McGill Algebra I Lectures (Math 235)

Hy Vu

Professor: Magid Sabbagh

August 2024

Foreword

Mathematics and Statistics: Sets, functions and relations. Methods of proof. Complex numbers. Divisibility theory for integers and modular arithmetic. Divisibility theory for polynomials. Rings, ideals and quotient rings. Fields and construction of fields from polynomial rings. Groups, subgroups and cosets; homomorphisms and quotient groups. This note includes all the lectures for fall 2024.

This note includes a few terminologies. The following is the brief description of each terms:

1. **Definition:** An explanation of a mathematical term.

2. **Theorem:** An important statement that can be proven to be true.

3. **Corollary:** A deduction from a theorem that can be proven to be true.

4. **Proposition:** A less important statement that can be proven to be true.

5. **Lemma:** A statement that can be proven to be true (relevant to prove another result).

6. **Proof:** An explanation of why statement is true.

Prerequisites: MATH 133 (linear algebra) and or equivalent.

Contents

Lecture 1: August 28th, 2024

1 Sets and Functions

Definition 1.1. A **set** is a well-defined collection of objects. It's defined in a way that allows us to determine whether or not a abstract object x belongs to a set. N.B. Most of the time, if not all, a set is symbolized as a capital letter e.g. A, B, H, etc.

Definition 1.2. When an object belongs to a set, we call said object **element** and is written as

$$x \in A \tag{1.1}$$

read as "x belongs to A" (where x is the element of A). On the contrary, if an object x does not belong to a set A, we denote it as

$$x \notin A \tag{1.2}$$

read as "x does not belong to A".

Remark 1.1. *A set is specified by either: listing its elements (if possible) or by stating a property that its elements have to satisfy.*

Example 1.0.1. $A = \{1,2,3,4\}$, $E = \{\text{set of even numbers}\}$. For the set E, we can make it "mathematics-like". To do so, notice that even numbers are all divisible by 2 which means we can construct a set of even numbers by using 2 as a multiple for all the integers. That is, $E = \{2x : x \in \mathbb{Z}\}$.
N.B. the symbol ":" means "such that". There are variations of this too like: "s.t." or "|".

We can represent intervals in set notations too like:

- $A = [1,3] = \{x : 1 \le x \le 3\}$
- $B = (1,3] = \{x : 1 < x \le 3\}$[1]

The following are important sets that we may use through out the course.

1. **The Natural Number:** $\mathbb{N} = \{1,2,3,\dots\} = \{x : x \text{ are positive integers}\}$[2]

[1] In this course, you can either use open square bracket "][" or parentheses "()" for an open interval.

[2] The set of natural number we'll be using, does not include 0

2. **The Integer:** $\mathbb{Z} = \{\dots, -1, 0, 1, \dots\} = \{x : x \text{ are integers}\}$

3. **The Rational Number:** $\mathbb{Q} = \{x : x \text{ are rationals}\} = \left\{\frac{p}{q} : p, q \in , q \neq 0\right\}$

4. **The Real Number:** $\mathbb{R} = \{x : x \text{ are reals}\} = (-\infty, +\infty)$

Definition 1.3. A set A is a **subset** of a set B if $\forall x \in \implies x \in B$.[3] We denote A is a subset of B as

$$A \subset B \tag{1.3}$$

Example 1.0.2. $\{1,2\} \subset \{1,2,3\}$, $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$, and $[2,3) \subset \mathbb{R}$ but $\not\subset \mathbb{N}$.

Definition 1.4. If set A and B have the same element, then A and B are said to be **equal** which is denoted as

$$A = B \tag{1.4}$$

Remark 1.2. *In a typical proof, if you want to show that $A = B$, you must first prove that $A \subset B$ and $B \subset A$. This is similar to saying $1 = 1$ because only $1 \leq 1$ and $1 \geq 1$.*

Example 1.0.3. Let $E = \{2n : n \in \mathbb{Z}\}$ and $A = \{4n : n \in \mathbb{Z}\}$. Show that $A \in E$.

Proof. Let $x \in A$ then we can find an $n : x = 4n$ which also means $x = 4n = 2(2n)$. Since n is an integer, $2n$ is also an integer which means x is even and divisible by 2 $\implies x \in E$. So $x \in A \implies x \in E$ hence $A \subset E$. □

The opposite is not true since we can find a counterexample, that is, $2 \in E$ but $\notin A$.

1.1 Operations of Set

Definition 1.5. Let A and B be sets then, the **union** of A is B is defined and written as:

$$A \cup B = \{x : x \in A \text{ or } x \in B\} \tag{1.5}$$

and the **intersection** of A and B is defined as:

$$A \cap B = \{x : x \in A \text{ and } x \in B\} \tag{1.6}$$

Example 1.1.1. $\{1,2,3\} \cap \{3,4,5\} = \{3\}$ and $\{1,2,3\} \cup \{3,4,5\} = \{1,2,3,4,5\}$.

[3] "$\forall$" means "for all", and "$\implies$" means "implies".

1.1.1 Properties of Operations

Like any arithmetic operations (+,-,etc.), these 2 set operations also have its own law and properties.

Theorem 1.1. ***(Distributive Law)*** *Let A, B_1 and B_2 be sets. Then,*

$$A \cup (B_1 \cap B_2) = (A \cup B_1) \cap (A \cup B_2) \tag{1.7}$$

Proof.

$$\begin{aligned} A \cup (B_1 \cap B_2) &= A \cup \{x : x \in B_1 \text{ and } x \in B_2\} \\ &= \{x : x \in A \text{ or } (x \in B_1 \text{ and } x \in B_2)\} \\ &= \{x : (x \in A \text{ or } x \in B_1) \text{ and } (x \in A \text{ or } x \in B_2)\} \\ &= (A \cup B_1) \cap (A \cup B_2) \end{aligned}$$

□

An alternative way of proving it is the following:

Proof. We must show that $A \cup (B_1 \cap B_2) \subset (A \cup B_1) \cap (A \cup B_2)$. So, let $x \in A \cup (B_1 \cap B_2) \implies x \in A$ or $x \in (B_1 \cap B_2)$.

- If $x \in A$ then, $x \in A \cup B_1$ and $x \in A \cup B_2$ hence $x \in (A \cup B_1) \cap (A \cup B_2)$.
- If $x \in (B_1 \cap B_2)$ then, $x \in B_1$ and $x \in B_2 \implies x \in B_1 \cup A$ and $x \in B_2 \cup A$ hence $x \in (A \cup B_1) \cap (A \cup B_2)$.

□

End of Lecture

Definition 1.6. Let A be a set then the **complement** of a set is defined as

$$A' = \{x : x \notin A\} \tag{1.8}$$

Example 1.1.2. Let $U = \mathbb{R}$ and $A = [1,3)$ then $A' = (-\infty, 1) \cup [3, \infty)$

Theorem 1.2. ***(De Morgan's Law).*** *If A and B are sets then*

1. $(A \cup B)' = A' \cap B'$
2. $(A \cap B)' = A' \cup B'$

Lecture 2: August 30th, 2024

Proof. We first prove that $(A \cup B)' \subseteq A' \cap B'$. Let $x \in (A \cup B)'$. We need to show that $x \in A' \cup B'$.

$$\begin{aligned} x \in (A \cup B)' &\implies x \in A' \text{ and } x \in B' \\ &\implies x \notin A \text{ and } x \notin B \\ &\implies x \notin A \cup B \\ &\implies x \notin (A \cup B)' \end{aligned}$$

So $(A \cup B)' \subseteq A' \cap B'$. To make sure that they're equal, we need to also show $A' \cap B' \subseteq (A \cup B)'$.

$$\begin{aligned} \text{Let } x \in A' \cap B' &\implies x \in A' x \in B' && (1.9) \\ &\implies x \notin A \wedge x \notin B && (1.10) \\ &\implies x \notin A \cup B && (1.11) \\ &\implies x \in (A \cup B)' && (1.12) \end{aligned}$$

So $A' \cap B' \subseteq (A \cup B)'$. With the above, we will get that $x \in (A \cup B)' \iff x \in A' \cap B'$.[4] For the proof of the $(A \cap B)' = A' \cup B'$, it follows the same structure as the first. □

1.2 Cartesian Product

Definition 1.7. Let A and B be sets then the **Cartesian product** of A and B is defined by

$$A \times B = \{(a, b) : a \in A \wedge b \in B\} \tag{1.13}$$

Example 1.2.1. $A = \{1, 2\}$ and $B = \{a, b, c\}$ so $A \times B = \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c)\}$

Definition 1.8. A **function** $f : A \to B$ is a subset $f \subset A \times B$ such that $\forall a \in A, \exists! b : (a, b) \in f$.[5] We write

$$f(a) = b \tag{1.14}$$

Example 1.2.2. Using the same set A and B as example 1.2.1 then,

1. $f = \{(1, a), (1, b), (2, a)\}$ is not a function from $A \to B$.

2. $f = \{(1, a), (2, a)\}$ is a function from $A \to B$.

[4] The symbol " $\iff$ " stands for "if and only if" or "implies both way".

[5] "$\exists!$" means "there exists uniquely one". If "!" is removed, it will be "there exists".

1.2.1 Properties of Function

Definition 1.9. Let A and B be sets and $f : A \to B$. Then, f is said to be **injective (one-to-one)** if $\forall a_1, a_2 \in A, f(a_1) = f(a_2) \iff a_1 = a_2$.

Example 1.2.3. $f : \mathbb{R} \to \mathbb{R}, f(x) = x^2$. f is not injective since $f(1) = f(-1) = 1$. For $f : \mathbb{R}_0^+ \to \mathbb{R}, f(x) = x^2$. f is injective (see the following proof)

Proof. Let $a_1, a_2 \in \mathbb{R}_0^+$ such that $f(a_1) = f(a_2)$. Then, $a_1^2 = a_1^2 \implies \sqrt{a_1^2} = \sqrt{a_2^2} \implies |a_1| = |a_2|$ so $a_1 = a_2$. □

Definition 1.10. $f : A \to B$ is said to be **surjective (onto)** if $\forall b \in B, \exists a \in A : f(a) = b$ i.e. For every $b \in B$, there have to be at least 1 pre-image in A.

Example 1.2.4. The following mappings are either not surjective or surjective

$$\begin{tikzcd} & 1 \arrow[r] & a & & & & \\ & & & & & 1 \arrow[r] & a \\ f: & 2 \arrow[r] & b & \text{is surjective,} & f: & 2 \arrow[r] & b & \text{is surjective} \\ & 3 \arrow[r] & c & & & 3 \arrow[ru] & \\ & & d & & & & \end{tikzcd}$$

Definition 1.11. A function $f : A \to B$ is said to be **bijective** if f is both surjective and injective

Example 1.2.5. The following function is bijective.

$$\begin{tikzcd} & 1 \arrow[rdd] & a \\ f: & 2 \arrow[r] & b \\ & 3 \arrow[ruu] & c \end{tikzcd}$$

1.2.2 Composition of Function

Definition 1.12. Let A, B and C be sets and $f : A \to B$ and $g : B \to C$ be functions then the **composition** of f and g is denoted as

$$g \circ f : A \to C \tag{1.15}$$

Which simply means

$$(g \circ f)(a) = g(f(a)) \tag{1.16}$$

Example 1.2.6. Consider the following function composition $(g \circ f)(a) := g(f(a))$

$$\begin{tikzcd}
1 \arrow[r, "f"] & a \arrow[r, "g"] & \alpha \\
2 \arrow[r] & b \arrow[dr] & \beta \\
3 \arrow[r] & c \arrow[ur] & \gamma
\end{tikzcd}$$

Then, $(g \circ f)(1) = g(f(1)) = g(a) = \alpha$ and $(g \circ f)(3) = \beta$

Theorem 1.3. *Let $f : A \to B$ and $g : B \to C$ be functions.*

1. *If f and g are injective then so is $g \circ f$.*
2. *If f and g are surjective then so is $g \circ f$.*
3. *If $g \circ f$ is injective then f is injective.*
4. *If $g \circ f$ is injective and f is surjective then g is surjective.*
5. *If $g \circ f$ is surjective and g is injective then f is surjective.*

Proof. 1. We need to show that if $a_1, a_2 \in A$ and $g \circ f(a_1) = (g \circ f)(a_2)$ then $a_1 = a_2$.

$$\begin{aligned}
(g \circ f)(a_1) &= (g \circ f)(a_2) \\
g(f(a_1)) &= g(f(a_2)) \\
f(a_1) &= f(a_2) && \text{since } g \text{ is injective} \\
a_1 &= a_2 && \text{since } f \text{ is injective}
\end{aligned}$$

□

End of Lecture

1.3 Inverse of Functions

Definition 1.13. Let S be a set and let 1_S or Id_S be the function $1_S : S \to S, 1_S(x) = x, \forall x \in S$. We call this function the **identity function of S**.

Definition 1.14. Let $f : A \to B$ be a function. We say that $f : B \to A$ is the **inverse of f** if

$$f \circ g = 1_B \tag{1.17}$$

i.e. $f(g(b)) = b \forall b \in B$; and,

$$g \circ f = 1_A \tag{1.18}$$

i.e. $g(f(a)) = a \forall a \in A$.

Lecture 3: September 4th, 2024

Example 1.3.1. The function $f:\mathbb{R}_0^+ \to \mathbb{R}, x \mapsto \ln x$ is the inverse of the function $g:\mathbb{R}\to\mathbb{R}_0^+, y \mapsto e^y$ and v.v.

