g^{-1}h) \in gH.$$

Thus, $H \subseteq gH$. So $H = gH$.

(3) ($\Rightarrow$) Suppose $g_1H = g_2H$. Since $g_1 \in g_1H$, this implies that $g_1 \in g_2H$. ($\Leftarrow$) Take $t \in g_1H$ so g_1h for some h. And we are given that $g_1 \in g_2H$, so $g_1 = g_2h'$ for some h'. Then, $t = g_h = (g_2h)h' = g_2(hh') \in g_2H$. So $g_1H \subseteq g_2H$. Now, take $t \in g_2H$ so t_2h and sw know $g_1(h')^{-1} = g_2$. So

$$\begin{aligned}
t = g_2h &= \left(g_1(h')^{-1}\right) h \\
&= g_1[(h')^{-1}h] \in g_1H.
\end{aligned}$$

So $g_2H \subseteq g_1H$. Hence, $g_1H = g_2H$.

(4) Since g_1H and g_2H are sets, we can have (a) $g_1H \cap g_2H = \varnothing$, (b) $g_1H = g_2H$, or (c) $g_1H \neq g_2H$ and $g_1H \cap g_2H$. Suppose $x \in g_1H \cap g_2H$. So $x \in g_1H$ implies that $g_1H = xH$. Also, $x \in g_2H$ implies that $g_2H = xH$. So $g_1H = xH = g_2H$. So $g_1H = g_2H$. So (c) cannot happen.

(5) Details are same as the proof of **(3)**

(6) Define a map

$$f\,:\,g_1H \to g_2H$$

by $f(g_1h) = g_2h$. I claim that f is a bijection.

(one-to-one) If $f(g,h) = f(g,h')$, we have $g_2h = g_2h'$. By cancellation, $h = h'$ so $g_1h = g_1h'$.

(onto) Take $t = g_2h \in g_2H$. Then, $g_1h \in g_1H$ and $f(g_1h) = g_2h_2 = t$. Since f is a bijection,

$$|g_1H| = |g_2H|$$

(7) Same idea but we use a map

$$f\,:\,gH \to Hg$$

by $f(gh) = hg$. □

Theorem 3.18 (Lagrange's Theorem)**.** *If G is a finite group and $H \subseteq G$ is a subgroup, then, $|H|\big||G|$. Also, the number of distincts cosets is $\frac{|G|}{|H|}$.*

Proof. Suppose that there are a distinct left cosets of H in G, say $g_1H, g_2H, \ldots, g_nH$. For each $g \in G$,

$$g \in gH = g_iH$$

for some g_i. Thusm,

$$G = g_1H \cup g_2H \cup \cdots \cup g_nH.$$

Since cosets are distinct,

$$\begin{aligned}|G| &= |g_1H| + |g_2H| + |g_3H| + \cdots + |g_nH| \\ &= |H| + |H| + \cdots |H| \\ &= n|H|\end{aligned}$$

So $|H|\big||G|$ and $\frac{n=|G|}{|H|}$ is the number of distinct cosets. □

Definition 3.16. *The index of H in G is the number of distinct left cosets and denoted $[G : H]$. So $[G : H] = \frac{|G|}{|H|}$.*

Example 3.5.4. Consider

$$\begin{cases} G = u(8) = \{1,3,5,7\} \\ H = \{1,5\} \subseteq G \end{cases}$$

Then, $[G : H] = 4/2 = 2$.

Note that Lagrange is not true if $|G| = \infty$.

Example 3.5.5. Consider $G = \mathbb{Z}$ and $H = \{2n \mid n \in \mathbb{Z}\}21$, the set of even integers. Then, there are only two distinct left cosets: $0 + H = H$ and $1 + H$. So $[G : H] = 2$. However,

$$\frac{|G|}{|H|} = \frac{\infty}{\infty}.$$

Corollary 3.3. *For any $g \in G$ (G finite), then $|g|\big||G|$.*

Proof. For any $g \in G$, $|g| = |\langle g \rangle|$. Since $\langle g \rangle$ is a subgroup of G, $|g|\big||G|$. □

Corollary 3.4. *If $|G| = p$ is a prime, then G must be cyclic and is generated by any non-identity element.*

Proof. Let $g \in G$ with $g \neq e$. Then, $1 < |g|\big||G| = p$ so $|g| = p$, i.e. $\langle g \rangle = G$. □

Roughly this says all cyclic cyclic groups of order p are the same as $\mathbb{Z}_p$.

Corollary 3.5. *Let H and K be subgroup of G such that $K \subset H \subset G$. Then,*

$$[G : K] = [G : H][H : K]$$

Proof.

$$[G : K] = \frac{|G|}{|K|} = \frac{|G|}{|H|} \times \frac{|H|}{|K|} = [G : H][H : K]$$

□

Note that the converse of Lagrange's theorem is false, i.e. if $d\big||G|$, then G has a subgroup of order d.

Example 3.5.6. Consider an altenatring group A_4. Then,

$$|A_4| = 4!/2 = 12$$

Note that $6|12$, but we will show that A_4 has no subgroup of order 6.

Suppose $H \subseteq A_4$ was a subgroup of order t. So $[A_4 : H] = 12/6$. For all $g \in A_4$, $gH = Hg$. So

1. if $g \in H$, then $gH = H = Hg$
2. if $g \notin H$, then $gH \neq H$.

Since $[A_4 : H] = 2$, this means $A_4 = H \cup gH$ but we also would have $Hg \neq H$ and $A_4 = H \cup Hg/$ Thus,

$$H \cup gH = H \cup Hg \implies gH = Hg,$$

since those unions are disjoint. So

$$gHg^{-1} = H,$$

for all $g \in A_4$.

Note that the group A_4 has 8 three cycles:

$$(123), (132), (124), (142), (134), (143), (234), (243).$$

So H has at least one of three cycles, say $(123) \in H$. This implies that $(123)^{-1} = (132) \in H$. Then,

$$(124)(123)(124)^{-1} = (243) \in H, (243)(123)(243)^{-1} \quad = (142) \in H,$$

But then H has at least 7 elements:

$$(id), (123), (132), (243), (243)^{-1}, (142), (142)^{-1}$$

But $|14| = 6$. So H does not exist.

4 Fermat's little theorem

4.1 Fermat's little theorem

Definition 4.1. *Euler's ϕ-function $\phi : \mathbb{N} \to \mathbb{N}$ is defined as*

$$\begin{aligned}&\phi(1) = 1\\ &\phi(n) = \{m \mid 1 \leq m < n, \gcd(m,n) = 1\} = |U(n)|.\end{aligned}$$

Theorem 4.1. *Let a and n be integers with $n > 1$ and $\gcd(a,n) = 1$. Then,*

$$a^{\phi(n)} \equiv \mod n$$

Proof. Since $\gcd(a,n) = 1$, this means that $a \in U(n)$. Then, $|a|\big|U(n)| = \phi(n)$. So

$$\phi(n) = |a|l$$

and

$$a^{\phi(n)} = a^{|a|l} = \left(a^{|a|}\right)^l = 1$$

in $U(n)$. As a result,

$$a^{\phi(n)} \equiv 1 \mod n.$$

□

Theorem 4.2. *Let p be prime. Then, for all integers a,*

$$a^p = a \mod p$$

Proof. If $p|a$, then $a^p \equiv a \mod p$. If $p \not| a$, then $\gcd(a,p) = 1$. By Euler's Theorem,

$$a^{\phi(p)} \equiv 1 \mod p.$$

But p prime means $\phi(p) = p - 1$. So

$$a^{p-1} \equiv 1 \mod p \implies a^p \equiv a \mod p.$$

□

Example 4.1.1. Consider $a = 32$ and $p = 7$. Then,

$$32^7 \equiv 32 \mod 7.$$

This is extremely useful for modular computation.

5 Isomorphisms

5.1 Isomorphisms

Informally, two sets are isomorphic if they are the same, but just have different labels.

Definition 5.1. *Let G and H be groups with operations $*$ and $\circ$, respectively. Then, G is isomorphic to H if there is a bijection $\phi : G \to H$ that preserves the operation, i.e.,*

$$\phi(a * b) = \phi(a) \circ (\phi b),$$

where $*$ is an operation in G and $\circ$ is an operation in H. Then, we write $G \simeq H$.

Example 5.1.1. Consider

$$G = u(8) = \{1, 3, 5, 7\}$$
$$H = u(12) = \{1, 5, 7, 11\}$$

Prove that $u(8) \simeq u(12)$.

Define our map $\phi : u(8) \to u(12)$ by

$$1 \to 1$$
$$3 \to 5$$
$$5 \to 7$$
$$7 \to 11$$

This is a bijection. To check the operation is preserved, we can compare cayley tables:

	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

	1	3	5	7
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

5.2 Cyclic groups

Theorem 5.1. *(A) Every infinite cyclic group is isomorphic to $\mathbb{Z}$. (B) Every finite cyclic group G with $|G| = n$ is isomorphic to $\mathbb{Z}_n$.*

Proof. (A) Let $G = \langle a \rangle = \{a^i \mid i \in \mathbb{Z}\}$. Define a map $\phi : \mathbb{Z} \to G$ by $\phi(i) = a^i$. Then this is a bijection:

- (onto) For any $g \in G$, $g = a^i$ for some $i \in \mathbb{Z}$. Then, $\phi(i) = a^i = g$.
- (one-to-one) Suppose that $\phi(k_1) = a^{k_1} = a^{k_2} = \phi(k_2)$. Since G is infinite, $k_1 = k_2$. So ϕ is one-to-one.

Let $i, j \in \mathbb{Z}$. Then,

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

(B) We are given that $G = \{a^0, a^1, \ldots, a^{n-1}\} = \langle a \rangle$. Define

$$\phi : \mathbb{Z}_n \to G$$

by $\phi(i) = a^i$. This is clearly a bijection. Given $i, j \in \mathbb{Z}_n$, suppose $i+j = k \in \mathbb{Z}_n$. Then,

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

□

Theorem 5.2 (Properties of isomorphisms)**.** *If $\phi : G \to H$ is an isomorphism, then*

1. $\phi(e_G) = e_H$.
2. $\phi(g)^{-1} = \phi(g^{-1})$
3. $|G| = |H|$
4. *If G is abelian, so is H*
5. *If G is cyclic, then so is H*
6. *If G has a subgroup of order m, then so does H*
7. *For all $g \in G$, $|g| = |\phi(g)|$*

Proof. **(1)** We know $e_G e_G = e_G$. So $\phi(e_G) = \phi(e_G e_G) = \phi(e_G)\phi(e_G)$. Then,

$$e_H \phi(e_G) = \phi(e_G)\phi(e_G).$$

By the cancellation property, $e_H = \phi(e_G)$.

(2) Observe that

$$e_H = \phi(e_G) = \phi(gg^{-1}) = \phi(g)\phi(g^{-1}).$$

Since inverses are unique, $\phi(g)^{-1} = \phi(g^{-1})$.

(3) Since ϕ is a bijection, $|G| = |H|$.

(4) Let $h_1, h_2 \in H$. Then,

$$\begin{aligned} h_1 h_2 &= \phi(g_1)\phi(g_2) \\ &= \phi(g_1 g_2) \\ &= \phi(g_2 g_1) \\ &= \phi(g_2)\phi(g_1) = h_2 h_1 \end{aligned}$$

(5) Same type of proof

(6) Homework

(7) Let $a = |g|$, i.e. $g^a = e_G$. Then,

$$e_H = \phi(e_G) = \phi(g^a) = \phi(g) \cdots \phi(g) = \phi(g)^a$$

So $b = |\phi(g)| \leq a$.

Now, let $b = |\phi(g)|$. So

$$\phi(g)^b = \phi(g \cdots g) = \phi(g^b) = e_H = \phi(e_G).$$

Since ϕ is one-to-one and $g^b = e_G$, so $a \leq b$. Therefore, $a \leq b \leq a$. So $a = b$. □

Example 5.2.1. D_4 and $\mathbb{Z}_8$ are not isomorphic because $\mathbb{Z}_4$ is cyclic whereas D_4 is not.

Example 5.2.2. $u(8)$ and $\mathbb{Z}_4$ are not isomorphic because $|1| = 4$ in $\mathbb{Z}_4$ but every element has order to in $u(8)$.

Example 5.2.3. Let G be any finite group of order p (prime). Then, $G \simeq \mathbb{Z}_p$ because G is cyclic with order p.

Fundamental problem of finite group theory. Classify all finite groups up to isomorphism (memorize this table):

n	all groups of order n up to isomorphism
1	$\{e\}$
2	$\mathbb{Z}_2$
3	$\mathbb{Z}_3$
4	$\mathbb{Z}_4$, $u(8) = \mathbb{Z}_2 \times \mathbb{Z}_2$
5	$\mathbb{Z}_5$
6	$\mathbb{Z}_6$, S_3
7	$\mathbb{Z}_7$

5.3 Cayley's Theorem

Theorem 5.3. *Every group is isomorphism to a group of permutations.*

Example 5.3.1. Consider

$$U(8) = \{1, 3, 5, 7\}.$$

For each $g \in U(8)$, we acn define a bijection

$$\lambda_g : U(8) \to U(8)$$

by letting $\lambda_g(x) = gx$. So λ_3 is defined by $\lambda_3(x) = 3x$:

$$\begin{aligned} 1 &\to 3 \cdot 1 = 3 \\ 3 &\to 3 \cdot 3 = 1 \\ 5 &\to 3 \cdot 5 = 7 \\ 7 &\to 3 \cdot 7 = 5 \end{aligned}$$

So we can write λ_3 as a permutation:

$$\begin{pmatrix} 1 & 3 & 5 & 7 \\ 3 & 1 & 7 & 5 \end{pmatrix}$$

Likewise,

$$\lambda_1 = \begin{pmatrix} 1 & 3 & 5 & 7 \\ 1 & 3 & 5 & 7 \end{pmatrix}, \lambda_5 = \begin{pmatrix} 1 & 3 & 5 & 7 \\ 5 & 7 & 1 & 3 \end{pmatrix}, \lambda_7 = \begin{pmatrix} 1 & 3 & 5 & 7 \\ 7 & 5 & 3 & 1 \end{pmatrix}$$

Example 5.3.2. Let $\bar{U}(8) = \{\lambda_1, \lambda_3, \lambda_5, \lambda_7\}$ as a set of bijections from $U(8)$ to itself. Then, $U(8) \simeq \bar{U}(8)$ as groups.

Proof. For each $g \in G$, define$\lambda_g : G \to G$ given by $\lambda_g = g(x)$. □

Theorem 5.4. *Each $\lambda_g : G \to G$ is a bijection, i.e., a permutation of elements of G.*

Proof. (surjective) Let $g \in G$. Since $g^{-1} \in G$, so is $g^{-1}G$. Then,

$$\lambda_g(g^{-1}G) = g(g^{-1}G) = (gg^{-1})G = G.$$

(injective) Suppose $\lambda_g(x) = gx = gy = \lambda_g(y)$. But, by cancellation, $gx = gy$ implies $x = y$. So λ_y is injective.

Therefore,

$$H = \{\lambda_g \mid g \in G\} = \bar{G}.$$

□

Theorem 5.5. *H is a subgroup of all the permutations of the elements of G under composition.*

Proof. (closed) Take $\lambda_g, \lambda_h \in H$. Then,

$$\begin{aligned} (\lambda_g \circ \lambda_h)(x) &= \lambda_g(\lambda_h(x)) \\ &= \lambda_g(hx) \\ &= ghx \end{aligned}$$

But $g, h \in G$ so $gh \in G$ and $\lambda_{gh} \in H$ and $\lambda_{gh}(x) = ghx$. So

$$(\lambda_g \lambda_h)(x) = ghx = \lambda_{gh}(x).$$

(identity) Since $e \in G$, $\lambda_e \in H$. For all $x \in G$, $\lambda_e(x) = ex = x$. So λ_e is the identity function.

(inverse) Consider $\lambda_g \in H$. Since $g \in G$, $g^{-1} \in G$, and so $\lambda_{g^{-1}} \in H$. Then, for all $x \in G$,

$$(\lambda_g \circ \lambda_{g^{-1}}) = g(g^{-1}(x)) = x = \lambda_e(x)$$

□

Theorem 5.6. $G \simeq \bar{G} = H$

Proof. Define $\phi : G \to H$ by $g \to \lambda_g$. We check that this is an isomorphism.

(surjective) If $\lambda_g \in H$, then $g \in G$, and $\phi(g) = \lambda_g$.

(injective) Suppose $\phi(g) = \lambda_g = \lambda_h = \phi(h)$. Since $e \in G$, we have

$$\lambda_g(e) = ge = he = \lambda_h(e).$$

So $g = h$ (ϕ preserves operation).

So

$$\phi(g) \circ \phi(h) = (\lambda_g \circ \lambda_h) = \lambda_{gh} = \phi(gh)$$

So $H \simeq G$, as desired. □

5.4 Direct Products

Let $(G, *)$ and $(H, \circ)$ be two groups.

Definition 5.2 (External direct product)**.** $G \times H = \{(g, h) \mid g \in G$ *and* $h \in H\}$ *is a group under the operation*

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

Example 5.4.1. Consider $\mathbb{Z}_2 = \{0, 1\}$. Then,

$$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0), (0,1), (1,0), (1,1)\}$$

Note that $|\mathbb{Z}_2 \times \mathbb{Z}_2| = 4$ but $\mathbb{Z}_2 \times \mathbb{Z}_2 \neq \mathbb{Z}_4$ since $\mathbb{Z}_2 \times \mathbb{Z}_2$ has no element of order 4.

Example 5.4.2. $\mathbb{Z}_2 \times \mathbb{Z}_3 = \{(0,0), (0,1), (0,2), (1,0), (1,1), (1,2)\}$

Theorem 5.7. *If* $(g, h) \in G \times H$ *and* $|g| = r$ *and* $|h| = s$*, then* $|(g, h)| = \operatorname{lcm}(r, s)$.

Example 5.4.3. In $\mathbb{Z}_3$, $|1| = 3$ and $\mathbb{Z}_5$, $|1| = 5$. So in $\mathbb{Z}_3 \times \mathbb{Z}_5$,

$$|(1,1)| = 15 = \operatorname{lcm}(3,5)$$

So $\mathbb{Z}_3 \times \mathbb{Z}_5 \simeq \mathbb{Z}_{15}$

Theorem 5.8. $\mathbb{Z}_n \times \mathbb{Z}_m \simeq \mathbb{Z}_{nm}$ *if and only if* $\gcd(m, n) = 1$.

Proof. ($\Rightarrow$) Suppose $\mathbb{Z}_n \times \mathbb{Z}_m \simeq \mathbb{Z}_{nm}$, but $\gcd(m, n) = d > 1$. So

$$\frac{mn}{d} = m\left(\frac{n}{d}\right) = \left(\frac{m}{d}\right)n < mn.$$

But then, for all $(a, b) \in \mathbb{Z}_n \times \mathbb{Z}_m$,

$$\underbrace{(a,b) + \cdots (a,b)}_{\frac{mn}{d}} = (an\left(\frac{m}{d}\right), bm\left(\frac{n}{d}\right)) = (0,0)$$

So every element in $\mathbb{Z}_n \times \mathbb{Z}_m$ ahs order less than mn/d but $\mathbb{Z}_{nm}$ has at least 1 element of order mn, which allows a contradiction to arise.

($\Leftarrow$) $|1| = n$ in $\mathbb{Z}_n$ and $|1| = m$ in $\mathbb{Z}_m$. Since $\gcd(m,n) = 1$ and $\operatorname{lcm}(m,n) = mn$,

$$|(1,1)| = \operatorname{lcm}(m,n) = mn,$$

i.e., $\langle(1,1)\rangle = \mathbb{Z}_{nm}$ since $|\mathbb{Z}_n \times \mathbb{Z}_m| = mn$. □

Remark. $\gcd(a,b) \cdot \operatorname{lcm}(a,b) = ab$.

Given a group G, can we find subgroups H and K such that $G = H \times K$?

Definition 5.3. *Let G be a group with two subgroups H and K. Then, G is an internal direct product of H an K if*

- $G = HK = \{hk \mid h \in H, k \in K\}$
- $H \cap K = \{e\}$
- $hk = kh$ *for all* $k \in K$ *and* $h \in H$.

Example 5.4.4. Let $G = U(8) = \{1,3,5,7\}$, $H = \{1,3\}$ and $K = \{1,5\}$. Then,

- $HK = \{1 \cdot 1, 1 \cdot 5, 3 \cdot 1, 3 \cdot 5\} = \{1,5,3,7\}$.
- $H \cap K = \{e\} = \{1\}$
- Since $U(8)$ is abelian, $hk = kh$ for all $k \in K$ and $h \in H$.

So $U(8)$ is the internal direct product of H and K.

Theorem 5.9. *If G is the internal direct product of H and K, then $G = H \times K$.*

Example 5.4.5. $U(8) = H \times K$

Proof. Observe that every $g \in G$ can be written as $g = hk$ for some $h \in H, k \in K$. So we define $\phi : G \to H \times K$, by $\phi(g) = (h,k)$. First, we need to show that ϕ is well defined. Suppose $g = h_1k_1 = h_2k_2$. Then, $h_2^{-1}h_1 = k_2k_1^{-1}$. Since $h_2^{-1}h_1 \in H$ and $k_2k_1^{-1} \in K$,

$$h_2^{-1}h_1 = k_2k_1^{-1} \in H \cap K = \{e\}.$$

So $h_1 = h_2$ and $k_1 = k_2$ so $g = hk$ is the unique ay of factoring g.

We claim that ϕ is one-to-one and onto (check this fact) so we just need to show that the operation is preserved.

$$\begin{aligned}
\phi(g_1g_2) &= \phi(h_1k_1h_2k_2) \\
&= \phi(h_1h_2k_1k_2) \\
&= (h_1h_2, k_1k_2) \\
&= (h_1,k_1)(h_2,k_2) \\
&= \phi(g_1)\phi(g_2)
\end{aligned}$$

□

Example 5.4.6. Let $T = \{2^n 3^m \mid n, m \in \mathbb{Z}\} \subseteq \mathbb{Q}$. Prove that $T \simeq \mathbb{Z} \times \mathbb{Z}$.

Proof. So we want to show that T is an internal direct product of $T_1 = \{2^n \mid n \in \mathbb{Z}\}$ and $T_2 = \{3^m \mid m \in \mathbb{Z}\}$.

- Note that $T_1 \cap T_2 = \{1\} = \{2^0\} = \{3^0\}$
- Also, note that $t_1 t_2 = t_2 t_1$ for all $t_1 \in T_1$ and $t_2 \in T_2$, since T is abelian.
- Let $t \in T$. So $t = 2^n 3^m$. But $2^n \in T_1$ and $3^m \in T_2$, so $T = T_1 T_2$.

So T is an internal direct product of T_1 and T_2. Then, we apply the previous theorem to conclude that $T \simeq T_1 \times T_2$. □

Remark. For finite groups, we can proe cancellation:

$$G \times H = G \times K \implies H = K$$

If G is not finite, this is false. Let $G = \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \cdots$. Let $H = \mathbb{Z}$ and $\mathbb{K} = \mathbb{Z} \times \mathbb{Z}$. Then, $H \times G = K \times G$ but $H \neq K$.

6 Factor groups

6.1 Factor groups

Recall that if $H \subseteq G$ is a subgroup, then we have left and right cosets: gH and Hg. Hereafter, we write $\frac{G}{H}$ to denote the set of all distinct left cosets.

Example 6.1.1. Consider $G = \mathbb{Z}_8$ and $H = \{0, 4\}$. Then,

$$\frac{G}{H} = \{0 + H, 1 + H, 2 + H, 3 + H\}$$

So $\frac{G}{H}$ is a set. Does $\frac{G}{H}$ have extra structure? In particular, is $\frac{G}{H}$ a group?

Definition 6.1. *$\frac{G}{H}$ is a factor group (or quotient group) if $\frac{G}{H}$ is a group.*

So how should an operation on $\frac{G}{H}$ be defined? Our first guess is to use

$$(aH)(bH) = (abH),$$

We have defined our operation in terms of coset representative but the problem is that there are many a' such that $aH = a'H$.

Example 6.1.2. Consider the following in $\frac{\mathbb{Z}_8}{H}$:

$$\begin{aligned}(1 + H) &= (5 + H)\\ (2 + H) &= (6 + H)\\ (1 + H) + (2 + H) &= (3 + H)\\ (5 + H) + (6 + H) &= (11 + H) = (3 + H)\end{aligned}$$

Example 6.1.3. Consider

$$\begin{aligned}&S_3 = \{(1), (12), (13), (23), (132), (123)\}\\ &N = \{(1), (12)\}\end{aligned}$$

Then,

$$\frac{S_3}{N} = \{(1)N, (123)N, (23)N\}$$

In this case, $(123)N$ and $(13)N$ are same cosets but $(123)N(23)N$ and $(13)N(23)N$ are different:

$$\begin{aligned}(123)N(23)N = (123)(23)N = (12)N\\ (13)N(23)N = (13)(23) = (132)N\end{aligned}$$

So when is $\frac{G}{H}$ a group? It depends on H. H neeeds and extra property!

Definition 6.2. *A subgroup $N \subseteq G$ is a normal subgroup if $gN = Ng$ for all $g \in G$.*

Theorem 6.1. *If G is abelian, every subgroup is normal.*

Proof. For any $g \in G$ and subgroup $N \subseteq G$,

$$gN = \{gn \mid n \in N\}$$

Since G is abelian, $gn = ng$ for all $n \in N$. Thus,

$$gN = Ng,$$

and N is normal. □

Example 6.1.4. Consider

$$N = \{(1), (12)\} \subseteq S_3.$$

Then, N is not normal since

$$(123)N \neq N(123).$$

Theorem 6.2 (Normal subgroup test)**.** *Let $N \subseteq G$ be a subgroup. Then, following are equivalent:*

1. *N is normal in G*
2. *$gNg^{-1} \subseteq N$ for all $g \in G$*
3. *$gNg^{-1} = N$ for all $g \in G$*

Proof. ($1 \implies 2$) Suppose N is normal, i.e., $gN = Ng$ for all $g \in G$. So for any $g \in G$, there exists n and $n' \in N$ such that $gn = n'g$. So, for any $g \in G$ and $n \in N$,

$$gng^{-1}n'$$

for some $n' \in N$. But this means

$$gNg^{-1} = \{gng^{-1} \mid n \in N\} \subseteq N$$

($2 \implies 3$) It suffices to show that $N \subseteq gNg^{-1}$ for $g \in G$. Let $n \in N$ and let $g \in G$. By (2),

$$(g^{-1})N(g^{-1})^{-1} \subseteq N.$$

Thus,

$$g^{-1}n(g^{-1})^{-1} \in N$$

but then

$$n = g\left(g^{-1}n(g^{-1})^{-1}\right)g^{-1} \in gNg^{-1}$$

($3 \implies 1$) We are given $gNg^{-1} = N$ for all $g \in G$. So

$$gng^{-1} = n'$$

for some $n \in N$ and $n' \in N$. Then,

$$gn = n'g.$$

So for any $g \in G, n \in N$, $gn \in gN$ is also in Ng since $ng = n'g$. So $gN \subseteq Ng$. By a similar argument $Ng \subseteq Ng$. □

Remark. $gN = Ng$ does not imply $gn = ng$ for all $g \in G$ and $n \in N$. It means that there exists n and n' such that $gn = n'g$.