Proof. $f(g(y)) = \ln e^y = y$ and $g(f(x)) = e^{\ln x} = x$ □

Theorem 1.4. *Let $f : A \to B$ be a function. Then, f is bijective $\iff$ f has an inverse.*

Proof. ($\Longleftarrow$) Supposed that f has an inverse, let $g : B \to A$ be an inverse of f. We then wants to show that f is bijective i.e. both injective and surjective. First, let $a_1, a_2 \in A : f(a_1) = f(a_2)$ then,

$$\begin{aligned} g(f(a_1)) &= g(f(a_2)) \\ 1_A(a_1) &= 1_A(a_2) \\ a_1 &= a_2 \end{aligned}$$

Hence f is injective. Now, let $b \in B$ so that $g(b) \in A$ then,

$$(f \circ g)(b) = f(g(b)) = 1_B(b) = b$$

So if we let $g(b) = a \implies f(a) = b$ hence, f is surjective. If f is both surjective and injective, it's bijective. □

Theorem 1.5. *Let $f : A \to B$ be a bijective function then the inverse of f, denoted as f^{-1} is unique.*

Proof. ... □

1.4 Equivalence Relation

Definition 1.15. Let X be a set then, an **equivalence relation** on X is a subset $R \subset X \times X$ with the following properties.

a) **(Reflexivity)** If $x \in X$ then $(x, x) \in R$.

b) **(Symmetry)** If $x, y \in X$ then $(x, y) \in R \implies (y, x) \in R$.

c) **(Transitivity)** If $x, y, z \in X$ then $(x, y \in R)$ and $(y, z) \in R \implies (x, z) \in R$.

Remark 1.3. *We say that $x \sim_R y$ if $(x, y) \in R$.* [6]

[6] Another convention of writing this is using the R i.e. $x \sim_R y$ is the same as writing xRy.

Example 1.4.1. Let X be a set and $x, y \in X$ then $x \sim y$ if $x = y$

Proof. Let $x \in X$ then $x = x \implies x \sim x$ (reflexivity). If $x \sim y$ then $x = y \implies y = x \implies y \sim x$ (symmetry). If $x \sim y \implies x = y$ and $y \sim z \implies y = z$ then $x = z \implies x \sim z$ (transitivity). □

Example 1.4.2. Let $x = \mathbb{Z}$ and let $x, y \in \mathbb{Z}$ then $x \sim y$ if $3 \mid x - y$.[7]

Proof. $x \sim x \implies x - x = 0$ and $3 \mid 0$. $x \sim y \implies x - y \implies -(x - y)$ which are both divisible by 3, but $-(x-y) = y - x$ so then $y \implies x$. Supposed $x \sim y \implies x - y = 3b$ and $y \sim z \implies y - z = 3c$ for some $b, c \in \mathbb{Z}$. Then, $x - z \implies x - y + y - z = 3b + 3l = 3(b+1)$ so $3 \mid x - z$ so $x \sim z$. □

Definition 1.16. Let $x \in X$ and $\sim$ be an equivalence reaation on X. Then, the **equivalence class of X**, denoted as $[X]$ or $[x]_R$, is defined as

$$[x]_R = \left\{y \in X : x \sim y\right\} \tag{1.19}$$

Example 1.4.3. Let $X = \mathbb{Z}$ and $x \sim y$ if $3 \mid x - y$. Then, we can defined the equivalence class of 0 and 1 as

$$\begin{aligned}[0] &= \left\{y \in \mathbb{Z} : 3 \mid y - 0\right\} \\ &= \left\{y \in \mathbb{Z} : y = 3a \text{ for some } a \in \mathbb{Z}\right\} \\ &= \{\dots, -3, 0, 3, \dots\} \\ &= 3\{\dots, -1, 0, 1, \dots\} = 3\mathbb{Z}\end{aligned} \qquad \begin{aligned}[1] &= \left\{y \in \mathbb{Z} : y - 1 = 3a \text{ for some } a \in \mathbb{Z}\right\} \\ &= \{\dots, -2, 1, 4, 7, \dots\} \\ &= \{\dots, -3, 0, 3, 6, \dots\} - 1 = 3\mathbb{Z} - 1\end{aligned}$$

You'll realize also that $[0] = [3] = 3\mathbb{Z}$ and $[1] = [4] = 3\mathbb{Z} + 1$

End of Lecture

Theorem 1.6. *Let $x, y \in X$, then*

1. $[x]_R \neq \emptyset$
2. *If $y \in [x]_R$ then $[x]_R = [y]_R$*
3. $[x]_R \cap [y]_R = \emptyset$ *or* $[x]_R = [y]_R$

Proof. 1) $x \in [x]_R$ since $x \sim_R x$ so $[x]_R \neq \emptyset$
2) Let $y \in [x]_R$, we need to show $[x]_R = [y]_R$ which means we need to show $[x]_R \subseteq [y]_R$ and $[y]_R \subseteq [x]_R$. So let $z \in [y]_R$ then we need to show $z \in [x]_R$. If $z \in [y]_R$ then $z \sim_R y$ and $y \in [x]_R$ (or $y \sim_R x$). So by properties of R, $z \sim_R$

[7] $a|b$ means b is divisible by a

Lecture 4: September 6^{th}, 2024

$x \implies z \in [x]_R \implies [y]_R \subseteq [x]_R$. The fact that $[x]_R \subseteq [y]_R$ also holds since $x \sim_R y$ then $y \sim_R x$. We've already shown that $y \sim_R x$, then by symmetry of R, $x \sim_R y \implies [x]_R \subseteq [y]_R$. Thus $[x]_R = [y]_R$.
3) If $[x]_R \cap [y]_R =$ then there's nothing to prove. If $[x]_R \cap [y]_R \neq$ then let $z \in [x]_R \cap [y]_R$. This means $z \in [x]_R \implies [z]_R = [x]_R$ and similarly, $z \in [y]_R \implies [z]_R = [y]_R$. Thus $[z]_R = [x]_R = [y]_R \implies [x]_R = [y]_R$. □

Example 1.4.4. Recall, let $x, y \in \mathbb{Z}$ and $x \sim_R y$ if $3 \mid x - y$. From last time, we know that $[0] = 3\mathbb{Z}$. Since $3 \in [0]$ then $[3] = [0]$. Similarly for $[1]$ and $[4]$, and $[2]$ and $[8]$, etc.

Notice that when writing out all the equivalence class, 1 element will appear. This also means that when we take the union of all the equivalence class, we will get the original set.

Remark 1.4. *x for $[x]_R$ is called the **representative** of its equivalence class.*

Definition 1.17. Let X be a set. A **partition** of X is a collection of subsets $\{X_i\}$ of X such that

1. $X_i \neq \emptyset, \forall i$
2. $X_i \cap X_j = \emptyset$ if $i \neq j$
3. $X = \bigcup_i X_i$

Theorem 1.7.

1. *Let R be an equivalence relation on X. Then, the equivalence class of X forms a partition of X. And $X = \bigcup_{i \in I} [x_i]_R$ is a set of representatives of equivalence classes.*
2. *Let $\{X_i\}_{i \in I}$ be a partition of X. Then $\exists R$ on X whose equivalence classes are the X.*

where I is an index set.

Hint: $x \sim y$ if $x, y \in X_i$ for some $i \in I$.

2 Integers and Induction

Well-Ordering Principle. Let $S \subset \mathbb{N}$ is not $\emptyset$. Then S has a minimal element.

First Principle of Mathematical Induction. Let $S \subset \mathbb{N}$ such that

1. $1 \in S$.
2. If $n \in S$ then $n+1 \in S$.

Then $S = \mathbb{N}$

Theorem 2.1. *The well-ordering principle implies the first principle of mathematical induction.*

Proof. Suppose that $S \subseteq \mathbb{N}$ with the following porperties: $1 \in S$ and $n \in S \implies n+1 \in S$. Suppose that $S \neq \mathbb{N}$. Then, $S' \neq \emptyset$ which by the well-ordering principles, S' has a least element $m \in \mathbb{N}$. $m-1 \notin S'$ since m is the least element thus $m-1 \in S$. Then, $(m-1)+1 = m \in S$ which is a contradiction. □

End of Lecture

Lecture 5: September 9^{th}, 2024.

Definition 2.1. Let $a, b \in \mathbb{Z}, b \neq 0$. We say ***b* divides *a*** uf $\exists k \in \mathbb{Z} : a = kb$. We denote this as $b \mid a$.

Example 2.0.1. $2 \mid 4$,

Theorem 2.2. *Let $a, b, c \in \mathbb{Z} : a, b \neq 0$. If $a \mid b$ and $b \mid c$ then $a \mid c$.*

Proof. If $a \mid b$ then $b = ka$ for some $k \in \mathbb{Z}$. If $b \mid c$ then $c = rb$ for some $r \in \mathbb{Z}$. Thus, $c = r(ka) = (rk)a$ hence $c \mid a$. □

Definition 2.2. Let $p > 1$ and $p \in \mathbb{N}$ Then p is a **prime number** if the only divisor for p is ± 1 and $\pm p$

Example 2.0.2. 2 is a prime, 7 is a prime and 4 is not a prime

Theorem 2.3. *Let $n > 1$ be an integer that is not prime. Then, n has a prime divisor p and $p \leq \sqrt{n}$*

Proof. Let S be the set of positive divisors of n that are strictly bigger than 1. This also means that $S \subseteq \mathbb{N}$ and $S \neq \emptyset$ (since $n \in S$). S has a least element p; which we need to show p is prime. Suppose p is not prime then $\exists d \in \mathbb{N}$ such that $1 < d < p$ and $d|p$, but also $p|n$ which means that $d|n$ which is a contradiction since p is not the least element anymore. So p is a prime.
Now, $p|n$ is simply $n = pq$ for some $q \in \mathbb{N}$. We can also say $q \mid n$ and $q < 1$ which means $q \in S \implies q \geq p \implies n = pq \geq p^2 \implies p \leq \sqrt{n}$. Hence every $n \in \mathbb{N}$ with $n > 1$ has prime divisor. □

Corollary 2.1. *There are infinitely many prime numbers*

Definition 2.3. Suppose that there are finitely many prime numbers: $p_1 < p_2 < \cdots < p_n$. Let $N = p_1 p_2 \cdots p_n + 1$. N is not a prime since $N > p_n$ and it must have a prime divisor i.e. $\exists p_i$ for some $i \in \{1, 2, \ldots, n\}$ such that $p_i \mid N$. $p_i \mid N$ and $p_i | p_1 \cdots p_n \implies p_i \mid N - (p_1 \cdots p_n) = 1$ which is a contradiction sine $p_i > 1$. Therefore, there are infinitely many prime numbers.

2.1 Euclidean Division

Theorem 2.4. *Let $a, b \in \mathbb{Z}$ with $b > 0$. Then, $\exists! q, r$ with $0 < r < b$ such that*

$$a = bq + r \tag{2.1}$$

r is called the remainder of Euclidean division of a by b.

Proof. Homework exercise 1. □

Example 2.1.1. $34 = 6 \times 5 + 4$, $101 = 14 \times 7 + 3$.

Definition 2.4. Let a and b be 2 integers not both 0. The **greatest common divisor** of a and b is the largest positive divisor that divides both a and b. This is denoted as $\text{GCD}(a, b)$.

Example 2.1.2. $\text{GCD}(2, 5) = 1$, $\text{GCD}(7, 14) = 7$.

Theorem 2.5. ***(Bezout's Theorem).*** *Let $a, b \in \mathbb{Z}$ and not both 0. $\exists u, v \in \mathbb{Z}$: $au + bv = GCD(a, b)$. Moreover, if d is a common divisor of a and b then d divides $gcd(a, b)$.*

End of Lecture

Proof. Let $S = \{ma + nb : m, n \in \mathbb{Z}$ and $ma + nb > 0\}$. So, $S \neq \emptyset$ and $S \subseteq \mathbb{N}$. Then, for $m = a$ and $n = b$ then $a^2 + b^2 > 0$ since $(a, b) \neq (0, 0)$. So, S has a least element $D = au + bv$ for some $u, v \in \mathbb{Z}$.

Lecture 6: September 11th, 2024.

Claim: $D \mid a$
If $D \mid a$ then $a = qD + r$ where $q \in \mathbb{Z}$ and $0 \geq r < d$. Thus $r = a - qD = a - q(au + bv) = (1 - qu)a - (vq)b$

Claim: $r = 0$
Assume $r \neq 0$, then $0 < r < D$. r is an integer linear combination of a and $r > 0 \implies r \in S$ which is a contradiction since D is the minimal element in $S \implies r = 0 \implies a = qD + r = qD \implies D \mid a$. Similarly, we can do that claim for b thus $D \mid b$.

claim: If $d \mid a$ and $d \mid b$ and $D = au + bv$. D is a common divisor of a and b then $d \leq \gcd(a, b)$.
Since $\gcd(a, b)$ divides both a and $b \implies \gcd(a, b)$ divides both au and bv. Then $\gcd(a, b) \mid au+bv = D$ so $\gcd(a, b) \leq D$. Then, $\gcd(a, b) = D = au+bv$. (This proved the first part of the theorem).

Claim: Let d be a common divisor of a and b then $d \mid \gcd(a, b)$.
If d is a common divisor of a and b then $d \mid a$ and $d \mid b \implies d \mid au$ and $d \mid bv \implies d \mid au + bv = D = \gcd(a, b)$ □

How do you find *u* and *v*? Well...let's look at an example.