Theorem 6.3. *Let G be a group with a normal subgroup N. Then,*

$$G/N = \{\textit{all distinct let cosets}\}$$

is a group where the operation is

$$(aN)(bN) = (ab)N$$

Definition 6.3. *G/N is called the factor group or quotient group.*

Proof. (Step 1) First, we show that the operation is closed and well defined. The operation is closed since $abN \in G/N$. To check for well definedness, we need to show that if $aN = a'N$ and $bN = b'N$, then

$$abN = a'b'N.$$

Let $t \in abN$, so $t = abn$. Since $bn \in bN = b'N$, there is n_2 such that

$$bn = b'bn_2.$$

Also, since N is normal,

$$b'N = Nb'.$$

So $b'n_2 = n_3b'$ for some $n_3 \in N$. Then,

$$t = abn = a(b'n_2) = a(n_3b') = (an_3)b'.$$

So $an_3 = aN = a'N$. So $an_3 = a'n_4$ for some $n_4 \in N$. Then,

$$t = (an_3)b' = (a'n_4)b' = a'(n_4b').$$

Since $n_4b' \in Nb' = b'N$, we have

$$n_4b' = b'n_5$$

for $n_5 \in N$ since N is normal. So

$$t = a'(n_4b') = a'b'n_5 \in a'b'N.$$

Thus, $abN \subseteq a'b'N$. A similar argument can be made for the other direction.

(Step 2 - identity) eN is the identity.

(Step 3 - inverse) If $gN \in G/N$, $g^{-1}N \in G/N$ and

$$(gN)(g^{-1}N) = (gg^{-1})N = eN.$$

(Step 4 - associativity) Since operations in G is associative, this operation is asociative. □

Example 6.1.5. Consier the following normal set:

$$D = \{R_0, R_{180}\} \subseteq D_4.$$

Then,

$$D_4/N = \{R_0N, R_{90}N, Hn, D_1N\},$$

where

$$\begin{aligned} R_0N &= \{R_0, R_{180}\} \\ R_{90}N &= \{R_{90}, R_{270}\} \\ HN &= \{H, V\} \\ D_1N &= \{D_1, D_2\} \end{aligned}$$

Then, we can make the following operation table:

	R_0N	$R_{90}N$	HN	D_1N
R_0N	R_0N	$R_{90}N$	HN	D_1N
$R_{90}N$	$R_{90}N$	R_0N	D_1N	HN
HN	HN	D_1N	R_0N	$R_{90}N$
D_1N	D_1N	HN	$R_{90}N$	R_0N

Note that properties of G/N are related to property of G and N.

Theorem 6.4. *Suppose $N \subseteq G$ is normal. Then, the quotient G/N is abelian if and only if $ghg^{-1}h^{-1} \in N$ for all $g, h \in G$.*

Proof. G/N is abelian if and only if

- $(gN)(hN) = (hN)(gN)$
- $ghN = (hg)N \qquad$ for all $h, g \in N$
- $(gh)(hg)^{-1} \in N$
- $(gh)(g^{-1}h^{-1}) \in N$

□

Theorem 6.5 (Cayley's theorem for finite abelian groups)**.** *Let G be a finite abelian group. If p is a prime such that $p\big||G|$, then G has an element of order p (a partial converse of Lagrange's theorem)*

Proof. If $n = 2 \simeq \mathbb{Z}_2$. Now, $2\big||G| = 2$ is the only prime that divides 2 and $\mathbb{Z}_2$ has an element of order 2.

Now, I claim that if $\frac{G}{N}$ has an element of order m and $|G| < \infty$, then G has an elemnt of order m. First, suppose that gN has order m. So

$$(gN)^m = g^mN = eN.$$

If $d = |g|$, then $(gN)^d = g^dN = eN$. This means that

$$m|d \iff d = mk.$$

But then, $|g| = mk$ implies $|g^k| = m$.

Suppose $n = |G| > 2$. Let $e \neq x \in G$ and let $|x| = qm \geqq 2$ where q is a prime. If $q = p$, then $|x^m| = p$, and we are done. If $q \neq p$, then $\langle x^m \rangle$ is a cyclic group of order q. This is normal in G since G is abelian, so

$$\bar{G} = \frac{G}{\langle x^m \rangle}$$

is a group with $|\bar{G}| = |G|/q = n/q < n$. Since $p\big||G| = n$ and $p \neq q$ and $p|n/q$, so $p\big||\bar{G}|$. By definition, $\bar{G}$ has an element of order p. By the claim, we then have G has an element of order p. □

Example 6.1.6. Observe that

$$|U(23)| = 22.$$

Since $2|22$ and $11|22$, this group has elemnts of order 2 and 11.

Example 6.1.7. Since $|U(43)| = 42 = 2 \times 3 \times 7$, $U(43)$ has an element of order $2, 3, 7$.

6.2 Simple groups

Definition 6.4. *A group G is a simple group if it does not have any non-trivial normal subgroups.*

Theorem 6.6. *If p is prime, $\mathbb{Z}_p$ is simple.*

Proof. If p is prime, the only subgroups of $Z\mathbb{Z}_p$ are the trivial subgroups. So it can't have nontrivial normal subgroups. □

Theorem 6.7. *For all $n \geq 3$, A_n is simple.*

Proof. We provide an outline of the proof instead:

1. For all $n \geq 3$, A_n is generated by 3 cycles.
2. If N is a normal subgroup in A_n with $n \geq 3$ and if N contains a 3 cycle, then $N = A_n$.
3. If $n \geq 5$, any normal subgroup $N \leq A_n$ contains a 3 cycle.

Then, steps 2 and 3 imply the theorem. □

Example 6.2.1. If $n = 3$, A_3 is also simple since $|A_3| = \frac{3!}{2} = 3$, so $A_3 \simeq \mathbb{Z}_3$.

Example 6.2.2. If $n = 4$, then A_n has a normal subgroup:

$$N = \{(1), (12)(34), (13)(24), (14)(23)\} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$$

N does not have a 3-cycle.

Remark. While A_n is simple if $n \geq 5$, S_n is never simple except if $n = 1$ or $n = 2$.

Theorem 6.8. *For all $n \geq 3$, A_3 is normal in S_n.*

Proof. We want to show that

$$\sigma A \sigma^{-1} \subseteq A_n$$

for all $\sigma \in S_n$.

If $\sigma = \sigma_1 \sigma_2 \cdots \sigma_{2l}$ is an even permutation, then so is σ^{-1}. Let $\tau = \tau_1 \cdots \tau_{2m} \in A_n$. Then, $\sigma \tau \sigma^{-1}$ consists of even number of permutations. So

$$s\sigma\tau\sigma^{-1} \in A_n.$$

If σ is odd, then $\sigma\tau\sigma^{-1}$ still consists of even number of permutations. So

$$s\sigma\tau\sigma^{-1} \in A_n.$$

□

Corollary 6.1. $\frac{S_n}{A_n} \simeq \mathbb{Z}_2$

Proof. Note that

$$\left| \frac{S_n}{A_n} \right| = \frac{|S_n|}{|A_n|} = \frac{n!}{\left(\frac{n!}{2}\right)} = 2$$

Since there is only one group with order 2, $\frac{S_n}{A_n} \simeq \mathbb{Z}_2$. □

Example 6.2.3. If G/N is abelian and N abelian, is G abelian? No, $S_3/A_3 \simeq \mathbb{Z}_2$ is abelian and $A_3 \simeq \mathbb{Z}_3$ is abelian but S_3 is not.

7 Homomorphism

7.1 Homomorphism

Definition 7.1. *Let $(G, *)$ and $(H, \circ)$ be two groups. A homomorphism is a function, $\phi : G \to H$ such that*

$$\phi(a * b) = \phi(a) \circ \phi(b),$$

for all $a, b \in G$.

Note that we drop the bijection condition of an isomorphism.

Example 7.1.1. Define a map $\phi : \mathbb{Z} \to \mathbb{Z}_n$ by

$$\phi(a) = a \mod n.$$

This is an isomorphism since

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

Example 7.1.2. Consider $\phi : \mathbb{R}^* \to \mathbb{R}^*$ defined by

$$\phi(x) = |x|.$$

This is an isomorphism because

$$\phi(ab) = |ab| = |a||b| = \phi(a)\phi(b)$$

Example 7.1.3. Consider $\phi : \mathrm{GL}_2(\mathbb{R}) \to \mathbb{R}^*$ defined by

$$\phi(A) = \det(A)$$

This is an isomorphism because

$$\begin{aligned}\phi(AB) &= \det(AB) \\ &= \det(A)\det(B) \\ &= \phi(A)\phi(B)\end{aligned}$$

Theorem 7.1. *Let $\phi : G \to H$ be any group homomorphism. Then,*

1. $\phi(e_G) = e_H$
2. $\phi(a)^n = \phi(a^n)$ *for all $n \in \mathbb{Z}$*
3. $\phi(a)^{-1} = \phi\left(a^{-1}\right)$

4. *If $N \subseteq G$ is a subgroup, then*

$$\phi(N) = \{\phi(n) \mid n \in \mathbb{N}\}$$

is a subgroup of H

5. *If K is any group of H, then*

$$\phi^{-1}(K) = \{g \in G \mid phi(g) \in K\}$$

is a subgroup of G. If K is normal, so it $\phi^{-1}(K)$.

Proof. **(1)** Note that $e_G = e_G e_G$. So

$$\phi(e_G) = \phi(e_G e_G) = \phi(e_G)\phi(e_G)$$

We multiply both sides by $\phi(e_G)^{-1}$, we have

$$e_H = \phi(e_G)^{-1}\phi(e_G) = \phi(e_G)^{-1}\phi(e_G)\phi(e_G) = \phi(e_G)$$

(2) If $n = 0$, this is just 1. So suppose $n \geq 1$:

$$\phi(a)^n = \underbrace{\phi(a) \cdots \phi(a)}_{n} = \phi(a^n)$$

by homomorphism property. If $n \leq 1$, then $-n \geq 1$ so

$$\phi(a)^{-n} = \phi(a^{-n})$$

On the other hand,

$$\phi(a)^n \left(\phi(a)^n\right)^{-1} = \phi(a)^n \phi(a)^{-n} = e_H$$

Also, since $a^n a^{-n} = e_G$, we have

$$\phi(e_G) = e_H = \phi(a^n)\phi(a^{-n}).$$

So

$$\phi(a^n)\phi(a^{-n}) = \phi(a)^n \phi(a)^{-n}$$

Finally, we can cancel $\phi(a^{-n})$ with $\phi(a)^{-n}$ to obtain

$$\phi\left(a^n\right) = \phi(a)^n.$$

(3) This is property 2 with $n = -1$.

(4) Apply the usbgroup test to

$$\phi(N) = \{\phi(n) \mid n \in \mathbb{N}\}$$

- (identity) Since $e_G \in N$, and $\phi(e_G) = e_H$, so $e_H \in \phi(N)$.

- (closure) Let $a, b \in \phi(N)$. THen,

  $$\begin{aligned} a &= \phi(n_1), \\ b &= \phi(n_2), \end{aligned}$$

  for some $n_1, n_2 \in N$. Then,

  $$ab = \phi(n_1)\phi(n_2) = \phi(n_1 n_2).$$

  But $n_1 n_2 \in N$. Since $n_1 n_2 \in N$, so $ab \in \phi(N)$.

- (inverse) Let $a \in \phi(N)$, so $a = \phi(n_1)$ for some $n_1 \in N$. Then,

  $$a^{-1} = \phi(n_1)^{-1} = \phi(n_1^{-1}).$$

  But $n_1^{-1} \in N$ since $n_1 \in N$. So $a^{-1} \in \phi(N)$.

(5) We use a subgroup test to show that

$$\phi^{-1}(K) = \{g \in G \mid \phi(a) \in K\}$$

is a subgroup.

- (identity) Since $e_H \in K$ and $\phi(e_G) = e_H$, $e_G \in \phi^{-1}(K)$.
- (closure) take $a, b \in \phi^{-1}(K)$. So $\phi(a)$ and $\phi(b) \in K$. So $\phi(a)\phi(b) \in K$ since K is closed. But since $\phi(a)\phi(b) = \phi(ab)$, we have $ab \in \phi^{-1}(k)$.
- (inverse) Take $a \in \phi^{-1}(K)$. So $\phi(a) \in K$ and $\phi(a)^{-1} = \phi(a^{-1}) \in K$. So $a^{-1} \in \phi^{-1}(K)$. Now, assume K is normal. We want to show that

  $$g\phi^{-1}(K)g^{-1} \subseteq \phi^{-1}(K).$$

  Take $t \in g\phi^{-1}(K)g^{-1}$ so $t = gag^{-1}$ with $\phi(a) \in K$. Then,

  $$\begin{aligned} \phi(t) &= \phi(gag^{1}) \\ &= \phi(g)\phi(a)\phi(g^{-1}) \\ &= \phi(g)\phi(a)\phi(g)^{-1} \in \phi(g)K\phi(g)^{-1} \subseteq K \end{aligned}$$

  Since K is normal, so it $\phi(t) \in K$ so $t \in \phi^{-1}(K)$.

□

7.2 Kernels

Definition 7.2. *If $\phi : G \to H$ is a group homomorphism, then the kernel of ϕ is*

$$\mathrm{Ker}(\phi) = \{g \in G \mid \phi(g) = e_H\}$$

Example 7.2.1. Consider

$$\phi : \mathbb{Z} \to \mathbb{Z}_n$$

given by $\phi(a) = a \mod n$. Then,

$$\mathrm{Ker}(\phi) = \{9, \pm n, \pm 2n, \dots\} = n\mathbb{Z}.$$

Theorem 7.2. *Let $\phi : G \to H$ be any group homomorphism. Then,* $\mathrm{Ker}(\phi)$ *is a normal subgroup of G.*

Proof. $\{e_H\}$ is a normal subgroup in H. So $\phi^{-1}(\{e_H\})$ is normal subgroup in G. But

$$\begin{aligned}\phi^{-1}(\{e_H\}) &= \{g \in G \mid \phi(g) \in \{e_H\} \iff \phi(g) = e_H\} \\ &= \mathrm{Ker}\phi\end{aligned}$$

□

Remark. Given $\phi : G \to H$ a group homomorphism, $\frac{G}{\mathrm{Ker}(\phi)}$ is a group also.

Theorem 7.3 (First isomorphism theorem)**.** *Let $\phi : G \to H$ be any group homomorphism with $k = \mathrm{Ker}(\phi)$ and $L = \mathrm{Im}(\phi)$. Then, $G/K = \mathrm{Im}(\phi)$*

Example 7.2.2. $f : \mathbb{Z} \to \mathbb{Z}_4$ is a group homomorphism when $f(a) = a \mod 4$. Then, $\mathrm{Im}f = \mathbb{Z}_4$ because f is onto. Furthermore,

$$\mathrm{Ker}f = \{0, \pm 4, \pm 8, \cdots\} = \langle 4 \rangle.$$

By the first isomorphism theorem, $\mathbb{Z}/\langle 4 \rangle = \mathbb{Z}_4$.

Lemma 7.1. *Let $\phi : G \to H$ be a group homomorphism with $K = \mathrm{Ker}(\phi)$. Then, $\phi(a) = \phi(b)$ iff $aK = bK$.*

Proof. ($\Rightarrow$) Suppose $\phi(a) = \phi(b)$. Then, $\phi(a)\phi(b)^1 = e_H$. So

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

So $ab^{-1} \in K$ but this means $aK = bK$.

($\Leftarrow$) If $aK = bK$, then $ab^{-1} \in K$. So

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

But then $\phi(a) = \phi(b)$. □

Definition 7.3. *Let G be a group with normal subgroup $\mathbb{N}$. Then, the map $\pi : G \to G/N$ defined by $\phi(g) = gN$ is called the natural homomorphism.*

Proof. We cliam that $\varphi : G/K \to \mathrm{Im}\phi$ given by $\varphi(gK) = \phi(g)$ is an isomorphism.

First, we want to show that φ is well-defined. Suppose $aK = bK$ with respect to $\varphi(aK) = \varphi(bK)$. Now, $\varphi(aK) = \phi(a)$ and $\varphi(bK) = \phi(b)$, and by the Lemma, $\phi(a) = \phi(b)$. So $\phi(aK) = \phi(bK)$.

Now, we want to show that φ is a group homomorphism. Let $aK, bK \in G/K$. Then,

$$\begin{aligned}\varphi(aKbK) &= \varphi(abK)\\ &= \phi(ab)\\ &= \phi(a)\phi(b)\\ &= \varphi(aK)\varphi(bK)\end{aligned}$$

Now, we want to show that φ is surjective. Let $t \in \text{Im}\phi$. So there is a $g \in G$ such that $\phi(g) = t$. But then $gK \in G/K$, and $\varphi(gK) = \phi(g) = t$.

Finally, we want to show that φ is injective. Let $aK, bK \in G/K$. Suppose

$$\varphi(aK) = \phi(a) = \pi(b) = \varphi(bK).$$

Since $\phi(a) = \phi(b)$, by the Lemma, $aK = bK$ so φ is injective.

So by these facts, $G/K \simeq \text{Im}\phi$. □

Example 7.2.3. For any $n \geq 1$, $\mathbb{Z}/\langle n\rangle \simeq \mathbb{Z}$.

Proof. We have a group homomorphism $f : \mathbb{Z}_n \to \mathbb{Z}_n$ given by $f(a) = a \mod n$. Then,

$$\begin{aligned}\text{Im}f &= \mathbb{Z}_n\\ \text{Ker}f &= \{a_1 \pm n, \dots\} = \langle m\rangle\end{aligned}$$

So by the first isomorphism theorem, $\mathbb{Z}/\langle a\rangle = \mathbb{Z}_n$. □

Example 7.2.4. Let S_n be the symmetric group with $n \geq 3$. Define $f : S_n \to \mathbb{Z}_2$ by

$$f(\sigma) = \begin{cases} 0 & \text{if } \sigma \text{ is even}\\ 1 & \text{if } \sigma \text{ is odd}\end{cases}$$

This is a homomorphism.

Proof. Let $\sigma_1, \sigma_2 \in S_n$. Then,

1. σ_1, σ_2 both even:

$$f(\sigma_1\sigma_2) = 0 = 0 + 0 = f(\sigma_1) + f(\sigma_2)$$

2. σ_1 even, σ_2 odd:

$$f(\sigma_1\sigma_2) = 1 = 0 + 1 = f(\sigma_1) + f(\sigma_2)$$

3. σ_1 odd, σ_2 even: same as above

4. σ_1, σ_2 both odd:

$$f(\sigma_1\sigma_2) = 0 = 1 + 1 = f(\sigma_1)f(\sigma_2)$$

□

Note that $\text{Ker}(f) = A_n$ and $\text{Im}(\phi) = \mathbb{Z}_2$. So $S_n/A_n \simeq \mathbb{Z}_2$.

Corollary 7.1. *For $n \geq 3$, A_n is is normal in S_n.*

Proof. Since A_n is the kernel of some homomorphism, and because all kernels are normal, A_n is normal. □

Example 7.2.5. Suppose $\phi : \mathbb{Z}_{30} \to \mathbb{Z}_{30}$ is a group homomorphism and $\text{Ker}(\phi) = \{0, 10, 20\}$. If $\phi(23) = 9$, find all elements of $\mathbb{Z}_{30}$ that get mapped to 9, i.e. find all b such that $\phi(b) = 9$.

We want all b such that

$$\begin{aligned} \phi(23) = 9 &\iff 23 + K = b + K \\ &\iff (23 - b) \in K = \{0, 14, 20\} \\ &\iff b = 3, 13, 23 \end{aligned}$$

Theorem 7.4. *Let $\phi : G \to H$ be a group homomorphism. Then, ϕ is one-to-one if and only if* $\text{Ker}(\phi) = \{e_G\}$. *(Kernel measures injectivity)*

Proof. ($\Rightarrow$) Assume ϕ is one to one with repsect to $\text{Ker}(\phi) = \{e_G\}$. Take $g \in \text{Ker}(\phi)$. So

$$\phi(g) = e_H = \phi(e_G).$$

Since ϕ is one-to-one, $g = e_G$.

($\Leftarrow$) Assume $\text{Ker}(\phi) = \{e_G\}$. Suppose $\phi(a) = \phi(b) \in H$. Hence,

$$\begin{aligned} e_H &= \phi(a)\phi(b)^{-1} \\ &= \phi(a)\phi\left(b^{-1}\right) \\ &= \phi\left(ab^{-1}\right) \end{aligned}$$

So $ab^{-1} \in \text{Ker}(\phi)$. So $ab^{-1} = e_G \implies a = b$. □

Theorem 7.5. *If $\phi : G \to H$ is injective, H has a subgroup isomorphic to G, namely* $\text{Im}(\phi)$.

Proof. ϕ injective implies that $\text{Ker}(\phi) = \{e_G\}$. By the first isomorphism theorem, we find that $G/\{e_G\} \simeq \text{Im}(\phi)$. But $G \simeq G/\{e_G\}$. So $G \simeq \text{Im}(\phi)$ □

Theorem 7.6. *Suppose $\phi : G \to H$ is an onto homomorphism with* $\text{Ker}(\phi) = K$. *If $|G|, |H| < \infty$, then,*

$$|G| = |k||H|$$

Proof. Since ϕ is onto, by the first isomorphism theorem, we have $G/K = H$. So

$$|H| = |G/K| = |G|/|K| \implies |G| = |H||K|,$$

by the Lagrange's theorem. □

Definition 7.4. *The* trivial homomorphism $\phi : G \to H$ *is the homomorphism $\phi(g) = e_H$ for all $g \in G$.*

Here are some useful facts:

1. $G/\{e_G\} \simeq G$.
2. $G/G \simeq \{e_G\}$.

Example 7.2.6. Suppose $\phi : \mathbb{Z}_p \to H$ with p a prime such that if ϕ is not the trivial homomorphism, then ϕ is one-to-one.

For this example, it is sufficient to show that $\text{Ker}(\phi) = \{0\}$. Note that $\mathbb{Z}_p$ only has trivial subgroups. Since the Kernel of ϕ is a subgroup of $\mathbb{Z}_p$, we know that the kernel of ϕ is either equal to $\{0\}$ or $\mathbb{Z}_p$. If $\text{Ker}(\phi) = \mathbb{Z}_p$, then ϕ is the trivial homomorphism so it must be that $\text{Ker}(\phi) = \{0\}$.

Theorem 7.7 (Second isomorphism theorem)**.** *Let H be a subgroup of G (not necessarily normal) and N a normal subgroup of G. Then,*

1. *$HN = \{hn | h \in H, n \in N\}$ is a subgroup of G*
2. *N is normal in HN*
3. *$H \cap N$ is normal in N*
4. *$HN/N \simeq H/(H \cap N)$*

Proof. Here's an idea of the proof:

1. Prove that HN is subgroup of G
2. Prove that N isnormal in HN and $H \cap N$ is normal in H
3. Define a map $\phi : H \to HN/N$ by $\phi(h) = hN$
   (a) Show ϕ is a homomorphism
   (b) Show ϕ is onto
4. So 3 implies that $H/\text{Ker}(\phi) \simeq HN/N$ by the first isomorphism theorem
5. Show $\text{Ker}(\phi) = H \cap N$.

□

Theorem 7.8 (Correspondance theorem)**.** *Let G be a group with a normal subgroup N.*

- *If K is a subgroup such that $N \subseteq K \subseteq G$, then K/N is a subgroup of G/N.*
- *If L is a subgroup of G/N, then there is a subgroup $N \subseteq K \subseteq G$ such that $L = K/N$.*

Example 7.2.7. Consider $G = \mathbb{Z}_8$ and $N = \{0, 4\}$.

- Subgroups of $N \subseteq K \subseteq G$:
  1. $N \subseteq N = \{0, 4\} \subseteq G$
  2. $N \subseteq \{0, 2, 4, 6\} \subseteq G$
  3. $N \subseteq G \subseteq G$
- Subgroups of $G/N \simeq \mathbb{Z}_8/N \simeq \mathbb{Z}_4$
  1. $N/N = \{0 + N\}$
  2. $\{0, 2, 4, 6\}/N = \{0 + N, 2 + N\}$
  3. $G/N = \{0 + N, 1 + N, 2 + N, 3 + H\}$

Theorem 7.9 (Third isomorphism theorem)**.** *Let G be a group with H and N normal subgroups such that $N \subseteq H \subseteq G$. Then,*

$$G/H \simeq (G/N)/(H/N)$$

Proof. Here's a sketch of the proof:

1. Define a group homomorphism $\phi : G/N \to G/H$ by $\phi(gN) = gH$ (need to check that this is well-defined and a homomorphism)
2. Show that ϕ is onto
3. Show $\text{Ker}(\phi) = H/N \subseteq G/N$.

Combining (1), (2), (3), and the first isomorphism gives

$$(G/N)/(H/N) \simeq G/H,$$

as required. □

8 Rings

8.1 Introduction

Informally, a ring is an additive group with more structure.

Definition 8.1. *A ring R is a set with two binary operations (usually addition and multiplication) such that for all $a, b \in R$,*

1. $a + b = b + a$
2. $(a + b) + c = a + (b + c)$
3. *There is an additive identity* $0 \in R$ *such that* $a + 0 = 0 + a = a$
4. *There is an additive inverse* $(-a)$*, i.e., for all* $a \in R$*, we have*

$$a + (-a) = (-a) + a = 0$$

5. $(ab)c = a(bc)$
6. $a(b + c) = ab + ca$ *and* $(a + b)c = ac + bc$

Note that the first four conditions imply that a ring is an abelian group under addition

Definition 8.2. *A ring R has an identity if there is $1 \in R$ such that $a1 = 1a = a$ for all a.*

Definition 8.3. *A ring R is commutative if $ab = ba$ for all $a, b \in R$.*

Definition 8.4. *A ring R is an (integral) domain if R has identity, is commutative, and $ab = 0$ implies $a = 0$ or $b = 0$*

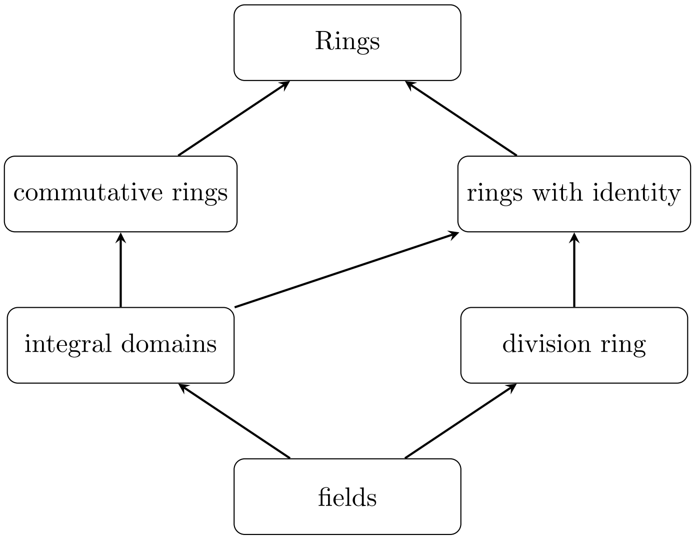
Definition 8.5. *A ring R is a division ring if R has an identity and if every element $a \in R$ has a multiplicative inverse, i.e., there exists $a^{-1} \in R$ such that $aa^{-1} = 1$.*

Definition 8.6. *A* field *is a division ring that is commutative.*

Remark. If $a \in R$ has a multiplicative inverse, we say a is a unit.