Example 2.1.3. $\gcd(2, 1) = 1 \implies 2 \times 1 + 1 \times (-1) = 1$ or $2 \times 3 + 1 \times (-5)$.

Obviously, determining u and d would be challenging as writing it as a linear combination would yield a host of different unique solution. Luckily, we have the Euclidean algorithm.

Example 2.1.4. $\gcd(120, 14) = 2$ then $120 = 14 \times 8 + 8$, we will now do the Euclidean division between the divisor 14 (of 120) and remainder 8 (of 120/14) which means $14 = 8 \times 1 + 6$ then $8 = 6 \times 1 + 2$ then $6 = 2 \times 3 + 0$.

Similarly, $\gcd(150, 9) = 3$ which means $150 = 9 \times 16 + 6 \implies 9 = 6 \times 1 + 3 \implies 6 = 2 \times 3 + 0$

What we'll notice that the algorithm will lead to a remainder of 0 and the remainder prior to that is the gcd. Now let's figure out how to format it.

We'll first look back at example 2.1.4 for $\gcd(120, 14) = 2$ that

$$\begin{aligned} 2 &= 8 - 6 \times 1 \\ &= 8 - (14 - 8 \times 1) \times 1 \\ &= -14 + 2 \times 8 \\ &= -14 + 2 \times (120 - 14 \times 8) \\ &= 2 \times 120 - 14 \times 17 \end{aligned}$$

Basically, we're getting the linear combination of the 2 element in gcd.

Example 2.1.5. $\gcd(252, 105)$, then $252 = 105 \times 2 + 42 \implies 105 = 42 \times 2 + 21 \implies 42 = 21 \times 2 + 0$

$$\begin{aligned} \implies 21 = 105 - 42 \times 21 &= 105 - (252 - 105 \times 2) \times 2 \\ &= 105 - 252 \times 2 + 105 \times 4 \\ &= 105 \times 5 - 252 \times 2 \end{aligned}$$

Theorem 2.6. ***(Euclidean Algorithm).*** *Let $a, b \in \mathbb{Z}$ with $b > 0$. Construct the following algorithm to find $\gcd(a, b) = d$ by performing repeated divisions to obtain a decreasing sequence of positive integers $r_1 > r_2 > \cdots > r_n = d$; that is,*

$$\begin{aligned} b &= aq_1 + r_1 \\ a &= r_1 q_2 + r_2 \\ r_1 &= r_2 q_3 + r_3 \\ &\vdots \\ r_{n-2} &= r_{n-1} q_n + r_n \\ r_{n-1} &= r_n q_{n+1} \end{aligned}$$

To find r and s such that $ar + bs = d$, we begin with this last equation and substitute the results obtained from previous equations:

$$\begin{aligned} d &= r_n \\ &= r_{n-2} - r_{n-1} q_n \\ &= r_{n_2} - q_n (r_{n-3} - q_{n-1} r_{n-2}) \\ &= -q_n r_{n-3} + (1 + q_n q_{n-1}) r_{n-2} \\ &\vdots \\ &= ra + sb \end{aligned}$$

Finding the value of d and writing it as the linear combination of a and b is called the Euclidean algorithm.

End of Lecture ——————

Lecture 7: September 13^{th}, 2024.

2.2 Fundamental Theorem of Arithmetic

Before getting into the fundamental theorem of arithmetic, let's look at some example and theorems.

Example 2.2.1. Say we want to break the number 12 into its multiple, we can write that $12 = 2 \times 6 = 2 \times 2 \times 3$ or even $12 = 3 \times 4 = 3 \times 2 \times 2$. Notice that 2 and 3 are prime and regardless of if we start with 3×4 or 2×6, we will always end with the same multiple of primes.

Theorem 2.7. *Let p be a prime number and let $a, b \in \mathbb{Z}$. If $p \mid ab$ then $p \mid a$ and $p \mid b$.*

Proof. If $p \mid a$m then the theorem holds. If $p \nmid a$, we need to show that $p \mid b$. In this case $p \gcd(a, p) \mid p$ so $\gcd(a, p)$ must be 1 or p since p is prime. So $\gcd(a, p) = 1$ because if $\gcd(a, p) = p \implies p \mid a$. Then $\exists u, v \in \mathbb{Z}$ s.t.

$$\begin{aligned} av + pu &= \gcd(a, p) = 1 \\ b(av + pu) &= b \\ bau + bvp &= b \end{aligned}$$

$p \mid ab \implies p \mid abu$ and $p \mid p \implies p \mid pbu \implies$. Thus, $p \mid (abu + bvp) = b$ □

Corollary 2.2. *Let $a_1, \dots, a_b \in \mathbb{Z}$ and p is a prime. If $p \mid a_1 \cdots a_n$ then $p \mid a_i$ for some $i \in \{1, 2, \dots, n\}$*

Proof. Will be used as exercise. □

Theorem 2.8. ***(Strong Induction).*** *Let $P(n)$ be a statement/proposition for $n \in \mathbb{N}$. Suppose that*

1. *$P(1)$ is true*

2. *If $n \in \mathbb{N}, P(1), P(2), \dots, P(n)$ are true $\implies P(n+1)$ is true*

Then $P(n)$ is true $\forall\, n \in \mathbb{N}$.

Theorem 2.9. ***(Fundamental Theorem of Arithmetic).*** *Let $n \geq 2$ be an integer. Then,*

1. *(Existence) $\exists l \in \mathbb{N}$ and $x_1, \ldots, x_l$ that are prime with $n = x_1 \ldots x_l$.*

2. *(Uniqueness) Suppose that $n = x_1, \ldots, x_l$ where $x_1 < \cdots < x_l$ where $x_1, \ldots, x_l$ are prime. Then, if $n = y_1 \cdots y_n$ where $y_1 < \cdots < y_t$ where $y_1, \ldots, y_t$ are prime then $t = l$ and $y_1 = x_1, y_2 = x_2, \ldots$*

i.e. any integer $n \geq 2$ can be factored uniquely into products of prime numbers.

Proof. (Existence) We'll prove using strong induction.

1. $\underline{(n = 2):}$ $2 = 2$, already a prime

2. $\underline{n \implies n+1:}$ Supposed the statement is true for all integer $\leq n$. Then, we need to show that $n+1$ is a product of prime number.
   If $n+1$ is prime then the existence holds. If $n+1$ is not prime, then $n+1 = a \times b$ where $1 < a, b < n+1$. By the induction hypothesis, $a = a_1 a_2 \cdots a_d$ where $d \in \mathbb{N}$ and $a_1, \ldots, a_d$ are prime. Similarly for $b = b_1 b_2 \cdots b_d$ etc. Then $n+1 = a_1 \cdots a_d b_1 \cdots b_d$. So $n+1$ is a product of prime numbers.

Thus by strong induction, every $n \in \mathbb{N}, n \geq 2$ is a product of prime numbers.

(Uniqueness) If $n = \alpha_1 \cdots \alpha_l = \beta_1 \cdots \beta_t$ where $\alpha_1 \cdots \alpha_l$ are prime with $\alpha_1 \leq \cdots \leq \alpha_l$ and $\beta_1 \cdots \beta_t$ are prime with $\beta_1 \leq \cdots \leq \beta_t$. Then $t = l$ and $\alpha_i = \beta_i \forall i \in \{1, \ldots, n\}$. By strong induction:

1. $\underline{n = 2:}$ This is clear since $2 = 2$.

2. $\underline{n-1 \implies n}$: Supposed that this hold for all integers $2, 3, \ldots, n-1$. Let $n = \alpha_1 \cdots \alpha_l = \beta_1 \cdots \beta_t$ where $\alpha_1 \cdots \alpha_l$ are prime with $\alpha_1 \leq \cdots \leq \alpha_l$ and $\beta_1 \cdots \beta_t$ are prime with $\beta_1 \leq \cdots \leq \beta_t$. We need to show that $\alpha_1 = \beta_1 \implies \alpha_1 \mid n$ so $\alpha_1 \mid \beta_1 \cdots \beta_l$. α_1 is prime so $\alpha_1 \mid \beta_j$ for some $j \in \{1, 2, \ldots, t\}$. Since β_j is prime then α_1 and β_j are equal and are prime by definition. $\beta_1 \mid n \implies \beta_1 \mid \alpha_1 \cdots \alpha_l$ is prime so $\beta_1 \mid \alpha_i$ for some $i \in \{1, \ldots, l\}$. So $\beta_1 = \alpha_i$. Since $\alpha_1 = \beta_j \geq \beta 1 = \alpha_i \geq \alpha_1$ then $\alpha_1 = \beta_1$. Then $\alpha_2 \cdots \alpha_l = \beta_2 \cdots \beta_l$ (cancel out α_1 and β_1).

By the induction hypothesis, $l = t$ and $\alpha_1 = \alpha_2, \ldots \alpha_i = \beta_i$ for some $i \in \{1, \ldots, t\}$. Hence we've proved the statement. □

2.2.1 Some Exercise

1. Let $a, b \in \mathbb{Z}$. Then, $\gcd(a, b) = 1$ if and only if $\exists u, v \in \mathbb{Z}$ such that $au + bv = 1$.

2. Let $a, b, c \in \mathbb{Z}$. Prove that if $\gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$.

End of Lecture

Lecture 8: September 16^{th}, 2024.

3 Groups

Definition 3.1. Let G be a set. A **binary operation** $\circ$ on G is a function $\circ : G \times G \to G$ that maps $(g_1, g_2) \mapsto g_1 \circ g_2$

Example 3.0.1. Consider $G = \mathbb{Z}$, then $+$ is a binary operation and similarly to $\times$.

Definition 3.2. A **group** G is a non-empty set equipped with a binary operations $\circ$ such that

1. **(Identity)** $\exists e_G \in G : \forall g \in G,\ g \circ e_G = e_G \circ g = g$
2. **(Inverse)** $\forall g \in G,\ \exists h \in G : g \circ h = h \circ g = e_G$.
3. **(Associativity)** $\forall g_1, g_2, g_3 \in G, g_1 \circ (g_2 \circ g_3) = (g_1 \circ g_2) \circ g_3$.

Example 3.0.2. $(\mathbb{Z}, +)$ is a group

Proof. 1) Let $g \in \mathbb{Z}, \exists g + 0 = 0 + g = g$. In this case $(e_G = 0)$.
2) Let $g \in \mathbb{Z}$, then $g + (-g) = (-g) + g = 0$.
3) The integers are closed under associative by definition.
Because it satisfies all of these axioms, $(\mathbb{Z}, +)$ is group. □

We can also check if $(\mathbb{Z}, \times)$ is a group or not.

Proof. Let $g \in Z$ then $g \times 1 = 1 \times g = g$. Let $g \in \mathbb{Z}$ then there's not necessarily $h \in \mathbb{Z} : g \times h = 1$. In fact, the only case this applied is for 1 and -1. Thus this axiom does not hold.We do not need to continue as axiom 2 does not hold thus $(\mathbb{Z}, \times)$ is not closed under multiplication and thus is not a group. □

From then, we can use the same argument to prove that $(\mathbb{R}, +)$ is a group. What about $(\mathbb{R}, \times)$? It is not a group as it won't satisfy axiom 2 because of 0.

Now we can ask ourselves, is $(\mathbb{R} \backslash \{0\}, \times)$ a group? Well We first consider that $a, b \neq \implies a \times b \neq 0$.

Proof. 1, Let $x \in \mathbb{R}$ then $x \times 1 = 1 \times x = x$. 2, Let $x \in \mathbb{R} \backslash \{0\}$ then $x \times (\frac{1}{x}) = \frac{1}{x} \times x = 1$. 3, The real number has associative properties. Thus $(\mathbb{R} \backslash \{0\}, \times)$ is a group. □

Let's construct some groups.

Example 3.0.3. Let $n \in \mathbb{N}$ and let $\mathrm{GL}_n(\mathbb{R})$ denote the set of invertible $n \times n$ matrices with real entries. Then, $(\mathrm{GL}_n(\mathbb{R}), \times)$ is a group. [1]

Proof. First if A and B are invertible matrices then AB is an invertible matrices. This is because $(B^{-1}A^{-1})(AB) = I_{n\times n}$. Another thing is $\det AB = \det A \det B \neq 0$. Now we can begin proving that it's a group.

1. Let $A \in \mathrm{GL}_n(\mathbb{R})$ then $A \times I_{n\times n} = I_{n\times n} \times A = A$.
2. Let $A \in \mathrm{GL}_n(\mathbb{R})$ then $A^{-1} \in \mathrm{GL}_n(\mathbb{R})$ and $\det(A^{-1}) = \frac{1}{\det A^{-1}}$. This means $A \times A^{-1} = A^{-1} \times A = I_{n\times n}$.
3. $A \times (B \times C) = (A \times B) \times C$.

Since $\mathrm{GL}_n(\mathbb{R})$ satisfy all 3 conditions, it's a group. □

Example 3.0.4. Let X be a set then consider G to be the set of bijections from $X \to X$. Then, G is a group under the law of composition of function.

Proof. Let $f, g \in G$, $f, g : X \to X$ are bijections and $g \circ f : X \to X$.

1. Let $Id_X = 1_x : X \to X, x \mapsto x$. Then $f \circ \mathrm{id}_X = f$. Let $x \in X, (f \circ \mathrm{id}_X)(x) = f(\mathrm{id}(x)) = f(x)$. Similarly $\mathrm{id}_x \circ f = f$ via the same argument.
2. Let $f \in G$, then $f : X \to X$ is bijective. Hence $f^{-1} : X \to X$ is a bijection so $f^{-1} \in G$. Thus $f^{-1} \circ f = f \circ f^{-1} = \mathrm{Id}_X$.
3. Let $f, g, h : X \to X$ be bijections. Then, $f \circ (g \circ h) = (f \circ g) \circ h$.

Thus G, a set of bijections from $X \to X$ is a group under the law of composition. □

End of Lecture ——

Example 3.0.5. If $X = \{1, 2, \dots, n\}$, we call S_n the group of bijective functions from $X \to X$. (Symmetric group on n letters). S_n has $n!$ element.

Proposition 3.1. *Let $(G, \circ)$ be a group. Then, the identity element e_G is unique.*

Proof. Suppose that e'_G and e_G are 2 identities. we need to show that $e_G = e'_G$. So, $e'_G = e_G \circ e'_G = e_G \implies e_G = e'_G$. □

Proposition 3.2. *Let $g \in G$. Then, $\exists! h \in G : g \circ h = h \circ g = e_G$. We call h the inverse of g and we write $h \circ g^{-1}$.*

Proof. Let h_1 and h_2 satisfy $g \circ h_1 = h_1 \circ g = e_G$ and similarly for h_2. Then, $h_1 = h_1 \circ g = h_1 \circ (g \circ h_2) = (h_1 \circ g) \circ h_2 = e \circ h_2 = h_2$ □

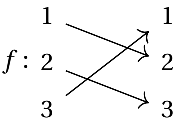
[1] GL stands for "general linear".

Lecture 9: September 18th, 2024.

3.1 Symmetric Group

Definition 3.3. Let X be a set. The set of bijections $X \to X$ or $\mathrm{sym}(X)$ is a group under the law of composition of function. This group is called the **symmetric group**.If $X = \{1, 2, \ldots, n\}, \mathrm{sym}(X) = S_n$. Which is the **symmetric group on n letters**.

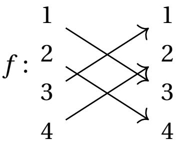
Example 3.1.1. Consider the following $f \in S_3$:



$$f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

For the function f, the first row is the input while the second row is the output. We can even further simplify this notation as $f = (123)$. We interpret this as f maps 1 to 2, then 2 to 3, finally 3 would loop around back to 1. This creates 1 loop/cycle i.e. anything in the parentheses is a loop of number.

Example 3.1.2. $f \in S_4$:

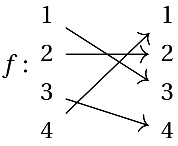


$$f = (13)(24)$$

Basically, the function has 2 loops: first is the loop between 1 and 3 and the other is a loop between 2 and 4.

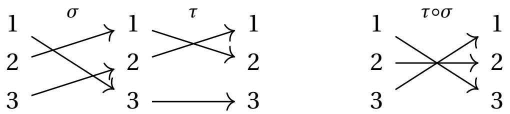
Remark 3.1. *When there's a loop with only 1 input e.g.* $1 \mapsto 1$, *then we can ignore said loop.*

Example 3.1.3. $f \in S_4$:



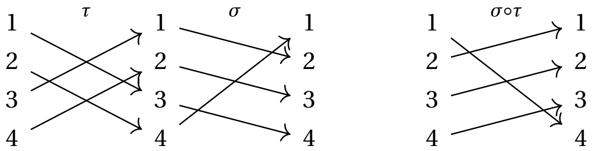
$$f = (134)(2) = (134)$$

Example 3.1.4. $\tau, \sigma \in S_3$:



We can see that $\tau = (12)(3) = (12)$ and $\sigma = (132)$ So $\tau \circ \sigma = (12)(132) = (13)(2) = (13)$

Example 3.1.5. $\sigma = (1234)$ and $\tau = (13)(24)$. Then, $\sigma \circ \tau = (1234)(13)(1432) = (1432)$. e.g. $(\sigma \circ \tau)(1) = \sigma(\tau(1)) = \sigma(3) = 4$.



Example 3.1.6. Let $\sigma = (12)(345)$ and $\tau = (14)(23)$.
Then, $\sigma\tau = (12)(345)(14)(23) = (153)(24)$.

Example 3.1.7. Let $\sigma = (123456)$ and $\tau = (12)(34)(56)$.
Then $\sigma\tau = (123456)(12)(34)(56) = (135)(2)(4)(6)$.

Example 3.1.8. Let $\sigma = (12)(34)(56)$ and $\tau = (1234567)$.
Then, $\tau\sigma = (1234567)(12)(34)(56) = (1357)(2)(4)(6) = (1357)$

With this kind of notation, it will be easy to find the inverse function:

Example 3.1.9. $\tau = (1357)$, then $\tau^{-1} = (7531)$. $\tau\tau^{-1} = 1 = ()$.

End of Lecture

Definition 3.4. Let $(G, \circ)$ be a group, a **subgroup** of G is a nonempty subset H such that

1. $e_G \in H$
2. If $a, b \in H$ then $a \circ b \in H$
3. If $a \in H$, then $a^{-1} \in H$

Thus we can also say that $(H, \circ)$ is a group itself

Example 3.1.10. Consider the group $(\mathbb{R}, +)$. Then $(\mathbb{Z}, +)$ and $(\mathbb{Q}, +)$ are subgroups of $\mathbb{R}$.

Lecture 10: September 20th, 2024.

Definition 3.5. A group $(G, \circ)$ is **abelian** [2]if $\forall g, h \in G$, we have $g \circ h = h \circ g$.

Example 3.1.11. $(\mathbb{R}, +)$ is abelian, $(\mathbb{R}\backslash 0, \times)$ is abelian. Contrarily, $\mathrm{GL}_2(\mathbb{R})$ is not abelian, and so is S_n for $n \geq 3$. e.g. $(12)(13) = (132)$ while $(13)(12) = (123)$ which are different.

3.2 The Group $\mathbb{Z}/n\mathbb{Z}$ and U_n

Definition 3.6. Let $n \in \mathbb{N}$, we say that $a, b \in \mathbb{Z}$ are **congruent modulo n**, denotes as $a \equiv b \mod n$, iff $a - b$ is divisible by n

Recall: Define a relation on $\mathbb{Z}$, $a \sim b$ if $a - b$ is divisible by n or simply $a \equiv b \mod n$. Thus $\equiv \mod n$ is an equivalence relation on $\mathbb{Z}$.

Example 3.2.1. For $n = 3$, $[0]_3 = \{x \in \mathbb{Z} : x \equiv 0 \mod 3\} = 3\mathbb{Z}$. Simiarly,

$$\begin{aligned}
[1]_3 &= \{x \in \mathbb{Z} : x \equiv 1 \mod 3\} \\
&= 1 + 3\mathbb{Z} \\
[2]_3 &= 2 + 3\mathbb{Z} \\
[5]_3 &= 5 + 3\mathbb{Z} = 2 + 3\mathbb{Z}
\end{aligned}$$

If $n = 5$, you would have 5 equivalence classes.

Example 3.2.2. $7 \equiv 2 \mod 5$ since $7 - 2 = 5$ which is divisible by 5. Similarly or $7 \equiv 12 \mod 5$, $7 \equiv 17 \mod 5$.

$7 \equiv 3 \mod 4$ and $9 \equiv 1 \mod 4$. We know that $9 + 7 \equiv 16 \equiv 0 \mod 4$ and same for $3 + 1 \equiv 4 \equiv 0 \mod 4$. What about multiplication? Well...we get that $7 \times 9 \equiv 63 \equiv 3 \mod 4$ and $3 \times 1 \equiv 3 \equiv 3 \mod 4$.

Proposition 3.3. *Let $a, b, c, d \in \mathbb{Z}$ and $n \in \mathbb{N}$. Suppose that $a \equiv b \mod n$ and $c \equiv d \mod n$. Then*

$$a + c \equiv b + d \mod n \tag{3.1}$$

and

$$ac \equiv bd \mod n \tag{3.2}$$

[2] Another way to say it "commutative".

Proof. Let's prove for (3.1). We need to show that $a+c-(b+d)$ is divisible by n. We have that

$$a+c=(b+d)= \underbrace{(a-b)}_{\text{divisible by n}} + \underbrace{(c-d)}_{\text{divisible by n}}$$

Another way to show this is because let $a=b+kn$ and $c=d+qn$. Then,

$$\begin{aligned} a+c=(b+d) &= (a-c)+(b-d) \\ &= kn+qn \\ &= (k+q)n \end{aligned}$$

which is divisible by $n \implies a+c \equiv b+d \mod n$.
For the product, we need to show that $ac-bc$ is divisible by n. Then,

$$\begin{aligned} ac-bn &= (b+kn)(d+qn)-bd \\ &= bd+bqn+knd+kqn^2-bd \\ &= n(bq+kd+kqn) \end{aligned}$$

which is divisible by n $\implies ac \equiv bd \mod n$ □

Example 3.2.3. If $a=nq+r$ where $0 \le r < n$. Then, $a \equiv r \mod n$. e.g. $66=4\times 12+2 \implies 66 \equiv 2 \mod 4$;

Definition 3.7. The set of equivalence classes of congruence modulo n is a set of n elements:

$$[0]_n, [1]_n, [2]_n, \ldots, [n-1]_n$$

We denotes the set with the above elements as $\mathbb{Z}/n\mathbb{Z}$ or sometimes $\mathbb{Z}_n$.

Example 3.2.4. We can define an addition on $\mathbb{Z}/n\mathbb{Z}$. Consider the equivalence classes of $\mod 5$: $[0]_5, \ldots, [4]_5$/ Then we get

$$[1]_5 + [4]_5 = [1+4]_5 = [5]_5 = [0]_5$$
$$[2]_5 + [4]_5 = [2+4]_5 = [6]_5 = [1]_5$$

We can also define a multiplication:

$$[3]_5 \times [2]_5 = [3\times 2]_5 = [6]_5 = [1]_5$$
$$[3]_5 \times [3]_5 = [3\times 3]_5 = [9]_5 = [4]_5$$

Remember, we also have to show that your operation <u>does not depend</u> on the element you choose to present your class.

$$[1]_5 + [4]_5 = [1+4]_5 = [0]_5$$
$$[6]_5 + [24]_5 = [30]_5 = [0]_5$$

Example 3.2.5. Let's see a counter example where the operation depends on the element you choose and is not a well–defined function:

$$f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}, [x]_n \mapsto x$$

Here's the problem: $[n]_n \mapsto n$ but $[0]_n = [n]_n$ and $[0]_n \mapsto 0 \implies 0 = n$ (contradiction). Thus it's not well–defined.

Proposition 3.4. *$+ : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, [x]_n + [y]_n = [x+y]_n$ is well–defined. Simiarly, $\times : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, [x]_n \times [y]_n = [xy]_n$ is well–defined.*

Proof. Suppose that $[x]_n = [a]_n$ and $[y]_n = [b]_n$. We need to show that $[x+y]_n = [a+b]_n$. We know that

$$[x]_n = [a]_n \iff x \equiv a \mod n$$
$$[y]_n = [b]_n \iff y \equiv b \mod n$$

Then, by proposition 3.3, $[x+y]_n = [a+b]_n$. We can use the same structure of argument along with proposition 3.3, to prove $[xy]_n = [ab]_n$ □

End of Lecture

Lecture 11: September 23rd, 2024.

Corollary 3.1. *$(\mathbb{Z}/n\mathbb{Z}, +)$ is a group*

Proof. We want to show that it satisfies all 3 properties of groups:

1. $\forall x \in \mathbb{Z} : [x]_n + [0]_n = [x+0]_n = [x]_n$.
2. $\forall x \in \mathbb{Z} : [x]_n + [-x]_n = [x-x]_n = [0]_n$
3. $\forall x, y, z \in \mathbb{Z} : [x]_n + [y+z]_n = [x+(y+z)]_n = [(x+y)+z]_n = [x+y]_n + [z]_n$

Thus, $(\mathbb{Z}/n\mathbb{Z}, +)$ is a group. □

How abouot $(\mathbb{Z}/n\mathbb{Z}, \times)$, is it a group? Well...we can tell right away that no since there's no inverse for 0.

Proposition 3.5. *Let $a \in \mathbb{Z}$ then the equation $ax \equiv 1 \mod n$ has a solution iff* $\gcd(a, n) = 1$.