Example 8.1.1. Consider $\mathbb{Z}$, a set of all integers.

- binary operations are regular + and ×.
- has an identity
- is commutative
- domain
- not a field since if $a \neq 1, -1, 0$, then a is not a unit



Example 8.1.2. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all rings. In fact, they are fields.

Example 8.1.3. $\mathbb{Z}_n$ is a ring where operations are addition and multiplication modulo n.

- binary operations are addition and multiplication modulo n
- commutative with identity
- not a domain because $2 \times 3 = 0 \mod 6$ but $2 \neq 0$ and $3 \neq 0$. However, $\mathbb{Z}_2$ is a domain (in fact a field).

Example 8.1.4. $E = \{2n | n \in \mathbb{Z}\}$ is a ring that is commutative without identity.

Example 8.1.5. $M_2(\mathbb{R})$, a set of all two by two real matrices, is a ring that is not commutative but has an identity (the identity matrix).

Theorem 8.1 (Properties of a ring)**.** *Let $a, b \in R$, then*

1. $a \cdot 0 = 0 \cdot a = 0$
2. $a(-b) = (-a)b = -(ab)$
3. $(-a)(-b) = ab$

If $1 \in R$, then

4. $(-1)a = -a$
5. $(-1)(-1) = 1$
6. *identity is unique*

Proof. (uniqueness of identity) Suppose 1 and $1'$ are identities of R. Then,

$$1 = 11' = 1'$$

So $1 = 1'$. □

Theorem 8.2 (uniqueness of inverses)**.** *If $a \in R$ and a is a unit, then a^{-1} is unique.*

8.2 Subring

Definition 8.7. *A subset S of a ring R is a subring if S is also a ring under the operation of R.*

Theorem 8.3. *Let $S \subseteq R$ be a subset of a ring R. Then, S is a subring if*

1. *$S \neq \varnothing$*
2. *$rs \in S$ for all $r, s \in S$ (closed under multiplication)*
3. *$r - s \in S$ for all $r, s \in S$ (closed under substraction)*

Example 8.2.1. $\{0\} \subseteq R$ and $R \subseteq R$ are the trivial subrings.

Example 8.2.2. $E = \{2n | n \in Z\}$ is a subring of $\mathbb{Z}$. Note that $\mathbb{Z}$ has an identity but E does not.

8.3 Integral Domains and Fields

Consider the following example:

Example 8.3.1. If $R = \mathbb{Z}_6$, then in this ring, $2, 3 \neq 0$ but $2 \times 3 = 0$.

So two non-zero elements can multiply together to get 0.

Definition 8.8. *A nonzero element a in ring R is called a zero divisor if there is an nonzero element b in R such that $ab = 0$.*

Example 8.3.2. 2 and 3 are zero divisors in $\mathbb{Z}_6$.

Definition 8.9. *A commutative ring R with identity is an (integral) domain if it has no zero divisors.*

Example 8.3.3. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all integral domains.

Theorem 8.4. *$\mathbb{Z}_n$ is domain if and only if n is prime.*

Proof. Assume $\mathbb{Z}_n$ is a domain. We want to show that n is prime. Instead, we can prove the contrapositive statement: "If n is not prime, then $\mathbb{Z}_n$ is not a domain". Since n is not prime, $n = ab$ with $1 < a, b < n$. Then, $a \neq 0$ and $b \neq 0$ in $\mathbb{Z}_n$ but $ab \equiv n \equiv 0 \mod n$. So $\mathbb{Z}_n$ has zero divisors, i.e., not a domain.

Suppose that n is prime. Suppose $a, b \in \mathbb{Z}_n$ and $ab = 0$. We want to show $a = 0$ or $b = 0$. Since $ab \equiv \mod n$, this means $ab = nk$. So n divides ab. But because n is prime, then $n|a$ or $n|b$. But if $n|a$, then $a = nl$ so $a \equiv= 0 \mod n$. Similarly, if $n|b$, then $b \equiv 0 \mod n$. □

Example 8.3.4. Consider

$$\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$$

This is a subring of $\mathbb{R}$. It is also a domain.

Definition 8.10. *If R and S are rings, then $R \times S$ is a ring with the following operations:*

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2)$$
$$(r_1, s_1)(r_2, s_2) = (r_1r_2, s_1s_2)$$

Example 8.3.5. Even if R and S are domains, $R \times S$ is not a domain.

Example 8.3.6. Consider $R = S = \mathbb{Z}$. $\mathbb{Z} \times \mathbb{Z}$ is not a domain because

$$(1, 0)(0, 1) = (0, 0).$$

Domains have cancelation property, i.e., $ab = ac$ implies $b = c$ if $a \neq 0$. In fact, we have the following theorem:

Theorem 8.5. *Suppose $ab = ac$ with $a \neq 0$. Then, R is a domain if and only if cancellation holds.*

Proof. ($\Rightarrow$) Suppose R is domain and $ab = ac$ with $a \neq 0$. Then,

$$ab - ac = a(b - c) = 0$$

Since R is a domain and $a \neq 0$, $b - c = 0$ and $b = c$.

($\Leftarrow$) Suppose that $ab = 0$ in R. If $a = 0$, we are done. So suppose $a \neq 0$. Then, $ab = 0 = a0$. Thus, by cancellation property, $b = 0$. □

Definition 8.11. *A domain F is a field if for every $0 \neq a \in F$, there exists an $a^{-1} \in F$ such that $aa^{-1} = 1$ (every nonzero element of F is a unit).*

Example 8.3.7. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ but not $\mathbb{Z}$.

Theorem 8.6. *If a domain is finite, then it is also a field.*

Proof. Suppose that $\{a_1, a_2, \ldots, a_n\}$ are the non-zero element of our domain D. We want to show that for every $a \in D$, we can find $a^{-1} \in D$ such that $aa^{-1} = 1$. Notice that $a_i = 1$ since $1 \in D$. Now, multiply everything in $\{a_1, a_2, \ldots, a_n\}$ by a to get $\{aa_1, aa_2, \ldots, aa_n\}$. If $aa_i = aa_j$, by cancellation, we have $a_i = a_j$. So when we multiply by a, we are shuffling all the elements. So $aa_k = 1$ for some a_k. But then, $a^{-1} = a_k$ So D is a field. □

Corollary 8.1. *$\mathbb{Z}_p$ is a field for all prime p.*

Example 8.3.8. Consider

$$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} \subseteq \mathbb{R}.$$

This is a field.

Take $a+b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$. We want to find $c+d\sqrt{2}$ such that

$$(a+b\sqrt{2})(c+d\sqrt{2}) = 1.$$

So

$$\begin{aligned}(a+b\sqrt{2})(c+d\sqrt{2}) =& ac+ad\sqrt{2}+bc\sqrt{2}+bd2 = 1\\ &\implies (ac+2bd)+(ad+bc)\sqrt{2} = 1+0\sqrt{2}\end{aligned}$$

By solving this, we find that

$$c = \frac{a}{a^2-2b^2}, d = \frac{-b}{a^2-2b^2}.$$

Definition 8.12. *The characteristic of a ring R is the smallest positive integer n such that for all $r \in R$, $nr = r+\cdots+r = 0$. If no such integers exist, we say that the characteristic is 0. We write* $\operatorname{char}(R) = n$.

Example 8.3.9. $\operatorname{Char}(\mathbb{Z}_p) = p$

Example 8.3.10. $\operatorname{Char}(\mathbb{Z}) = 0$

Lemma 8.1. *If $1 \in R$ and order of 1 is n, i.e., $n1 = 0$, then* $\operatorname{Char}(R) = n$.

Theorem 8.7. *If R is a domain, then* $\operatorname{Char}(R) = 0$ *or p, a prime.*

Proof. Suppose $\operatorname{Char}(R) \neq 0$, i.e., $\operatorname{Char}(R) = n$. If n is not a prime, then $n = ab$ with $1 < a, b < n$. Then,

$$\underbrace{1+\cdots+1}_{n} = 0.$$

Then,

$$\underbrace{\underbrace{(1+\cdots+1)}_{a}+\underbrace{(1+\cdots+1)}_{a}+\cdots+\underbrace{(1+\cdots+1)}_{a}}_{b} = 0.$$

But $ba = 0$. Byt R is a domain so $a = 0$ or $b = 0$. This is a contradiction since neither a nor b are equal to 0. □

9 Ideals

9.1 Ideals

Definition 9.1. *A subring I of a ring R is an idean if for all $x \in I$ and all $r \in R$, rx and xr are in I. I is a proper ideal if $I \subset R$.*

Example 9.1.1. Let R be any ring. The subring $I = \{0\}$ is an ideal since

1. $\{0\}$ is a subring of R
2. for all $r \in R$, and any $x \in \{0\}$,

$$rx = xr = r0 = 0r = 0 \in \{0\}$$

$I = \{0\}$ is the trivial ideal or zero ideal.

Example 9.1.2. $\mathbb{Z} \subset \mathbb{Q}$ is a subring but not an ideal. Note $1 \in \mathbb{Z}$ and $1/2 \in \mathbb{Q}$ but $s1/2 \cdot 1 \notin \mathbb{Z}$.

Example 9.1.3. If $R = \mathbb{Z}$ and fix $n \in \mathbb{Z}$, $n > 0$. Then,

$$\langle n \rangle = \{0, \pm n, \pm 2n, \dots\}$$

is an ideal of R.

Proof. This set is a subring of $\mathbb{Z}$. Take an elements $a \in \langle n \rangle$ and take any $r \in \mathbb{Z}$. Now, $a = nl$ for some $l \in \mathbb{Z}$. Then,

$$ra = ar = r(nl) = n(lr) \in \langle n \rangle$$

since $\mathbb{Z}$ is commutative. □

Remark. If R is commutative, then we only need to check that $rx \in I$.

Theorem 9.1. *Let R be a commutative ring with identity. For any $a \in R$, let II be the set*

$$I = \{ra \mid r \in R\}.$$

Then, I is an ideal of R.

Definition 9.2. *An ideal of the form $\{ra \mid r \in R\}$ for some $a \in R$ is called the principle ideal generated by a. We write this as $I = \langle a \rangle$.*

Before we prove Theorem 9.1, we present a way to test for an ideal: A nonempty set $I \subseteq R$ is an ideal if

1. For all $x, y \in I$, $x - y \in I$.
2. For all $x \in I$ and $r \in R$, $rx, xr \in I$

Here is the proof for Theorem 9.1:

Proof. Since $1 \in R$, $a = 1 \cdot a \in I$. So I is not empty.

1. First, let $x, y \in I = \{ra \mid r \in R\}$. So $x = ra$ and $y = sa$ for $r, s \in R$. Then, $x - y = ra - rs$.
2. Let $x \in I$ and $\in R$. So $x = ra$ and thus

$$tx = t(ra) = (tr)a \in I$$

since $(tr) \in R$.

□

Theorem 9.2. *All ideals in $\mathbb{Z}$ are principal.*

Theorem 9.3. *Recall that only subgroups of $\mathbb{Z}$ are*

$$n\mathbb{Z} = \{mn \mid m \in \mathbb{Z}\} = \langle n \rangle$$

But these are also ideals. For any ideal $I \in \mathbb{Z}$, I is also an additive subgroup of $\mathbb{Z}$. So $I = \langle n \rangle$ for some n.

9.2 Factor rings

Let I be an ideal of a ring R. Then, R is abelian additive group, so I is a normal subgroup of R. So as groups,

$$R/I = \{a + I \mid a \in R\},$$

this factor is defined. We want to show that R/I also has a multiplication and so is a ring. We call R/I a factor ring or a quotient ring and read it as R mod I.

Theorem 9.4. *Let R be a ring with ideal I. Then, the set of left cosets*

$$\{a + I \mid a \in R\}$$

forms a ring with operations:

$$(a + I) + (b + I) = (a + b) + I$$
$$(a + I)(b + I) = (ab) + I$$

Proof. All additive properties hold because R/I is an additive group. First, we wnat to check that multiplication is well defined. Suppose $a + I = c + I$ and $b + I = d + I$. Then, we want to show that

$$(a + I)(b + I) = (c + I)(d + I)$$

Given $a - c \in I$ and $b - d \in I$, we have

$$(a - c)b = ab - cb \in Ic(b - d) \quad = cb - cd \in I$$

Then,

$$(ab - cb) + (cb - cd) = ab - cd \in I$$

So

$$ab + I = cd + I.$$

But then

$$\begin{aligned}(a + I)(b + I) &= ab + I\\ &= cd + I\\ &= (c + I)(d + I)\end{aligned}$$

So multiplication is well defined.