Proof. We will need to show it implies in both direction.
$(\implies)$ let x_0 be such that $ax_0 \equiv 1 \mod n$. Then $\exists a \in \mathbb{Z}$ such that $ax_0 = 1 + kn \implies ax_0 - kn = 1$. Then $\gcd(a, b) | ax_0 - bn = 1 \implies gcd(a, n) = 1$.
$(\impliedby)$ Suppose $\gcd(a, n) = 1$. Then $\exists, u, b \in \mathbb{Z} : au + vn = 1 \implies au \equiv 1 \mod n$. Hence the equation $ax \equiv 1 \mod n$ has a solution. □

Definition 3.8. Let $U(n) = \{[a]_n : \gcd(a, n) = 1\}$. Then we call $U(n)$ the **set of numbers co-prime to n.** [3]

[3] These numbers are less than n

Example 3.2.6. $U(5) = \{1,2,3,4\}, U(8) = \{1,3,5,7\}$

Proposition 3.6. $(U(n), \times)$ *is a group.*

Proof. First note that if $\gcd(a,n) \equiv 1 \mod n$ and $\gcd(b,n) \equiv 1 \mod n$ then by homeword 2, $\gcd(ab,n) = 1 \mod n$. Hence $[ab]_n \in U(n)$. Then $U(n)$ is a group under $\times \mod n$ through the followings:

1. Let $x \in \mathbb{Z}, [x]_n \times [1]_n = [x \times 1]_n = [x]_n$.
2. Let $x \in \mathbb{Z} : \gcd(x,n) = 1$. Then $\exists u_0 : xu_0 \equiv 1 \mod n \implies [x]_n \times [u_0]_n = [xu_0]_n = [1]_n$.
3. Let $x,y,z \in \mathbb{Z} : [x]_n + [y+z]_n = [x+(y+z)]_n = [(x+y)+z]_n = [x+y]_n + [z]_n$

□

Remark 3.2. *$U(n)$ is a subset of $\mathbb{Z}/n\mathbb{Z}$ but is <u>not</u> its subgroup.*

3.3 Order of an element

Definition 3.9. The order of an element $g \in G$ is the smallest integer $n \in \mathbb{N}$ if it exists such that $g^n = e_G$ and $g^n = \underbrace{g \circ g \circ \cdots \circ g}_{n \text{ times}}$

Remark 3.3. *Note from author: Similar examples and more of order of an element is given in the next lecture recap.*

Proposition 3.7. *Let G be a group and $g \in G$ have order n.*

1. *If $g^k = e_G$, then $n \mid k$.*
2. *Order of $g^m = \frac{n}{\gcd(m,n)}$.*

Proof. 1) Let $k \in \mathbb{Z} : g^k = e_G$. Write $k = qn + r$ where $q \in \mathbb{Z}$ and $0 \leq 1 < n$. Then, $g^k = g^{qn+r} \implies g^k = g^{qn}g^r \implies e_G = e_G g^r$. So $g^r = e_G$ hence $r = 0 \implies n \mid k$.
2) We will first show that the order of g^m divides $\frac{n}{\gcd(m,n)}$. First,$(g^m)^{\frac{n}{\gcd(m,n)}} = g^{\frac{mn}{\gcd(m,n)}} = (g^n)^{\frac{m}{\gcd(m,n)}} = e_G^{\frac{m}{\gcd(m,n)}} = e_G$. We will now show that they're exactly equal. Let $k = \text{order}(g^m)$ hence $(g^m)^k = e_G$. Then $g^{mk} = e_G$, then also by the proposition 1 above, the order of g divides $mk \implies n \mid mk$ and $m \mid mk$

End of Lecture

so mb is a common multiple of m and n. Hence by homework 2, mk is a multiple of $\operatorname{lcm}(m,n) = \frac{mn}{\gcd(m,n)}$. So,

$$\begin{aligned} \frac{mn}{\gcd(m,n)} q &= mk && \text{for } q \in \mathbb{N} \\ \frac{n}{\gcd(m,n)} q &= k \end{aligned}$$

and hence $\frac{n}{\gcd(m,n)} \Big| k = \operatorname{order}(g^m)$. Thus, the order of g^m is $\frac{n}{\gcd(m,n)}$. □

Lecture 12: September 25th, 2024.

Definition 3.10. The order of an element $g \in G$ is the smallest integer $n \in \mathbb{N}$ if it exists such that $g^n = e_G$ and $g^n = \underbrace{g \circ g \circ \cdots \circ g}_{n \text{ times}}$

If for addition then $g^n = gn$

Example 3.3.1. Consider the following group and its order.

- The order of $(12) \in S_2$ is $()$ since $(12)(12) = ()$
- The order of $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R})$ will be
$$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$
- $2 \in \mathbb{R} \backslash \{0\}$ does not have a finite order.
- The order of $1 \in \mathbb{Z}$ is infinite.
- The order of $[3]_5 = U(5) = \{[1]_5, [2]_5, [3]_5, [4]_5,\}$ is 4 since $3^1 \neq 1, 3^2 = 9 = 4, 3^3 = 3^3 \times 3 = 4 \times 3 = 12 = 2, 3^4 = 3^3 \times 3 = 2 \times 3 = 6 = 1$
- The order of $[4]_8 \in \mathbb{Z}/8\mathbb{Z}$ is 2, since $[4]_8 \neq 0$ but $[4]_8 + [4]_8 = 2[4]_8 = 0$.
- The order of $[3]_4 \in \mathbb{Z}/4\mathbb{Z}$ is 4.
- The order of $[3]_8 \in U(8) = \{[1]_8, [3]_8, [5]_8, [7]_8,\}$ is 2.
- The order of $(1234) \in S_4$ is 4, since
$$\begin{aligned} (1234) &\neq 0 \\ (1234)^2 &= (1234)(1234) = (13)(24) \\ (1234)^3 &= (1234)^2(1234) = (1432) \\ (1234)^4 &= (1234)^3(1234) = () \end{aligned}$$

Corollary 3.2. *The order of* $(a_1 a_2 \cdots a_k) \in S_n$ *is* k.

Proposition 3.8. *If* g *has order* n *then* g^k *has order* $\frac{n}{\gcd(n,k)}$

Example 3.3.2. We know that in $U(5), [3]_5$ has order 4 since $3 \neq 1, 3^2 = 4, 3^3 = 2, 3^4 = 1$. Then, the order of 3^2 is $\frac{4}{\gcd(4,2)} = \frac{4}{2} = 2$. Similarly, the order of 3^3 is $\frac{4}{\gcd(4,3)} = 4$

Example 3.3.3. The order of $[2]_5 \in \mathbb{Z}/5\mathbb{Z}$ has order 5 since $[2]_5 = [1]_5 + [1]_5$ will have order $\frac{5}{\gcd(2,8)} = 5$

Theorem 3.1. ***(Lagrange's).*** *Let* G *be a finite group and* H *a subgroup of* G*. Then,* $|H|$ *divides* $|G|$.

Before doing the proof, we define the following relation on G. We say that $x \sim y$ if $y^{-1}x \in H$.
Claim: $\sim$ is an equivalence relation.

Proof. We need to show it satisfies the following properties

1. (Reflexive) Let $x \in G, x^{-1}x = e_G \in H$ since H is a subgroup of G.
2. (Symmetric) Suppose $x \sim y$. Then $y^{-1}x \in H$ hence $(y^{-1}x)^{-1} \in H$. Thus,
$$(y^{-1}x)^{-1}y^{-1}x = (x^{-1}y)y^{-1}x = e_G$$
3. (Transitive) Let $x, y, z \in G$ and suppose $x \sim y$ and $y \sim z$. Then, $y^{-1}x \in H$ and $z^{-1}y \in H$. Since H is a subgroup,
$$(z^{-1}y)(y^{-1}x) = z^{-1}x \in H$$
Thus $z \sim x$

Then $\sim$ is an equivalence relation. □

Hence G can be partitioned into the equivalence classes of $\sim$. Then we get

$$\begin{aligned}[x]_\sim &= \{y \in G : y \sim x\} \\ &= \{y \in G : x^{-1}y \in H\} \\ &= \{y \in G : y = xh \text{ for some } h \in H\} \\ &= xH = \{xh, h \in H\}\end{aligned}$$

End of Lecture

We will continue from the proof of last lecture.

Lecture 13: September 27th, 2024.

Definition 3.11. A subset of G of the form xH (where H is a subgroup of G i.e. $H < G$) is called a **left coset** of H.

Hence we can partition G into a disjoint union of equivalence classes i.e. into a disjoint union of left cosets of H. Note that $H = e_G H$ is also a left coset of H.

Let $x_1 = e_G, x_2, \ldots, x_k$ be representatives of the distinct equivalence classes of $\sim$. We will show that there is a bijection from H to xH.

Lemma 3.1. *There exists a bijection from H to xH*

Proof. Let $f : H \to xH, f : h \mapsto xh$ where $x \in G$. f is injective. If $f(h_1) = f(h_2)$ then $xh_1 = xh_2 \implies x^{-1}xh_1 = x^{-1}xh_2 \implies h_1 = h_2 \implies f$ is injective f is surjective. Let $g \in xH$. Then, there exists $h' \in H$ such that $g = xh'$, hence $g = f(h') \implies f$ is surjective. Thus f is bijective. □

Proof. (Lagrange's Theorem) From the above proof, we can see that $|H| = |xH|$ for all $x \in G$. Therefore $|H| = |x_2 H| = |x_3 H| = \cdots = |x_k H|$. $H = e_G H$, $x_2 H, x_3 H, \ldots, x_k H$ partition G. Thus, [4]

$$|G| = |H| + |x_2 H| + \cdots + |x_k H| = k|H| \tag{3.3}$$

Thus $|G|$ divides $|H|$. □

Definition 3.12. The numbers of left cosets of H in G is called the **index** of H in G denoted as $[G : H]$. If G is finite, then

$$[G : H] = \frac{|G|}{|H|} \tag{3.4}$$

Definition 3.13. The order of a group G is the number of elements of G. If G is finite

Corollary 3.3. *(Of Lagrange's Theorem) Let G be a finite group and let $g \in G$. Then, g has a finite order and the order of g divides $|G|$.*

Proof. g has finite order. Consider the following subset of G, $\{g^n : n \in \mathbb{N}\} \subseteq G$. Since G is finite so $\{g^n : n \in \mathbb{N}\}$ is also finite. Then, $\exists n_1, n_2 \in \mathbb{N} : n_1 < n < 2$ and $g^{n_1} = g^{n_2} \implies g^{n_2 - n_1} = e_G$.
Let $S = \{m \in \mathbb{N} : g^m = e_G\}$ then S is non-empty since $n_2 - n_1 \in S$. So S has a minimal element and hence g has finite order. [5] □

End of Lecture ——

[4] According to the professor, the proof of Lagrange's theorem was used often in finals...

[5] We will continue this proof in the next lecture.

Lecture 14: September 30^{th}, 2024.

Corollary 3.4. *If G is a finite group and $g \in G$. Then, order of g divides $|G|$. Particular, $g^{|G|} = e_G$.*

Proof. Last time we saw that g has finite order if G is finite. Consider the set $T = \{g^n : n \in \mathbb{Z}, 0 \le n < \text{ord}(g)\} = \{g^0, g^1, g^2, \dots, g^{\text{ord}(g)-1}\}$.
The elements in the set T are distinct since if $x, y \in \{0, 1, \dots, \text{ord}(g) - 1\}$, $g^x = g^y$ then $g^{x-y} = e_G \implies \text{ord}(g) \mid x - y$. Now, $0 \le x < \text{ord}(g)$ and $0 \le y < \text{ord}(g) \implies -\text{ord}(g) \le x - y < \text{ord}(y)$. So, $x - y = 0 \implies x = y$.

We'll thus see that T is a subgroup of G with $e_G \in T$. Let $s, t \in \{0, 1, \dots, \text{ord}(g) - 1\}$; suppose $g^s g^t = g^{s+t}$. Let r be such that $0 \le r < \text{ord}(g)$ and $s + t = q\text{ord}(g) + r \implies g^{s+t} = g^{q\text{ord}(g)+r} = (g^{\text{ord}(g)})^q g^r = g^r$.
We'll now check for inverse. $(g^s)^{-1} = g^{-s} = g^{\text{ord}(g)-s}$. Hence T is a group with $\text{ord}(g)$ elements. By Lagrange's theorem, $|T|$ divides $|G| \implies \text{ord}(g)$ divides $|G|$. Hence, $g^{|G|} = g^{k\text{ord}(g)} = e_G^k = e_G$ ($|G| = k\text{ord}(g)$). □

Definition 3.14. A right coset is a subset of G of the form $Hx = \{hx, h \in H\}$

Proposition 3.9. *Consider the following relation on G, $x \sim_{RH} y$ if $xy^{-1} \in H$ where $H < G$. This relation is an equivalence relation on G*

Proof. Exercise. □

Notice that

$$\begin{aligned} [x]_{\sim_{RH}} &= \{y \in G : yx^{-1} \in H\} \\ &= \{y \in G : yx^{-1} = h \text{ for some } h \in H\} \\ &= \{hx, h \in H\} = Hx \end{aligned}$$

G can be thus partitioned into disjoin right cosets (In general, it's not necessarily true that $xH = Hx$, only true if G is abelian).

Exercise. Consider the set $N_G(H) = \{x \in G : xH = Hx\}$. Show that $N_G(H)$ is a subgroup of G.

Proposition 3.10. *Let G be a group and $H < G$. Denote by*

$$\begin{aligned} \sim_L &: x \sim_L y \iff y^{-1}x \in H \\ \sim_R &: s \sim_R t \iff st^{-1} \in H \end{aligned}$$

Then the followings are equivalent:

1. $g_1 H = g_2 H$
2. $g_2^{-1} g_1 \in H$
3. $H g_1^{-1} = H g_2^{-1}$

Proof. (1 $\iff$ 2) $g_1 H = g_2 H \iff [g_1]_{\sim_L} = [g_2]_{\sim_R} \iff g_1 \sim_L = g_2$.
(3 $\iff$ 2) $Hg_1^{-1} = Hg_2^{-1} \iff [g_1^{-1}]_{\sim_R} = [g_2^{-1}]_{\sim_R} \iff g_1^{-1} \sim_R g_1^{-1} \iff g_2^{-1}(g_1^{-1})^{-1} \in H \iff g_2^{-1} g_1 \in H$ □

How many left and right cosets do we have? Well...if G is finite, then there are $\frac{|G|}{|H|}$ left cosets.

Remark 3.4. *We denote G/H the set of left cosets and $H\backslash G$ the left of right cosets.*

Proposition 3.11. *There is a bijection $\phi : G/H \to H\backslash G, \phi(gH) \mapsto Hg^{-1}$*

Proof. We need to show that ϕ is well-defined i.e. suppose that $g_2 H = g_1 H$, we need to show that $\phi(g_1 H) = \phi(g_2 H)$. If $g_1 H = g_2 H \iff g_2^{-1} g_1 \in H \iff Hg_1^{-1} = Hg_2^{-1} \implies \phi$ is well-defined.
Let $\tau : H\backslash G \to G/H, Hx \mapsto x^{-1}H$. Then $(\phi \circ \tau)(Hx) = \phi(\tau(Hx)) = \phi(x^{-1}H) = Hx \implies \phi \circ \tau = \mathrm{Id}_{H\backslash H}$. Meanwhile, $(\tau \circ \phi)(xH) = \tau(Hx^{-1}) = xH$. So ϕ and τ are invertible and are bijections. □

End of Lecture ——

Lecture 15: October 2nd, 2024.

Example 3.3.4. Consider the group $\mathbb{Z}$ under addition and the subgroup $n\mathbb{Z} = \{kn : k \in \mathbb{Z}\}$. $n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$. The left coset are the equivalence classes of the following relation $x \sim_L y \iff x - y \in n\mathbb{Z} \implies x - y$ is divisible by n.

$$\begin{gathered}[0]_n = 0 + n\mathbb{Z}\\ [1]_n = 1 + n\mathbb{Z}\\ \vdots\\ [n-1]_n = n - 1 + n\mathbb{Z}\end{gathered}$$

We can thus find that $[\mathbb{Z} : n\mathbb{Z}] = n$

Example 3.3.5. Compute the left cosets of $H = \{(), (12), (13), (23), (123), (132)\}$ in S_4.
Solution: $H = \mathrm{sym}(1,2,3) \implies H < S_4$. Therefore, there are $\frac{|S_4|}{|H|} = \frac{24}{6} = 4$

left cosets of H. Let's find those left cosets. First, we will have $e_G H$ as a left coset.

$$e_G H = \{(), (12), (13), (23), (123), (132)\}$$

Note: if we take any element of H to form a left coset, we'd get back $H \implies e_G$ is our representative. We'll pick an element in S_4 which give

$$(14)H = \{(14), (124), (134), (14)(23), (1234), (1324)\}$$

Now, let's pick (24) as it's not in the above coset.

$$(24)H = \{(24), (142), (24)(13), (234), (1423), (1342)\}$$

Similarly, (34) does not exists in any of the above so

$$(34)H = \{(34), (12)(34), (143), (243), (1243), (1432)\}$$

Notice that $(142)H = (24)H$ and $(143)H = (34)H$. Notice too that for each element from each left coset will have the same sort of mapping as its representative e.g. (14)H has its representative mapping from 1 to 4 and all of its element will map 1 to 4. Right coset will be the same.

3.4 Cyclic Groups

3.4.1 Subgroup generated by $g \in G$

Definition 3.15. Let G be a group and let $g \in G$. Denote by

$$\langle g \rangle = \{g^n : n \in \mathbb{Z}\} \tag{3.5}$$

We call $\langle g \rangle$ the **cyclic subgroup generated** by g

Lemma 3.2. $\langle g \rangle < G$

Proof. We will show that it follows the following properties:

1. $e_G = g^0 \implies e_G \in \langle g \rangle$
2. $g^{n_1} g^{n_2} = g^{n_1+n_2}$. Since $n_1 \wedge n_2 \in \mathbb{Z} \implies n_1 + n_2 \in \mathbb{Z}$.
3. $(g^n)^{-1} = g^{-1} \implies \langle g \rangle$ has an inverse.

Thus $\langle g \rangle$ is a subgroup of G. □

Example 3.4.1. Consider the following subgroup generated:

- $\langle 2\rangle \in (\mathbb{Z},+)$, $\langle 2\rangle = \{2k : k \in \mathbb{Z}\} = 2\mathbb{Z}$.
- $\langle 3\rangle \in (\mathbb{R}\backslash 0,\times)$, $\langle 3\rangle = \{2^n : n \in \mathbb{Z}\}$.

Lemma 3.3. *If $H < G$ and $g \in H$. Then $\langle g\rangle < H$.*

Proof. Exercise. □

End of Lecture ———

Lecture 16: October 4th, 2024.

Proposition 3.12. *If g has finite order n. Then, $\langle g\rangle = \{e_G, g, g^2, \dots, g^{n-1}\}$*

Proof. Let $k \in \mathbb{Z}$, we can write $k = qn + r$ for some $q \in \mathbb{Z}$ and $0 \leq r < n$. Then,

$$g^k = g^{qn+r} = \left(g^n\right)^q = e_G^q g^r = g^r$$

□

Example 3.4.2. Suppose g has order 5, $g^{101} = g^{100}g = \left(g^5\right)^{20} g = g$

Definition 3.16. A group G is said to be cyclic iff there exists $g \in G$ such that $G = \langle g\rangle$.

Example 3.4.3. $(\mathbb{Z},+)$ is cyclic since $\mathbb{Z} = \langle 1\rangle = \langle -1\rangle$. Similar logic, $\mathbb{Z} \neq \langle 2\rangle$.

- Is $\mathbb{R}$ a cyclic group? No.
- Is $\mathbb{Q}$ a cyclic group? No.
- $(\mathbb{Z}/n\mathbb{Z},+)$ is a cyclic group with $\mathbb{Z}/n\mathbb{Z} = \langle [1]_n\rangle$.
- $U(5) = \{[1]_5,[2]_5,[3]_5,[4]_5\}$. We can see that $2^2 = 4, 2^4 = 16 = 1, 2^3 = 3 \implies U(5) = \langle [2]_5\rangle$

Proposition 3.13. *Let G be a finite group with $|G| = n$. Then G is cyclic iff G has an element of order n.*

Proof. ($\Longrightarrow$) Suppose G has an element g order n. Then, $\langle g\rangle = \{e_G, g, g^2, \dots, g^{n-1}\}$ is a subset of G with n element. $\langle g\rangle \subset G$ and $|\langle g\rangle| = n, |G| =$ then $G = \langle g\rangle$.
($\Longleftarrow$) Left as an exercise. □

Remark 3.5. *If G is a group and $G = \langle g\rangle$, we say that g generates G and g is the generator of G.*

Example 3.4.4. Is $U(8)$ cyclic? $U(8) = \{[1]_8, [3]_8, [5]_8, [7]_8\}$. We can see that for 1, it has order 2, for 3 it's 2, for 5 it's 2 and for 7 it's 2. Thus, $U(8)$ is not cyclic since $|U(8)| = 4$ but has no element of order 4.

Proposition 3.14. *Let G be a cyclic group, G is abelian.*

Proof. Since G is cyclic, there exists $g \in G$ such that $G = \langle g \rangle$. Let $x, y \in G$, there exists $n_1, n_2 \in \mathbb{Z}$ such that $x = g^{n_1}$ and $y = g^{n_2}$. Then,

$$xy = g^{n_1} g^{n_2} = g^{n_1+n_2} = g^{n_2+n_1} = g^{n_2} g^{n_1} = yx$$

Thus G is abelian. □

Example 3.4.5. $S_n, n \geq 3$ is not abelian so is not cyclic. $\mathrm{GL}_2(\mathbb{R})$ is not abelian so is not cyclic. $U(8)$ is abelian but not cyclic.

Proposition 3.15. *Let G be a finite group with n elements and let $g \in G$. Then, $G = \langle g \rangle$ iff g has order n.*

Proof. Let as an exercise. □

Example 3.4.6. $U(5) = \{1, 2, 3, 4\}$ with multiplication mod 5. We've seen that 1 has order 1, 2 has order 4, 3 has order 4 and 4 has order 2. Thus $U(5) = \langle [2]_5 \rangle = \langle [3]_5 \rangle \neq \langle [4]_5 \rangle$

Theorem 3.2. *Let G be a cyclic group with n elements and let d divides n. Then G has a unique subgroup with d elements ($d \in \mathbb{N}$).*

Proof. Let $g \in G$ be a generator of the cyclic group G, g has order n. Then $g^{n/d} (\frac{n}{d} \in \mathbb{N})$ has order $\frac{\mathrm{ord}(g)}{\gcd(\mathrm{ord}(g), \frac{n}{d})} = \frac{n}{\gcd(n, \frac{n}{d})} = \frac{n}{n/d} = d$. So $g^{n/d}$ has order d. Thus, $\langle g^{n/d} \langle$ has d elements.

Now we need to prove uniqueness. Let H be a subgroup of G with d elements and let $y \in H$. We need to show that $y \in \langle g^{n/d} \rangle$. By Lagrange's theorem, $y^{|H|} = e_G$ so $y^d = e_G$. Since G is cyclic, there exists $k \in \{0, 1, \ldots, n-1\}$ such that $y = g^k \implies e_G = y^d = g^{kd}$. So $g^{kd} = e_G$ hence order of g divides kd so $n \mid kd$. Then,

$$\begin{aligned} qn &= kd && \text{for some } q \in \mathbb{N} \\ q\frac{n}{d} &= k && \left(\frac{n}{d} \in \mathbb{N} \text{ since } d \mid n\right) \end{aligned}$$

So $y = g^k = g^{n/d \cdot q} = (g^{n/d})^q \implies y \in \langle g^{n/d} \rangle$. Hence, $H \subseteq \langle g^{n/d} \rangle$. $|H| = d$ by assumption and $|\langle g^{n/d} \rangle| = d$ since $g^{n/d}$ has order d (shown above). Then $H = \langle g^{n/d} \rangle$. □

End of Lecture

Lecture 17: October 7th, 2024.

How many generators does G have? Well...Let $y \in G, \exists k \in \{0, 1, \dots, n-1\}$ such that $y = g^k$ since $G = \langle h \rangle$. y generates $G \iff G = \langle g^k \rangle \iff g^k$ has order $n \iff \frac{n}{\gcd(n,k)} = n \iff \gcd(n,k) = 1$. Hence the number of generators of a cyclic group with n elements is $|U(n)|$ (which is the number of integers between 0 and $n-1$ that are relatively prime to n).

Definition 3.17. Let $\phi : \mathbb{N} \to \mathbb{N}, n \mapsto |U(n)|$. $\phi(1) = 1$, $\phi(2) = 1$, $\phi(4) = 2$, etc. In particular, if p is prime then $\phi(p) = p - 1$

Example 3.4.7. Find all the generators of $\mathbb{Z}/8\mathbb{Z} = \langle [1]_8 \rangle$. Hence the generators of $\mathbb{Z}/8\mathbb{Z}$ are $[1]_8, [3]_8, [5]_8, [7]_8$.

Example 3.4.8. Find all the subgroups of $\mathbb{Z}/12\mathbb{Z}$. First, $\mathbb{Z}/12\mathbb{Z}$ is a cyclic group with 12 elements and is generated by $[1]_{12}$ i.e. $\mathbb{Z}/12\mathbb{Z} = \langle [1]_{12} \rangle$. For every divisor $d \in \mathbb{N}$ of 12, there exists a unique subgroup with d elements generated by $[n/d]_{12}$.

3.4.2 Fermat's and Euler's Theorem

Theorem 3.3. ***(Fermat's Little Theorem).*** *Let $a \in \mathbb{N}$ and p a prime number with p not dividing a. Then $a^{p-1} \equiv 1 \mod p$.*

Proof. If p is prime and $p \nmid a$. Then $\gcd(a,p) = 1$. Then $[a]_p \in U(p)$. Hence, $\text{ord}([a]_p) \big| |U(p)| \implies \text{ord}([a]_p) \mid p-1$. Hence $[a]_p^{p-1} = [1]_p \in U(p)$ and thus $a^{p-1} \equiv 1 \mod p$ □

Example 3.4.9. $3^4 = 81 \equiv 1 \mod 5$. $2^6 = 64 = 1 + 63 \equiv 1 \mod 7$.

Example 3.4.10. Let p be a prime number with $p \equiv 3 \mod 4$. Show that the equation $x^2 \equiv -1 \mod p$ has no solution.

Theorem 3.4. ***(Euler's Theorem).*** *Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$ such that* $\gcd(a,n) = 1$. *Then, $a^{\phi(n)} \equiv 1 \mod n, \phi(n) = |U(n)|$.*

Proof. If $\gcd(a,n) = 1$, then $[a]_n \in U(n)$, then $[a]_n^{\phi(n)} = [1]_n$. Hence $a^{\phi(n)} \equiv 1 \mod n$ where $\phi(n) = |U(n)|$. □

3.5 Normal Subgroups

Definition 3.18. Let G be a group and N a subgroup of G. N is said to be a **normal subgroup** of G if $\forall g \in G$,

$$gN = Ng \tag{3.6}$$

We denotes N is the normal subgroup of G as $N \lhd G$

Example 3.5.1. Consider the following normal subgroups:

1. If G is abelian, and H is a subgroup of G. Then, $H \lhd G$

   Proof. Let $g \in G$, $gH = \{gh : h \in G\} = \{hg : h \in H\} = Hg$. □

2. Consider the subgroup $H = \{(), (12)\}$ of S_3. We can see that $(13)H = \{(13), (123)\}$ and $H(13) = \{(13), (132)\}$. Thus $(13)H \neq H(13) \implies H \ntriangleleft S_3$. (is not)

3. Let $H = \{(), (123), (132)\}$. Then, $(13)H = \{(13), (12), (32)\}$ and $H(13) = \{(13), (23), (12)\} \implies (13)H = H(13) \implies H \lhd S_3$.