Now, we want to verify the ring operation with multiplication. Observe that

$$\begin{aligned}(a + I)[(b + I)(c + I)] &= (a + I)(bc + I)\\ &= a(bc) + I\\ &= (ab)c + I\\ &= (ab + I)(c + I)\\ &= [(a + I)(b + I)](c + I)\end{aligned}$$

So multiplication is associative. Then,

$$\begin{aligned}(a + I)[(b + I) + (c + I)] &= (a + I)[(b + c) + I]\\ &= a(b + C) + I\\ &= (ab = ac) + I\\ &= (ab + I) + (ac + I)\\ &= (a + I)(b + I) + (a + I)(c + I)\end{aligned}$$

So multiplication is distributive. □

Example 9.2.1. Consider $R = \mathbb{Z}$ and $I = \langle 5 \rangle = \{5n \mid n \in \mathbb{Z}\}$. Then, its distinct cosets are given by

$$R/I = \{0 + I, 1 + I, 2 + I, 3 + I, 4 + I\}$$

By the theorem, $\mathbb{Z}/\langle 5 \rangle$ is a ring:

$+$	$0+I$	$1+I$	$2+I$	$3+I$	$4+I$
$0+I$					
$1+I$					
$2+I$					
$3+I$					
$4+I$					

$\times$	$0+I$	$1+I$	$2+I$	$3+I$	$4+I$
$0+I$	$0+I$	$0+I$	$0+I$	$0+I$	$0+I$
$1+I$	$0+I$	$1+I$	$2+I$	$3+I$	$4+I$
$2+I$	$0+I$	$2+I$	$4+I$	$1+I$	$3+I$
$3+I$	$0+I$	$3+I$	$1+I$	$4+I$	$2+I$
$4+I$	$0+I$	$4+I$	$3+I$	$2+I$	$1+I$

9.3 Ring homomorphism

Definition 9.3. *a function $f : R \to S$ with R and S rings is a ring homomorphism if*

- $f(a+b) = f(a) + f(b)$ *for all* $a, b \in R$
- $f(ab) = f(a)f(b)$ *for all* $a, b \in R$

Definition 9.4. *We say that R and S isomorphic if there exists a ring isomorphism $f : R \to S$, i.e., f is a homomorphism that is bijective.*

Example 9.3.1 (Identity map)**.** Let $R = S$. Define a map $f : R \to R$ by $f(r) = r$. This is a ring isomorphism.

Remark. If R and S are isomorphic, we write $R \simeq S$.

Example 9.3.2 (Zero map)**.** Let R and S be any rings. Then, $f : R \to S$ defined by $f(r) = 0_s$ is a ring homomorphism.

Proof. Let $a, b \in R$. Then,

- $f(a+b) = 0_s = 0_s + 0_s = f(a) + f(b)$
- $f(a)f(b) = 0_s 0_s = 0_s = f(ab)$

□

Example 9.3.3. Define a function $f : \mathbb{Z} \to \mathbb{Z}$ by

$$f(a) = a \mod n.$$

We know this is a group homomorphism, so it satisfies the first part of the ring homomorphism. Furthermore,

$$f(ab) = ab \mod n = (a \mod n)(b \mod n) = f(a)f(b).$$

So this is a ring homomorphism

Remark. $\mathbb{Z}_n \simeq \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\langle n \rangle$ (isomorphic as groups but also for rings)

Theorem 9.5. *Let I be any ideal in R. Then, there is a homonorphism*

$$\pi : R \to R/I$$

given by $\pi(a) = a + I$ (called the natural homomorphism).

Proof. Let $a, b \in R$. Then,

- $\pi(a+b) = (a+b) + I = (a+I) + (b+I) = \pi(a) + \pi(b)$
- $\pi(ab) = ab + I = (a+I)(b+I) = \pi(a)\pi(b)$

□

Theorem 9.6 (Properties of homomorphism)**.** *Let $f : R \to S$ be a ring homomorphism*

1. $f(0_R) = 0_S$
2. *for any positive integer n and $r \in R$,*
$$f(nr) = nf(r) \text{ and } f(r^n) = f(r)^n$$
3. *If I is an ideal of R, and if f is onto, then*
$$f(I) = \{f(g) \mid g \in I\}$$
is an ideal of S
4. *If $1_R \in R$, and f onto, $f(1_R) = 1_S$.*

Proof. **(1)** Since $0_R = 0_R + 0_R$, we have

$$f(0_R) = f(0_R + 0_R) = f(0_R) + f(0_R)$$

Since $-f(0_R) \in S$, when we add this to both sides, we get

$$\begin{aligned} f(0_R) + (-f(0_R)) &= f(0_R) + (f(0_R) + (-f(0_R))) \\ 0_S &= f(0_R) + 0_S = f(0_R) \end{aligned}$$

(2) Let's fix some integer $n > 0$. Then,

$$f(nr) = f(\underbrace{r + \cdots + r}_{n}) = f(r) + \cdots + f(r) = nf(r)$$

Likewise,

$$f(r^n) = f(\underbrace{r \cdot r \cdots r}_{n}) = f(r) \cdot f(r) \cdots f(r) = f(r)^n$$

(3)

- (nonempty) Since $0_R \in I$ and $0_S = f(0_R) \in f(I)$, this set is nonempty
- (closed under subtraction) Take $a, b \in f(I)$. So there exists $g, h \in I$ such that $a = f(g)$ and $b = f(h)$. Then,
$$a - b = f(g) - f(h) = f(g - h)$$
But $g - h \in I$, so $a - b \in f(I)$.
- (closed under absorption property) Let $s \in S$ and $a \in f(I$. So there exists $g \in I$ such that $a = f(g)$. Since f is onto, there exists an $r \in R$ such that $f(r) = s$. Then, $rg \in I$. So $f(rg) \in f(I)$ but
$$f(rg) = f(r)f(g) = sa$$
So $sa \in f(I)$.

- Now, our goal is to show that $sf(1_R) = s$ for all $s \in S$. Since multiplicative idensity is unique, $f(1_R) = 1_S$. So let's take $s \in S$. Since f is onto, there exists $r \in R$ such that $f(r) = s$. Then,

  $$sf(1_R) = f(r)f(1_R) = f(r1_R) = f(r) = s$$

  So $f(1_R) = 1_S$.

□

Definition 9.5. *If $f : R \to S$ is a ring homomorphism, then Kernel of f is*

$$\text{Ker}(f) = \{r \in R \mid f(r) = 0_S\}$$

Theorem 9.7. Ker(f) *is an ideal of R.*

Proof.

- (nonempty) Since $f(0_R) = 0_S$, $0_R \in \text{Ker}(f)$.
- (subtraction) Let $a, b \in \text{Ker}(f)$. Then,

  $$f(a - b) = f(a) - f(b) = 0_S - 0_S = 0_S$$

  So $a - b \in \text{Ker}(f)$.
- (absorption) Let $a \in \text{Ker}(f)$ and $r \in R$. Then,

  $$f(ra) = f(r)f(a) = f(r)0_S = 0_S$$

  So $ra \in \text{Ker}(f)$.

□

Theorem 9.8. *Let I be any ideal of R and let $\pi : R \to R/I$ be the natural homomorphism. Then,* Ker$(f) = I$.

Proof. Let $a \in I$. Then,

$$\pi(a) = a + I = 0 + I$$

since $a \in I$. So $a \in \text{Ker}(\pi)$.

Let $b \in \text{Ker}(\pi)$. So

$$\pi(b) = b + I = 0 + I$$

So $b - 0 = b \in I$. So $\text{Ker}(\pi) \subseteq I$. □

Remark. Any ideal I can be the Kernel of some ring homomorphism.

9.4 First Isomorphism Theorem for rings

Lemma 9.1. *Let $f : R \to S$ be a ring homomorphism. Then,*

$$f(R) = \{f(r)|r \in R\} \subseteq S$$

is a subring of S.

Proof.

- (nonempty) $0_R \in R$ and so $0_S = f(0_R) \in f(R)$.
- (subtraction) Let $a, b \in f(R)$. So there exist $r, s \in R$ such that $a = f(r)$ and $b = f(s)$. Then,

  $$a - b = f(r) - f(s) = f(r - s)$$

  since f is a homomorphism. But $r - s \in R$ so $a - b \in f(R)$.
- (multiplication) Let $a, b \in f(R)$. Then, $a = f(r)$ and $b = f(s)$ for some $r, s \in R$. So

  $$ab = f(r)f(s) = f(rs)$$

  and $rs \in R$. So $ab \in f(R)$.

□

Lemma 9.2. *Let $f : R \to S$ be a ring homomorphism. Then, f is one-to-one if and only if*

$$\mathrm{Ker}(f) = \{0_R\}$$

Proof. ($\Rightarrow$) Let $b \in \mathrm{Ker}(f)$. Then,

$$f(b) = 0_S = f(0_R)$$

Since f is one-to-one, this forces $b = 0_R$. So $\mathrm{Ker}(f) = \{0_R\}$.

($\Leftarrow$) Suppose $f(a) = f(b)$. Then,

$$f(a) - f(b) = 0.$$

Since f is a homomorphism,

$$f(a - b) = f(a) - f(b) = 0_S.$$

So $a - b \in \mathrm{Ker}(f) = 0_R$. Thus, $a - b = 0_R$ so $a = b$. □

Theorem 9.9 (First isomorphism theorem for rings)**.** *Let $f : R \to S$ be a ring homomorphism. Then,*

$$R/\mathrm{Ker}(f) \simeq f(R).$$

Proof. The proof is similar to the group proof but we need to check that they are isomorphic as rings. So we want to find an isomorphism

$$\phi : R/\text{Ker}(f) \to f(R).$$

We claim that the desired function is $\phi(r + \text{Ker}(f)) = f(r)$. First, we want to show the wel-definedness. We need to check that

$$\phi(r + \text{Ker}(f)) = \phi(s + \text{Ker(f)})$$

implies $f(r) = f(s)$. So suppose that

$$r + \text{Ker}(f) = s + \text{Ker}(f)$$

Since

$$r + \text{Ker}(f) = s + \text{Ker}(f),$$

this means that $r - s \in \text{Ker}(f)$. So

$$f(r - s) = 0_S$$

But

$$f(r - s) = f(r) - f(s)$$

so

$$f(r) - f(s) = 0_S,$$

so $f(r) = f(s)$.

Now, we want to show surjectivity. Let $a \in f(R$. So $a = f(r)$ for some $r \in R$. But then

$$r + \text{Ker}(f) \in R/\text{Ker}(f)$$

and

$$\phi(r + \text{Ker}(f)) = f(r) = a$$

To show that it is injective, suppose $b + \text{Ker}(f) \in \text{Ker}(\phi)$. This means

$$\phi(v + \text{Ker}(f)) = f(b) = 0_S.$$

So $b \in \text{Ker}(f)$. Thus,

$$b + \text{Ker}(f) = 0 + \text{Ker}(f)$$

So

$$\text{Ker}(\phi) = \{a + \text{Ker}(f)\}$$

Then, the lemma implies that ϕ is one-to-one.

Finally, notice that

$$\begin{aligned}
\phi(a + \text{Ker}(f)) + \phi(b + \text{Ker}(f)) &= f(a) + f(b) \\
&= f(a + b) \\
&= \phi((a + b) + \text{Ker}(f)) \\
\phi(a + \text{Ker}(f))\phi(b + \text{Ker}(f)) &= f(a)f(b) \\
&= f(ab) \\
&= \phi(ab + \text{Ker}(f))
\end{aligned}$$

So ϕ is a homomorphism. Therefore, ϕ is an isomorphism. □

Example 9.4.1. Suppose $f : F \to S$ is a nontrivial ring homomorphis, (i.e., $\phi(x) \neq 0$ for some $x \in F$) and F is a field. Show that S has a subring isomorphic to F.

Proof. (Homework) The only ideal of a field F are $\{G\}$ and $\langle 1 \rangle = F$.

By first isomorphism theorem,

$$F/\mathrm{Ker}(f) \simeq f(F) \subseteq S.$$

Since $\mathrm{Ker}(f)$ is an ideal, $\mathrm{Ker}(f) = \langle 1 \rangle$ or $\mathrm{Ker}(f) = \langle 0 \rangle$. But $\mathrm{Ker}(f) \neq \langle 1 \rangle$ since there is an element not sent to 0. So $\mathrm{Ker}(f) = \langle 0 \rangle$. But then,

$$\mathrm{Ker}(F) \simeq F/\langle 0 \rangle \simeq F.$$

□

Example 9.4.2. Consider

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} \subseteq R$$

and

$$\begin{aligned} \mathbb{Q}[x] &= \{\text{all polynomials with coefficient in } \mathbb{Q}\} \\ &= \{a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \mid n \in \mathbb{N}, a_n \in \mathbb{Q}\} \end{aligned}$$

Then, the following homomorphism is called evaluation homomorphism:

$$\phi : \mathbb{Q}[x] \to \mathbb{Q}(\sqrt{2})$$

where $\phi(f(x)) = f(\sqrt{2})$ for $f(x) \in \mathbb{Q}[x]$.

Example 9.4.3. Consider $f(x) = 1 + x + x^2$. Then,

$$\begin{aligned} f(x) \to f(\sqrt{2}) &= 1 + \sqrt{2} + (\sqrt{2})^2 \\ &= 1 + \sqrt{2} + 2 \\ &= 3 + \sqrt{2} \end{aligned}$$

By the first isomorphism theorem,

$$\mathbb{Q}[x]/\mathrm{Ker}(\phi) = \mathbb{Q}(\sqrt{2})$$

where

$$\mathrm{Ker}(\phi) = \{f \in \mathbb{Q}[x] \mid f(\sqrt{2}) = 0\}.$$

Note that $x^2 - 2 \in \mathrm{Ker}(\phi)$. Then, one can prove that

$$\mathrm{Ker}(\phi) = \langle x^2 - 2 \rangle.$$

So

$$\mathbb{Q}[x]/\langle x^2 - x \rangle \simeq \mathbb{Q}(\sqrt{2})$$

9.5 Prime and maximal ideals

Definition 9.6. *An ideal M in a ring R is maximal if for every ideal J such that $M \subseteq J \subseteq R$, we have $J = M$ or $J = R$.*

Example 9.5.1. Let $R = \mathbb{Z}$ and fix a prime p. Let $\langle p \rangle = \{np | n \in \mathbb{Z}\}$ be the ideal generated by p. Then, $\langle p \rangle$ is a maximal ideal.