4. If $H < G$ and $[G : H] = 2$. Then $H \lhd G$.

   Proof. If $g \in H, gH = Hg = H$. If $g \notin H, gH \neq H$. Since left coset partition G and $[G : H] = 2$. Then, H and $G \backslash H$ are the left (right) cosets of H in G. Which means $gH = G \backslash H$ and $Hg = G \backslash H$ so $gH = Hg = G \backslash H$ if $g \notin H$. Hence, $\forall g \in G, gH = Hg \implies H \lhd G$. □

End of Lecture ——

Proposition 3.16. *$H \lhd G$ iff $gHg^{-1} = H$ for all $g \in G$, where $gHg^{-1} = \{ghg^{-1} : h \in H\}$ and $gHg^{-1} < G$.*

Proposition 3.17. *Let G be a group and H a subgroup of G. Then, the followings are equivalent:*

1. *$H \lhd G$*

2. *$xhx^{-1} \in H$ for all $x \in G, h \in H$.*

Corollary 3.5. *Let G be a group. Then, $\{e_G\} \lhd G$ and $G \lhd G$*

Proof. Let $x \in G, h \in \{e_G\}$. Then, $xhx^{-1} = xe_Gx^{-1} = xx^{-1} = e_G \in \{e_G\}$, hence $\{e_G\} \lhd G$. Let $x \in G, h \in G \implies xhx^{-1} \in G$ so $G \lhd G$. □

Lecture 18: October 9th, 2024.

3.5.1 Simple and Quotient Group

Definition 3.19. A group G is said to be a **simple group** if it's only normal subgroups are $\{e_G\}$ and G.

Example 3.5.2. Let p be prime, $\mathbb{Z}/p\mathbb{Z}$ is a simple group.

Proof. Let H be a subgroup of $\mathbb{Z}/p\mathbb{Z}$. Then, by Lagrange's theorem, $|H|$ divides p hence $|H| = 1$ or $|H| = p \implies H = \{[0]_p\}$ or $H = \mathbb{Z}/p\mathbb{Z}$. Thus, $\mathbb{Z}/p\mathbb{Z}$ is simple. □

Theorem 3.5. *Let G be a group and $N \lhd G$. Then G/N is a group under the following well-defined binary operation*

$$(aN)\cdot(bN) := abN \tag{3.7}$$

Proof. We need to show that if $a,b,c,d \in G : aN = cN$ and $bN = dN$; then, $(ab)N = (cd)N$. i.e. $(cd)^{-1}ab \in N$. First, $aN = cN \implies c^{-1}a = n_1$ for some $n_1 \in N$; and $bN = dN \implies d^{-1}b = n_2$ for some $n_2 \in N$. Then,

$$\begin{aligned}(cd)^{-1}(ab) = (d^{-1}c^{-1})(ab) &= d^{-1}(c^{-1}a)b \\ &= d^{-1}n_1 b \\ &= \underbrace{d^{-1}n_1 d}_{\in N}\,\underbrace{n_2}_{\in N}\end{aligned}$$

Thus $(cd)^{-1}(ab) \in N$. □

Proposition 3.18. *Let G be a group and $N \lhd G$. Then, N is the identity of G/N.*

Proof. Let G be a group and $N \lhd G$. Then, for G/N,

$$(g_1N)\cdot N = (g_1N)(e_GN) = (g_1e_G)N = g_1N$$

And

$$(g_1N)^{-1} = g_1^{-1}N$$

Thus N is the identity for G/N. □

Proposition 3.19. *Consider the following properties:*

1. *Let G be an abelian group and $N < G$. Then, G/N is abelian.*

2. *Let G be a cyclic group and $N < G$. Then, G/N is cyclic.*

Proof. We'll prove for 1. Let G be abelian and $N < G$. Then, $N \triangleleft G$ and G/N is a group,

$$\begin{aligned}(g_1N)(g_2N) &= (g_1g_2)N \\ &= (g_2g_1)N \\ &= (g_2N)(g_1N)\end{aligned}$$

□

End of Lecture ———

Definition 3.20. The set G/N is called the **quotient group**.

Lecture 19: October 11th, 2024.

3.6 Permutation and Alternating Groups

Definition 3.21. Let S_n be the symmetric on n letters. An element $s \in S_n$ is called a **permutation**.

Definition 3.22. A **cycle of length a** is of the form $(a_1, a_2, \ldots, a_k)$ where the a_i's are distinct (a $k-$cycle).

- A $k-$ cycle has order k.
- The inverse of a $k-$cycle is a $k-$cycle.

Example 3.6.1. Consider the cycle $(a_1a_2 \cdots a_k) \implies (a_1a_2\cdots a_k)^{-1} = (a_k \cdots a_2a_1)$

Proposition 3.20. *Any σ can be written as a product of disjoints cycles.*

Example 3.6.2. $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix} = (13)(2)(45) = (13)(45)$

Proposition 3.21. *Disjoints cycles commute*

Example 3.6.3. $(13)(45) = (45)(13)$

Proposition 3.22. *Suppose $\sigma = \sigma_1\sigma_2\cdots\sigma_k$ where $\sigma_1, \ldots, \sigma_k$ are disjoint cycles of length $l_1, \ldots, l_k$ respecively. Then, ord(σ) = lcm$(l_1, \ldots, l_k)$*

Example 3.6.4. Consider $(123)(45)$. Then, it has order $\text{lcm}(3,2) = 6$. Similarly, for $(12)(34)$, it has order $\text{lcm}(2,2) = 2$. Note that the cycle $(12)(13)$ are not disjoint since $(12)(13) = (132)$ which has order 3 instead of 2.

3.6.1 Sign of a Permutation

Definition 3.23. A **transposition** is a $2-$cycle

Proposition 3.23. *Every $\sigma \in S_n$ can be written as a product of transposition.*

Proof. We first show that an cycle can be written as a product of transposition. Let $\sigma \in S_n$, then σ can be written as a product of disjoint cycles. An each cycle can be written as a product of transposition, hence σ can be written as a product of transposition. □

Example 3.6.5. $(123)(4567) = (13)(12)(47)(46)(45)$

Definition 3.24. Let $\sigma \in S_n$ and suppose that σ can be written as a product of k transposition(s). Then, **sign of permutation** σ is defined as

$$\operatorname{sgn}(\sigma) = (-1)^k \tag{3.8}$$

If $\operatorname{sgn}(\sigma) = 1 \implies k$ is even, we then say σ is even. Equivalently, if $\operatorname{sgn}(\sigma) = -1 \implies k$ is odd, we then say σ is odd. Also, sgn() is a well-defined function.

Theorem 3.6. *Let $\sigma \in S_n$ and suppose that σ can be written as a product of even number of transposition. Then, any product of transposition equalling σ must contain an even number of transposition.*

Example 3.6.6. $() = (12)(12) = (12)(12)(34)(34)$.

Proposition 3.24. *Let $\sigma, \tau \in S_n$. Then,*

$$sng(\sigma\tau) = sng(\sigma)sng(\tau) \tag{3.9}$$

Proof. Suppose σ can be written as a product of k transposition and similarly for τ of l transposition. Hence, $\sigma\tau$ can be written as a product of $l + k$ transposition. Then,

$$\operatorname{sgn}(\sigma\tau) = (-1)^{l+k} = (-1)^l(-1)^k = \operatorname{sng}(\sigma)\operatorname{sng}(\tau)$$

□

Notice that we $\operatorname{sgn}(12) = -1$, $\operatorname{sgn}(123) = (13)(12) = (-1)^2 = 1$ and $\operatorname{sgn}(1234) = (14)(13)(12) = (-1)^3 = -1$. Thus, we can generlize the equation 3.8 to yield

$$\operatorname{sgn}(a_1 \cdots a_k) = (-1)^{k+1} \tag{3.10}$$

Example 3.6.7. Find the sign of $(123)(456)(78)(86)$.
Solution: $\operatorname{sgn}\underbrace{(123)}_{=1}\underbrace{(456)}_{=1}\underbrace{(78)}_{=-1}\underbrace{(86)}_{=-1} = 1$.

Proposition 3.25. *$sgn(\sigma^{-1}) = sgn(\sigma)$*

Proof. $\text{sgn}(\sigma^{-1}\sigma) = \text{sgn}() = 1$. Using proposition 3.24, we'd realize that

$$\begin{aligned} \text{sgn}(\sigma^{-1}\sigma) = \text{sng}(\sigma^{-1})\text{sng}(\sigma) = 1 \\ \text{sgn}(\sigma^{-1}) &= \frac{1}{\text{sgn}(\sigma)} \\ &= \text{sgn}(\sigma) \qquad \left(\text{since } \frac{1}{(-1)^k} = (-1)^k\right) \end{aligned}$$

□

Definition 3.25. $A_n = \{\sigma \in S_n : \text{sgn}(\sigma) = 1\}$ is called the **alternating group** on n letters.

Claim: $A_n < S_n$

Proof. $\text{sgn}() = 1 \implies () \in A_n$. Let $\sigma, \tau \in A_n, \text{sgn}(\sigma) = \text{sgn}(\tau) = 1$. So $\text{sgn}(\sigma\tau) = \text{sgn}(\sigma)\text{sgn}(\tau) = 1 \implies \sigma\tau \in A_n$.
Let $\sigma \in A_n$; then we have $\text{sgn}(\sigma^{-1}) = \text{sgn}(\sigma) = 1 \implies \sigma^{-1} \in A_n$. Therefore, $A_n < S_n$. □

Claim: $|A_n| = \frac{n!}{2}$ for $n \geq 2$.

Proof. Let τ be an odd permutation in S_n. We define $f : A_n \longrightarrow S_n \backslash A_n, \sigma \mapsto \tau\sigma$ (where σ is even). We'll now show that this function is bijective.

- Injectivity: Suppose that $f(\sigma_1) = f(\sigma_2) \implies \tau\sigma_1 = \tau\sigma_2 \implies \sigma_1 = \sigma_2$.
- Surjectivity: Let $\alpha \in S_n \backslash A_n$, Then α is an odd permutation. THen $\tau^{-1}\alpha$ is even so $\tau^{-1}\alpha \in A_n$. Then, $f(\tau^{-1}\alpha) = \tau(\tau^{-1}\alpha) = \alpha$

Hence,

$$\begin{aligned} |A_n| &= |S_n \backslash A_n| \\ |S_n| &= |A_n| + |S_n \backslash A_n| = 2|A_n| \\ \implies |A_n| &= \frac{|S_n|}{2} = \boxed{\frac{n!}{2}} \end{aligned}$$

□

Theorem 3.7. *Let $n \geq 5$. Then, A_n is a simple group.*

Proof. Book Chapter 10. □

Example 3.6.8. $A_3 = \{(), (123), (132)\}$ and $A_4 = \{(), (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (14)(23), (13)(24)\}$.

Remark 3.6. *A_4 has no subgroup of order 6.*

End of Lecture ———

4 Group Isomorphism

4.1 Group Homomorphism

Lecture 20: October 21st, 2024.

Definition 4.1. Let $(G, \cdot)$ and $(H, \circ)$ be groups. A **homomorphism** $\phi : G \to H$ is a function that satisfies

$$\phi(x \cdot y) = \phi(x) \circ \phi(y) \tag{4.1}$$

Example 4.1.1. $\phi : (\mathbb{R} \backslash \{0\}, \times) \to (\mathbb{R}, +), x \mapsto \ln x$ is a homorphism since

$$\phi(xy) = \ln(xy) = \ln(x) + \ln(y)$$

Proposition 4.1. *Let $\phi : G \to H$ be a group homomorphism. Then,*

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

Proof. 1) $\phi(e_G) = \phi(e_G \cdot e_G) = \phi(e_G) \circ \phi(e_G) \implies e_H = \phi(e_G)$[1]
2) We know that $g \cdot g^{-1} = e_G \implies \phi(g \cdot g^{-1}) = \phi(e_G)$. Then,

$$\begin{aligned} \phi(g \cdot g^{-1}) &= \phi(e_G) \\ \phi(g) \circ \phi(g^{-1}) &= e_H \\ \phi(g)^{-1} \circ \phi(g) \circ \phi(g^{-1}) &= \phi(g)^{-1} \circ e_H \\ e_H \circ \phi(g^{-1}) &= \phi(g)^{-1} \end{aligned}$$

Thus $\phi(g^{-1}) = \phi(g)^{-1}$. □

Example 4.1.2. Consider more examples of homomorphism:

1. $\mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^x = \{R \backslash \{0\}\}, A \to \det A$ is a homomorphism since

$$\det\,(AB) = \det\, A \det\, B$$

2. $S_n \to \{\pm 1\}, \sigma \to \mathrm{sgn}(\sigma)$ is a homomorphism since

$$\mathrm{sgn}\,(\sigma\tau) = \mathrm{sgn}\,(\sigma)\mathrm{sgn}\,(\tau)$$

3. $G \to H, g \mapsto e_H$ (Trivial homomorphism)
4. G is abelian, $G \to G, g \mapsto g^n$ (for some $n \in \mathbb{N}$) is a homomorphism

[1] This is obtained by multiply $\phi(e_G)^{-1}$ in both side since $\phi(e_G)^{-1} \circ \phi(e_G) = e_H$

4.2 Group Isomorphism

Definition 4.2. A homomorphism $\phi : G \to H$ is an **isomorphism** if it is bijective.