Proof. Suppose J is an ideal such that

$$\langle p \rangle \subseteq J \subseteq \mathbb{Z}$$

If $J = \langle p \rangle$, we are done. So suppose $J \neq \langle p \rangle$. Thus, there exists $m \in J \setminus \langle p \rangle$. Since $m \notin \langle p \rangle$, we have $p \not| m$. So $\gcd(p, m) = 1$. So

$$1 = pa + mb.$$

Since $\langle p \rangle \subseteq J$, $pa \in J$. Since $m \in J$, $mb \in J$, so

$$1 = pa + mb \in J.$$

Then,

$$R \subseteq J \subseteq R \implies R = J.$$

Note $1 \in J$ implies that $r \cdot 1 \in J$ for all $r \in R$ so $r \in J$ for all $r \in R$. □

Theorem 9.10. *Let R be a commutative ring with 1 with ideal M. Then, M is maximal if and only if R/M is a field.*

Proof. ($\Rightarrow$) Since M is maximal, $R/M \neq (0)$. Let

$$a + M \in R/M$$

such that $a + M \neq 0 + M$. So $a \neq M$. Consider the set

$$J = \{m + ar | m \in M, r \in R\}.$$

This set is an ideal of R. Since $M \subset J$ but $M \neq J$, and since M is maixmal, $J = R$. So $1 \in J$. Thus, there exists $m \in M$ and $r \in R$ such that

$$1 = m + ar.$$

So $ar - 1 = (-m) \in M$. Thus,

$$ar + M = 1 + M.$$

Then,

$$(1 + M) = (ar + M) = (a + M)(r + M).$$

So $(a + M)$ is a unit. Thus, R/M is a field.

($\Leftarrow$) Given R/M a field, we want to show that M is maximal. Suppose $M \subseteq J$ and $J \neq M$. Since $J \neq M$, there exists $a \in J$ such that $a \in M$. But this means $a + M \neq 0 + M$ in R/M. Since R/M is a field, there exists $(r + m)$ such that

$$(a + M)(r + M) = 1 + M$$

So $ar + M = 1 + M$, i.e., $ar - 1 \in M$. Thus, $ar - 1 \in M \subseteq J$ and since $a \in J$, $ar \in J$. Thus,

$$ar - (ar - 1) = 1 \in J.$$

So $J = R$. □

Example 9.5.2. For all primes $p \in \mathbb{Z}$, $\mathbb{Z}/\langle p \rangle \simeq \mathbb{Z}_p$ is a field.

Definition 9.7. *An ideal P of a ring R is prime if $P \subset R$ but $P \neq R$ and whenever $ab \in P$, either $a \in P$ or $b \in P$.*

Example 9.5.3. In $\mathbb{Z}$, every ideal generated by a prime p is a prime ideal.

Proof. Suppose $ab = \langle p \rangle$. So $ol = ab$ for some l. Then, $p|ab$. Then, either $p|a$ or $p|b$. If $p|a$, $a = pk$, so $a \in \langle p \rangle$. If $p|b$, $b = pk$, so $b \in \langle p \rangle$. □

Theorem 9.11. *Let R be a commutative ring with identity and an ideal $P \subset R$ but $P \neq R$. Then, P is a prime ideal if and only if R/P is an integral domain.*

Proof. ($\Rightarrow$) Suppose $(a + P)(b + P) = (0 + P)$ in R/P. So $ab + P = 0 + P$. Thus, $ab \in P$. Since P is prime, $a \in P$ or $b \in P$. If $a \in P$, $a + P = 0 + P$ and if $b \in P$, $b + P = 0 + P$.

($\Leftarrow$) Let $ab \in P$. So $ab + P = 0 + P$. Thus,

$$0 + P = (a + P)(b + P).$$

Since R/P is a domain, either $a + P = 0 + P$ or $b + P = 0 + P$. Thus, $a \in P$ or $b \in P$. □

Corollary 9.1. *Every maximal ideal is a prime ideal in a commutative ring with identity.*

Proof.

$$\begin{gathered} M \text{ maximal } \iff R/M \text{ a field} \\ \implies R/M \text{ a domain } \iff M \text{ prime} \end{gathered}$$

□

Example 9.5.4. Let I, J be ideals. Which of the following are ideals?

1. $I \cap J$
2. $I \cup J$

First one is an ideal.

- (nonempty) Consider $0 \in I$ and $0 \in J$, so $0 \in I \cap J$.

- (subtraction) Let $a, b \in I \cap J$. So

$$a, b \in I \implies a - b \in I.$$

  Likewise, $a - b \in J$. So $A - b \in I \cap J$.

- (absorption) Similar to above.

Second one is not an ideal. Consider $R = \mathbb{Z}$ and $I = \langle 2 \rangle$ with $J = \langle 3 \rangle$. Then,

$$I \cup J = \{0, 2, 3, \dots\}$$

is not closed under subtraction because $3 - 2 = 1 \notin I$.

10 Polynomial rings

10.1 Polynomial rings

Example 10.1.1. $2 + \pi x + \sqrt{3}x^2 + \log 7x^3$

Definition 10.1. *Let R be a commutative ring. The set of all polynomials with coefficients in R is called the polynomail ring. We write*

$$R[x] = \{a_0 + a_1 x + \cdots + a_n x^n \mid n \in \mathbb{N}, a_i \in \mathbb{R}\}$$

We sometimes call $R[x]$ the polynomial ring over R with indeterminate x.

Remark. $a_0 + a_1 x + \cdots a_n x^n = b_0 + b_1 x + \cdots b_m x^m$ if and only if $n = m$ and $a_i = b_i$ or all i.

Definition 10.2 (Addition)**.**

$$\begin{aligned}&(a_0 + a_1 x + \cdots + a_n x^n) + (b_0 + b_1 x + \cdots + b_n x^n)\\&= (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_n + b_n)x^n\end{aligned}$$

Definition 10.3 (Multiplication)**.**

$$\begin{aligned}&(a_0 + a_1 x + \cdots + a_n x^n)(b_0 + b_1 x + \cdots + b_m x^m)\\&= (a_0 b_0) + (a_1 b_0 + a_0 b_1)x + (a_2 b_0 + a_1 b_1 + a_0 b_2)x^2 + \cdots + (a_n + b_m)x^{n+m}\end{aligned}$$

where the coefficient of x^i in multiplication is

$$a_i b_0 + a_{i-1} b_1 + \cdots + a_1 b_{i-1} + a_0 b_i$$

where $a_j = 0$ if $j > n$ and $b_j = 0$ if $j > m$.

Definition 10.4. *If $f(x) = a_0 + a_1 x + \cdots a_n x^n$, with $a_n \neq 0$, then degree of $f(x)$ is*

$$\text{deg} f(x) = n$$

and a_n is called leading coefficient. If $a_n = 1$, we say $f(x)$ is monic.

Example 10.1.2. Consider

$$f(x) = 2x + 17x^3 + 82x^{2017}.$$

Then, the degree and leading coefficient of this polynomial is 2017 and 82.

Remark. $0 \in R[x]$ but by convention, $\deg 0$ is not defined.

Theorem 10.1. *If R is a commutative ring with identity, so is $R[x]$.*

Theorem 10.2. *If R is an integral domain, then so is $R[x]$.*

Proof. We will show that $\deg(f(x)g(x)) = \deg f(x) + \deg g(x)$ for any $f(x), g(x) \in R[x]$. Let

$$f(x) = a_n x^n + \cdots + a_0$$
$$g(x) = b_m x^m + \cdots + b_0$$

where $a_n, b_m \neq 0$. So

$$f(x)g(x) + (a_n b_m)x^{n+m} + \text{ lower order terms.}$$

Since $a_n \neq 0$ and $b_n \neq 0$ and since R is a domain, $a_n b_m \neq 0$. So $\deg f(x)g(x) = n + m = \deg f(x) + \deg g(x)$. So this menas that the product of two nonzero terms in $R[x]$ is non-zero. Therefore,

$$R[x]$$

must be a domain. □

Example 10.1.3. Consider $R = \mathbb{Z}_4$. Let

$$f(x) = 2x^2 + 2 \in \mathbb{Z}_4[x], \text{ and } g(x) = 2$$

Then,

$$f(x)g(x) = 2(2x^2 + 2) = 0$$

so $\deg f(x)g(x) \neq \deg f(x) + \deg g(x)$

So we can extend the construction to any number of variables:

$$R[x][y] = \{f_0 + f_1 y + f_2 y^2 + \cdots f_s y^s \mid f_i \in R[x]\}.$$

Likewise, we can define

$$R[x, y][z] = \{g_0 + g_1 z + \cdots g_t z^t \mid g_i \in R[x, y]\}.$$

In general, we have $R[x_1, \ldots, x_n]$, a set of all polynomials in $x_1, \ldots, x_n$ with coefficients in R.

Theorem 10.3 (Evaluation homomorphism)**.** *Let R be a commutative ring with identity and $\alpha \in R$. Then, the function $\phi_\alpha : R[x] \to R$ given by $f(x) \to f(\alpha)$ is a ring homomorphism called the evaluation homomorphism.*

Example 10.1.4. If $\alpha = 0$, then

$$\phi_0 : R[x] \to R$$

is given by

$$a_0 + a_1 x + \cdots + a_n x^n \to a_0.$$

So ϕ_0 takes polynomials to its constant term

10.2 Division algorithm for polynomials

The ring $\mathbb{Z}$ and $F[x]$ with F, a field, have similar properties.

Theorem 10.4. *Let F be a field, and $f(x), g(x) \in F[x]$ with $g(x) \neq 0_F$. Then, there exists unique polynomials $q(x)$ and $r(x)$ such that*

$$f(x) = g(x)q(x) + r(x)$$

with $r(x) = 0_F$ or $\deg r(x) < \deg g(x)$.

Example 10.2.1.

$$4x^4 + 3x^3 + 2x^2 + x = (2x^2 + 1)\left(2x^2 + \frac{3}{2}x\right) + \left(-\frac{1}{2}x\right)$$

10.3 Division algorithm

Theorem 10.5. *Let F be a field, and suppose $f(x), g(x) \in F[x]$ with $g(x) \neq 0_F$. Then, there exists unique $q(x), r(x) \in F[x]$ such that*

$$f(x) = g(x)q(x) + r(x)$$

with $r(x) = 0$ or $\deg r(x) < \deg g(x)$.

Proof of this theorem depends on strong induction: We assume that for each n, a statement $P(n)$ is given. If

- $P(0)$ is true
- If $P(0), P(1), \ldots, P(n-1)$ imply $P(n)$ true,

then $P(n)$ is true for all $n \geq 0$.

Proof. First, we want to show that $q(x)$ and $r(x)$ exists. We can think of two cases.

(Case 1 – $\deg f(x) < \deg g(x)$) Since $\deg f(x) < \deg g(x)$,

$$f(x) = 0 \cdot g(x) + f(x)$$

with $\deg f(x) < \deg g(x)$. So $q(x) = 0$ and $r(x) = f(x)$.

(Case 2 – $\deg f(x) \geq \deg g(x)$) First, consider the case when $0 = \deg f(x) \geq \deg g(x) \geq 0$. Then, $f(x) = a$ and $g(x) = b$ with $a, b \in F$. So

$$a = (b)(b^{-1}a) + 0$$

where $b^{-1}a \in F$ since F is a field. So $q(x) = b^{-1}$ and $r(x) = 0$.

Now, assume for all $f(x), g(x)$ with $n > \deg f(x) \geq \deg g(x)$, there exists $q(x), r(x)$ with

$$f(x) = g(x)q(x) + r(x)$$

with $\deg r(x) < \deg g(x)$ or $r(x) = 0$. Now, we want to show that statement is true if $\deg f(x) = n$. So we have

$$\begin{aligned} f(x) &= a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \\ g(x) &= b_m x^m + \cdots + b_0 \end{aligned}$$

with $n \geq m$.

Since $b_m \neq 0$ and $b_m \in F$, so is $b_m^{-1} \in F$. Consider the polyonmial $h(x)$:

$$h(x) = f(x) - a_n b_m^{-1} x^{n-m} g(x)$$

Note that

$$\begin{aligned} a_n b_m^{-1} x^{n-m} g(x) &= a_n b_m^{-1} x^{n-m}(b_m x^m + \cdots + b_0) \\ &= a_n x^n + (\text{lower order terms}) \end{aligned}$$

Since $f(x)$ and $a_n b_m^{-1} x^{n-m} g(x)$ have the same leading terms, it is cancelled in $h(x)$. So

$$\deg h(x) < \deg f(x) = n$$

Now, we apply induction hypothesis to $h(x)$ and $g(x)$. So there exists $q_1(x)$ and $r_1(x)$ such that

$$h(x) = g(x)q_1(x) + r_1(x)$$

with $r_1(x) = 0$ or $\deg r_1(x) < \deg g(x)$. But then,

$$\begin{aligned} f(x) &= h(x) + a_n b_m^{-1} x^{n-m} g(x) \\ &= [g(x)q_1(x) + r_1(x)] + a_n b_m^{-1} x^{n-m} g(x) \\ &= g(x)(q_1(x) + a_n b_m^{-1} x^{n-m}) + r_1(x) \\ &= g(x)q(x) + r(x) \end{aligned}$$

with $r(x) = 0$ or $\deg r(x) < \deg g(x)$. So we can always find $q(x)$ and $r(x)$.

Now, we want to show uniqueness. Suppose

$$\begin{aligned} f(x) &= g(x)q_1(x) + r_1(x) \\ &= g(x)q_2(x) + r_2(x) \end{aligned}$$

with $r_1(x) = 0$ or $\deg r_1(x) < \deg g(x)$ and $r_2(x) = 0$ or $\deg r_2(x) < \deg g(x)$. Thus,

$$g(x)q_1(x) + r_1(x) = g(x)q_2(x) + r_2(x)$$

So

$$g(x)(q_1(x) - q_2(x)) = r_2(x) - r_1(x).$$

If $q_1(x) - q_2(x) \neq 0$. then LHS has degree greater than $\deg g(x)$. But RHS has degree less than or equal to$\max\{\deg r_2(x), \deg r_1(x)\}$, which is less than $\deg g(x)$. This is a contradiction, so $q_1(x) = q_2(x)$, which implies $r_1(x) = r_2(x)$. □

Theorem 10.6. *Let F be a field, and $f(x) = F[x]$. Then, $f(a) = 0$ if and only if $f(x) = (x - a)g(x)$.*

Before we prove the theorem, we want to prove the following lemma first:

Lemma 10.1. *Let F be a field, $f(x) \in F[x]$. THen, for all $a \in F$,*

$$f(x) = (x-a)g(x) + f(a)$$

Proof. By division algorith,,

$$f(x) = (x-a)g(x) + r(x)$$

with $r(x) = 0$ or $\deg r(x) < \deg(x-a) = 1$. If $r(x) = 0$, $f(x) = (x-a)g(x)$, so $f(a) = 0$. So

$$f(x) = (x-a)g(x) + f(a)$$

IF $\deg r(x) < 1$, then $r(x) = c \in F$. So

$$f(x) = (x-a)g(x) + c$$

but then $f(a) = (a-a)g(a) + c = c$ So

$$f(x) = (x-a)g(x) + f(a)$$

□

So here is the proof for the theorem:

Proof. ($\Rightarrow$) By the lemma,

$$f(x) = (x-1)g(x) + f(a).$$

If $f(a) = a$ then $f(x) = (x-a)g(x)$.

($\Leftarrow$) If $f(x) = (x-a)g(x)$ then $f(a) = 0$. □

10.4 Irreducible Polynomials

Definition 10.5. *Let F be a field and $f(x) \in F[x]$, a non-constan polynomail. If $f(x)$ cannot be expressed as the product of two polynomials, $g(x)$ and $h(x)$, with smaller degree, i.e., $f(x) = g(x)h(x)$ with $0 < \deg g(x), \deg h(x) < \deg f(x)$, then $f(x)$ is irreducible. Otherwise, $f(x)$ is reducible.*

Example 10.4.1. Every polynomial of degree 1 is irreducible, i.e., $f(x) = ax + b$.

Example 10.4.2. x^2+1 is irreducible in $\mathbb{R}[x]$ but is reducible in $\mathbb{C}[x]$ ($x^2+1 = (x-i)(x+i)$).

Lemma 10.2. *Let $f(x) \in F[x]$ with $\deg f(x) \geq 2$. If there an $a \in F$ such that $f(a) = 0$, then f is reducible.*

Proof. Recall that

$$f(x) = (x-a)q(x) + f(a).$$

If $f(a) = 0$, then $f(x) = (x-a)q(x)$. Since $\deg f(x) \geq 2$, $\deg(x-a)q(x) = \deg(x-a) + \deg q(x) \geq 2$. So $\deg q(x) \geq 1$, so $f(x)$ is reducible. □

Corollary 10.1. *If $f(x)$ is irreducible, then $f(a) \neq 0$ for all $a \in F$.*

Note that the converse is not necessarily true. Even if $f(a) \neq 0$ for all $a \in F$, this does not mean that $f(x)$ that $f(x)$ is irreducible.

Example 10.4.3. $x^4 + 2x^2 + 1 = (x^2+1)(x^2+1)$ is reducible bus no root in $\mathbb{R}$.

Theorem 10.7. *Suppose $\deg f(x) = 2$ or 3. Then, $f(x)$ is irreducible if and only if $f(x)$ has no root in F.*

Proof. Proving the if statement follows directly from the previous corollary. Now, suppose $f(x)$ was reducible. T hen, $f(x) = g(x)h(x)$ with $1 \leq \deg g(x), \deg h(x) \leq \deg f(x)$ and $\deg g(x) + \deg h(x) = f(x)$. Since $\deg f(x)$ is either 2 or , at least one of the polynomials must have degree 1.

Without loss of generality, we can assume that $\deg g(x) = 1$, i.e. $g(x) = cx + d$. But then,

$$\begin{aligned} f(x) &= (cx+d)h(x) \\ \implies f(-c^{-1}d) &= 0 \end{aligned}$$

So $f(x)$ has a root, contradicting our assumption. Therefore, $f(x)$ must a reducible. □

Example 10.4.4. Show that $x^3 + x + 1$ is irreducible in $\mathbb{Z}_3[x.]$

Proof. Since $\deg \leq 3$, we can simply plug in all elements on $\mathbb{Z}_5$ and show that there are no roots:

$$\begin{aligned} 0^3 + 0 + 1 &= 1 \neq 0 \\ 1^3 + 1 + 1 &= 3 \neq 0 \\ 2^3 + 2 + 1 &= 1 \neq 0 \\ 3^3 + 3 + 1 &= 1 \neq 0 \\ 4^3 + 4 + 1 &= 1 \neq 0 \end{aligned}$$

□

10.5 Factor in $\mathbb{Q}[x]$

If $f(x) \in \mathbb{Q}[x]$, then there exists c, a least common multiple of all the coefficients in $f(x)$ such that $cf(x) \in \mathbb{Z}[x]$. So we can consider factoring in $\mathbb{Q}[x]$ equivalent to factoring in $\mathbb{Z}[x]$.

Theorem 10.8. *Let $f(x) = a_n x^n + \cdots + x_0 \in \mathbb{Z}[x]$. If $r \neq 0$, and if r/x is a root of $f(x)$, then $r|a_0$ and $s|a_n$.*

Proof. We are given

$$a_n\left(\frac{r}{s}\right)^n + a_{n-1}\left(\frac{r}{s}\right)^{n-1} + \cdots + a_1\left(\frac{r}{s}\right) + a_0 = 0.$$

So multiply both sides by s^n:

$$\begin{aligned} a_n r^n + a_{n-1}r^{n-1}s + \cdots + a_1 r s^{n-1} + a_0 s^n &= 0 \\ \iff s\left(a_{n-1}r^{n-1} + \cdots + a_0 s^{n-1}\right) &= -a_n r^n \end{aligned}$$

So $s| - a_n r^n$ but $\gcd(r,s) = 1$. So $s|a_n$. Note that the above equation also implies that

$$r(a_n r^{n-1} + \cdots + a_1 s^{n-1}) = -a_0 s^n$$

So $r|a_0$ for similar reasons. □

Example 10.5.1. Find a root of

$$f(x) = 2x^4 + 7x^3 + 5x^2 + 7x + 3$$

in $\mathbb{Q}$.

By the above result, $r|3$ and $s|2$ if r/s is a root. So

$$\begin{aligned} r|3 &\implies r = \pm 1 \text{ or } \pm 3 \\ r|2 &\implies r = \pm 1 \text{ or } \pm 2 \end{aligned}$$

So the posible values of r/s are

(r,s)	1	-1	2	-2
1	1	-1	1/2	-1/2
-1	-1	1	-1/2	1/2
3	3	-3	3/2	-3/2
-3	-3	3	-3/2	3/2

So we just have to check $1, -1, 3, -3, 1/2, -1/2, 3/2, -3/2$. We can also eliminate all positive rationals because $f(x)$ will be positive when $x > 0$. Then, we find that

$$f(-1/2) = 0 \text{ and } f(-3) = 0.$$

Theorem 10.9 (Eisenstein's criterion)**.** *Let*

$$f(x) = a_n x^n + \cdots a_0 \in \mathbb{Z}[x]$$

If there exists a prime p such that $p|a_0, p|a_1, \ldots, p|a_{n-1}, p \nmid a_n$ and $p^2 \nmid a_0$, then $f(x)$ is irreducible.

Example 10.5.2. Consider

$$f(x) = x^{17} + 6x^{13} - 15x^4 + 3x^2 - 0x + 12$$

Using $p = 3$, we can conclude that $f(x)$ is irreducible over $\mathbb{Q}[x]$.

Example 10.5.3. There are irreducible polynomials of every degree over $\mathbb{Q}[x]$. For example, we can take $f(x) = x^n + p$ with p prime.

10.6 Similarities between $F[x]$ and $\mathbb{Z}$

Definition 10.6. *A plynomail $d(f) \in F[x]$ is monic if its leading coefficient is 1.*

A monic polynomail $d(x)$ is the greatest common divisors of two polynomials $p(x)$ and $q(x)$ if $d(x)|p(x)$ and $d(x)|q(x)$, and if $d'(x)$ is any other monic polynomial such that $d'(x)|p(x)$ and $d'(x)|q(x)$, then $d'(x)|d(x)$. Like $\mathbb{Z}$, we can use the division algorithm to find $\gcd(p(x), q(x))$.

Example 10.6.1. Consider

$$\begin{aligned} f(x) &= 2x^4 + 5x^3 - 5x - 2 \\ g(x) &= 2x^3 - 3x^2 - 2x \end{aligned}$$

Then,

$$\begin{aligned} (2x^4 + 5x^3 - 5x - 2) &= (2x^3 - 3x^2 - 2x)(x+4) + (14x^2 + 3x - 2) \\ (2x^3 - 3x^2 - 2x) &= (14x^2 + 3x - 2)\left(\frac{1}{2}x - \frac{12}{49}\right) + \left(-\frac{48}{49}x - \frac{24}{49}\right) \\ (14x^2 + 3x - 2) &= \left(-\frac{48}{49}x - \frac{24}{49}\right)\left(-\frac{343}{24}x + \frac{49}{12}\right) + 0 \end{aligned}$$

Then, we can rescale last nonzero remainder to make it monic to find that

$$\gcd(f, g) = x + \frac{1}{2}$$

Definition 10.7. *An ideal $I \subseteq R$ is principal if there exists $e \in R$ such that*

$$I = \{re | r \in R\} = \langle e \rangle.$$

Theorem 10.10. *Every ideal of $\mathbb{Z}$ is principal.*

Proof. If $I = \{0\}$, then $I = \langle 0 \rangle$. Suppose $a \in I$ with $a \neq 0$. So either a or $-a$ is positive and is in I. So I has a smallest positive element, say c.

We claim that $I = \langle c \rangle$. Since $c \in I$, $\langle c \rangle \subseteq I$. Let $a \in I$, By division algorithm, $a = cq + r$ with $0 \leq r < c$. If $r \neq 0$, then $r = a - cq$. But then,

$$a, c \in I \implies r \in I.$$

This contradicts the fact that c is the smallest element in I. So $r = 0$. So $a = cq \in \langle c \rangle$. Thus, every ideal is principal. □

Theorem 10.11. *Every ideal of $F[x]$ is principal.*

Proof. If $I = \{0\}$, then $I = \langle 0 \rangle$. So suppose $0 \neq p(x) \in I$. If $\deg p(x) = 0$, then $p(x) = k \in F$. But then $1 \in I$ and $\langle 1 \rangle = I = R$.

Suppose $\deg p(x) > 0$. Let $c(x)$ be the polynomial of smallest degree in I. Let $c(x)$ be the polynomail of smallest degree in I. Then, I claim that $I = \langle c(x) \rangle$.

Since $c(x) \in I$, $\langle c(x) \rangle \in I$. Let $a(x) \in I$. By division algorithem,

$$a(x) = c(x)q(x) + r(x)$$

with $r(x) = 0$ or $\deg r(x) < \deg c(x)$. If $r(x) \neq 0$, then

$$r(x) = a(x) - c(x)q(x) \in I.$$

But this contradicts the fact that $c(x)$ has smallest degree in I. So $r(x) = 0$. Then, $a(x) = c(x)q(x) \in \langle c(x) \rangle$. So every ideal of $F[x]$ is principal. □

Definition 10.8. *Let R be a commutative ring with identity. An integral domain R is a principal ideal domin (PID) if every ideal is principal.*

Example 10.6.2. $\mathbb{Z}$ and $F[x]$ are PIDs.

Note that not every integral domain is a PID.

Example 10.6.3. Consider the following domain:

$$R = \mathbb{Z}[x].$$

Then,

$$I = \langle 6, x \rangle = \{6f + xg | f, g \in R\}$$

is not principal. Supppose

$$I = \langle 6, x \rangle = \langle c \rangle.$$

So

$$6 \in \langle c \rangle \implies 6 = cl.$$

and

$$x \in \langle c \rangle \implies x = ct$$

Since $\deg 6 = 0$, this implies that

$$\deg c = 0,$$

so $c \in \mathbb{Z}$. So

$$x = ct \implies \deg t = 1.$$

So $t = ax + b$. Thus, $x = cax + cb$ But $cb = 0$, and

$$c \neq 0 \implies b = 0.$$

So $a = c^{-1}$. So c is a unit in $\mathbb{Z}$. So $c = 1, -1$. But then

$$\langle c \rangle = \langle 1 \rangle = \mathbb{Z}[x],$$

but $1 \notin \langle 6, x \rangle$.

Definition 10.9. *A domain D is a Euclidean domain if there is a function $v : D \to \mathbb{N}$ such that*

- *If a, b are non-zero elements, $v(a) \leq v(a, b)$.*
- *If $a, b \in D$ and $b \neq q$, then there exists q and r such that*

$$a = bq + r$$

with $r = 0$ or $v(r) < v(b)$. Here, v is called a valuation.

Example 10.6.4. $\mathbb{Z}$ is a Euclidean domain. $v : \mathbb{Z} \to \mathbb{N}$ defined by $v(a) = |a|$.

Example 10.6.5. $F[x]$ is a Euclidean domain. $v : F[x] \to \mathbb{N}$ is given by $v(f(x)) = \deg f(x)$.

Theorem 10.12. *Every Euclidean domain is a PID.*

Proof. Let $v : D \to \mathbb{N}$ be the valuation. If $I = \{0\}$, then $I = \langle 0 \rangle$.

If $I \neq \{0\}$, let $c \in I$ with $v(c)$ smallest. I claim that $I = \langle c \rangle$. Since $c \in I$, $\langle c \rangle \subseteq I$. Let $a \in I$. Since D is a Euclidean domain, ther exists q and r such that

$$a = cq + r$$

with $r = 0$ or $v(r) < v(c)$. If $r \neq 0$, then $r(x) = a(x) - c(x)q(x) \in I$ with $v(r) < v(c)$. But this contradicts choice of c. So $r = 0$. □