Proposition 4.2. *Let $\phi : G \to H$ be an isomorphism. Then,*

1. *If $g \in G$, order($\phi(g)$)=order(g).*
2. *If K is a subgroup of G with $|K| = n$. Then, $\phi(K)$ is a subgroup of H with $|\phi(K)| = n$.*
3. *G is abelian $\iff$ H is abelian.*
4. *G is cyclic $\iff$ H is cyclic.*
5. *$\phi^{-1} : H \to G$ is an isomorphism.*

Remark 4.1. *When there exists an isomorphism between 2 groups, we call these 2 groups isomorphic (with the notation $\cong$).*

Example 4.2.1. Consider the followings isomorphisms:

- **Direct Product:** If $(A, \circ)$ and $(B, \cdot)$ are groups. Then, $A \times B$ is a group under
$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 \circ a_2, b_1 \circ b_2)$$
- **Groups with 4 Elements:** Consider 2 groups $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z}$. We see that the first group always have order of at most 2 while $\mathbb{Z}/4\mathbb{Z}$ would have order 4 $\implies$ the groups are not isomorphic.
- **Groups of Order 6:** Consider 2 groups $\mathbb{Z}/6\mathbb{Z}$ and S_3 are not isomorphic since $\mathbb{Z}/6\mathbb{Z}$ is abelian while S_3 is not.

Theorem 4.1. *Let G be a cyclic group with n elements. Then, G is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ which we denotes as*

$$G \cong \mathbb{Z}/n\mathbb{Z} \tag{4.2}$$

Proof. Consider $\phi : \mathbb{Z}/n\mathbb{Z} \to G, [a]_n \to g^a$ (and let $G = \langle g \rangle$). We need to show that ϕ is well-defined. $[a]_n = [b]_n \iff a - b$ is divisible by $n \iff a - n = nk$ for some $k \in \mathbb{Z}$. Then,

$$g^{a-b} = g^{nk} = (g^n)^k = (e_G)^k = e_G$$

Hence, $g^a = g^b \implies \phi([a]_n) = \phi([b]_n)$.
We now need to show that it's injective and surjective.

- Surjectivity: Let $y \in G$. $\exists 0 \geq m < n-1 : y = g^m \implies y = \phi([m]_n)$.
- Injectivity: Since the 2 sets have the same number of elements n. If ϕ is surjective, it must also be injective.

Therefore, ϕ is well-defined and bijective. Lastly, We need to show that ϕ is an isomorphism. Then,

$$\phi([a+b]_n) = g^{a+b} = g^a g^b = \phi([a]_n)\phi([b]_n)$$

Thus, if ϕ is an isomorphism, $G \cong \mathbb{Z}/n\mathbb{Z}$. □

Theorem 4.2. ***Chinese Remainder Theorem.*** *Let $m, n \in \mathbb{N}$. Then, $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ iff* $\gcd(m,n) = 1$

Proof. Suppose that $\gcd(m,n) > 1$. Then, $\operatorname{lcm}(m,n) = \frac{mn}{\gcd(m,n)} < mn$. Let $(a,b) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Then, $\{\operatorname{lcm}(m,n)\}(a,b) = ([0]_m, [0]_n)$. Thus, $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ has no element of order $mn \implies$ it is not cyclic $\implies$ it's not isomorphic. [2] □

End of Lecture

Lecture 21: October 23rd, 2024.

Proposition 4.3. *Let G be a group and $N \lhd G$. Then G/N is a group. The map $\Pi_N : G \longrightarrow G/N, g \mapsto gN$ is a group homomorphism.*

Proof. $\Pi_N(g_1, g_2) = (g_1 g_2 N) = (g_1 N)(g_2 N) = \Pi_N(g_1)\Pi_N(g_2)$. □

Example 4.2.2. $N = \{e_G\} \lhd G \implies G/N = \{g\{e_G\}, g \in G\} = \{\{g\} : g \in G\} \implies G/\{e_G\} \cong G$ with a homomorphism defined as $G \to G/\{e_G\}, g \mapsto \{g\} = g\{e_G\}$.

Similarly, $G/G \cong \{1\}$ where a homomorphism is defined as $G \to G/G, g \mapsto gG = e_G G = G$

4.2.1 Kernel

Definition 4.3. Let $\phi : G \longrightarrow H$ be a homomorphism. A **kernel** of ϕ is defined as

$$\ker\phi = \{g \in G : \phi(g) = e_H\} \tag{4.3}$$

Example 4.2.3. Consider the following kernels:

1. det: $\mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^x = \mathbb{R}\backslash\{0\}$. Then, $\ker(\det) = \{A \in \mathrm{GL}_n(\mathbb{R}) : \det A = 1\}$
2. sgn: $S_n \to \{\pm 1\}$. Then, $\ker(\operatorname{sgn}) = \{\sigma \in S_n : \operatorname{sgn}(\sigma) = 1\} = A_n$.
3. $\Pi_N : G \to G/N, g \mapsto gN$. Then $\ker \Pi_N = \{g \in G : gN = N\} = N$.

[2] If $\gcd(m,n) = 1$, $([1]_m, [1]_n)$ has order mn. (HW) and hence $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ is cyclic thus $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

Properties of Kernel

Proposition 4.4. *Let $\phi : G \to H$ be a group homomorphism. Then* $\ker\phi \lhd G$.

Proof. We need to first show that $\ker\phi < G$. $e_G \in \ker\phi$ by definition since $\phi(e_G) = e_H$. Let $x, y \in \ker\phi$. Then, $\phi(x) = e_H$ and $\phi(y) = e_H$. Hence $\phi(xy) = \phi(x)\phi(y) = e_H e_H = e_H \implies xy \in \ker\phi$. Lastly, let $x \in \ker\phi$ then, $\phi(x^{-1}) = \phi(x)^{-1} = e_H^{-1} = e_H \implies x^{-1} \in \ker\phi$.
We now show that $\ker\phi \lhd G$. Let $g \in G$ and $x \in \ker\phi$. We get that

$$\begin{aligned}\phi(gxg^{-1}) &= \phi(g)\phi(x)\phi(g^{-1})\\ &= \phi(g)e_H\phi(g^{-1})\\ &= \phi(g)\phi(g^{-1}) = \phi(gg^{-1}) = \phi(e_G) = e_H\end{aligned}$$

Hence $gxg^{-1} \in \ker\phi$. Thus, $\ker\phi \lhd G$. □

Proposition 4.5. *If $\phi : G \to H$ be a group homomorphism. Then, ϕ is injective $\iff$* $\ker\phi = \{e_G\}$.

Proof. ($\Longrightarrow$) Suppose that ϕ is injective. We show that $\ker\phi = \{e_G\} \implies e_G \in \ker\phi$ since $\phi(e_G) = e_H$. If $x \in \ker\phi$, then $\phi(x) = e_H = \phi(e_G)$. Since ϕ is injective, $x = e_G \implies \ker\phi = \{e_G\}$.

($\Longleftarrow$) Suppose that $\ker\phi = \{e_G\}$. We'll show ϕ is injective. Let $x, y \in G$ be such that:

$$\begin{aligned}\phi(x) &= \phi(y)\\ \phi(x)\phi(y)^{-1} &= e_H\\ \phi(x)\phi(y^{-1}) &= e_H\\ \phi(xy^{-1}) &= e_H \implies xy^{-1} \in \ker\phi\end{aligned}$$

So $xy^{-1} = e_G \implies x = y \implies \phi$ is injective. □

4.2.2 Isomorphism Theorem

Theorem 4.3. ***First Isomorphism Theorem.*** *Let G, H be groups and $\phi : G \to H$ be a group homomorphism. Then, $G/\ker\phi \cong \phi(G)$.*

Proof. Define $\overline{\phi} : G/\ker\phi \to \phi(G), g\ker\phi \mapsto \phi(g)$. We first need to show that it's well-defined. Suppose $g_1\ker\phi = g_2\ker\phi \implies g_2^{-1}g_1 \in \ker\phi \implies$

$\phi(g_2^{-1}g_1) = e_H \implies \phi(g_2)^{-1}\phi(g_1) = e_H \implies \phi(g_1) = \phi(g_2)$.
We need to show that ϕ is a homomorphism.

$$\begin{aligned}\overline{\phi}((g_1 \ker\phi)(g_2 \ker\phi)) &= \overline{\phi}(g_1 g_2 \ker\phi)\\ &= \phi(g_1 g_2)\\ &= \phi(g_1)\phi(g_2) = \overline{\phi}(g_1 \ker\phi)\overline{\phi}(g_2 \ker\phi)\end{aligned}$$

Thus it is a homomorphism.
We now show that it's injective.

$$\begin{aligned}\overline{\phi}(g \ker\phi) = e_H &\implies \phi(g) = e_H\\ &\implies g \in \ker\phi\\ &\implies g \ker\phi = \ker\phi\end{aligned}$$

Hence $\ker\overline{\phi} = \{\ker\phi\} = e_G / \ker\phi \implies \overline{\phi}$ is injective.
Now we show it to be surjective. Let $y \in \phi(G)$. Then, $y = \phi(x)$ for some $x \in G$ and hence $\overline{\phi}(x \ker\phi) = \phi(x) = y$. Thus $\overline{\phi}$ is surjective. □

Midterm Materials (Oct. 30th, 2024): First question: Euclidean algorithm. Second question: Cyclic groups. Third question: Langrange's theorem and possible applications. And fourth question: Fermat's and Euler's Theorem.

Frequently asked question: If p is a prime and $p \equiv 3 \pmod 4$. show that $x^2 \equiv -1 \pmod p$ has no solution.

Proof. Let $p = 3 + 4k$ for some $k \in \mathbb{N}$. Suppose that $x^2 \equiv -1 \pmod p$. If $p \mid x \implies x^2 \equiv \mod p$. Then, $p \nmid x$. Since p is prime, $\gcd(x, p) = 1$. Hence, by Fermat's little theorem, since $\frac{p-1}{2} \in \mathbb{N}$

$$\begin{aligned}x^{p-1} &\equiv 1 \pmod p\\ \left(x^2\right)^{\frac{p-1}{2}} &\equiv 1 \pmod p && \text{since } \frac{p-1}{2} \in \mathbb{N}\\ (-1)^{\frac{p-1}{2}} &\equiv 1 \pmod p\\ (-1)^{1+2k} &\equiv 1 \pmod p && \frac{p-1}{2} = 1 + 2k\\ -1 &\equiv 1 \pmod p\\ \implies 2 &\equiv 0 \mod p\end{aligned}$$

This is a contradiction since $p \geq 3$. (This proof can be done using Langrange's theorem: If $x^2 \equiv -1 \pmod p$, then x has order 4 in $U(p)$). □

End of Lecture

Lecture 22: October 26^{th}, 2024.

Continuing from last lecture, from the first isomorphism theorem, in particular, if ϕ is surjective then, $G/\ker\phi \cong H$ $(\phi(G) = H)$.

Theorem 4.4. ***Second Isomorphism Theorem.*** *Let G be a group and $N \lhd G, H < G$. Then, $H/H \cap N \cong HN/N$*

Proof. Consider $\Pi_N : G \to G/N, g \mapsto gN$. □

Theorem 4.5. ***Third Isomorphism Theorem.*** *Let G be a group and $N \lhd G$. If $H \lhd G$ containing N. Then, $H/N \lhd G/N$ and*

$$G/N\big/H/N \cong G/H \tag{4.4}$$

Proof. (Outline to proof.) Consider $\phi : G/N \to G/H, gN \mapsto gH$ then prove that this is well-defined bijective homomorphism. □

Theorem 4.6. ***Cayley's Theorem.*** *Let G be a group and sym(G) the of bijection from $G \to G$. Then, G is isomorphic to a subgroup of sym(G) i.e. There's an injective group homomorphism $G \to$ sym(G).*

Proof. Define $\lambda_g : G \to G, x \mapsto gx$. We've shown in assignment 3 that λ_g is bijective. Define $\phi : G \to \text{sym}(G), g \mapsto \lambda_g$. We now prove that ϕ is a group homomorphism.

$$\phi(g_1g_2) = \lambda_{g_1g_2} = \lambda_{g_1} \circ \lambda_{g_2} = \phi(g_1) \circ \phi(g_2)$$

This is because

$$\begin{aligned} \lambda_{g_1g_2} = (g_1g_2)x &= g_1(g_2x) \\ &= \lambda_{g_1}(g_2x) \\ &= \lambda_{g_1}(\lambda_{g_2}(x)) = (\lambda_{g_1} \circ \lambda_{g_2})(x) \end{aligned}$$

We now need to show ϕ is injective. Let $g \in \ker\phi$ then $\lambda_g = \text{id}_G \implies gx = x \forall x \in G \implies g = e_G$. $\ker\phi = \{e_G\}$ and hence ϕ is injective. Therefore, by the first isomorphism theorem. $G/\ker\phi \cong \phi(G) \implies G/e_G \cong \phi(G) \implies G \cong \phi(G) < \text{sym}(G)$. □

Application 1. Assume that G is finite. Define the following homomorphisms:

$$G \xrightarrow{\phi} \text{sym}(G) \xrightarrow{\text{sgn}} \{\pm 1\}$$

$\rho = \text{sgn} \circ \phi$ is a homomorphism $G \to \{\pm 1\}, \rho(g) = \text{sgn}(\lambda_g)$.
Application 2. $|G| = 2k$ where k is odd, then G has a subgroup with k elements.

5 Group Actions

Theorem 5.1. *If* $[x]_\sim$ *is a conjugacy class of* x*. Then,* $G/C(x) \to [x]_\sim, gC(x) \mapsto gxg^{-1}$ *where* $C(x) = \{g \in G : gxg^{-1} = x\}$

We've previously obtained the above theorem in the assignments. We will now attempt to generalize this (the mapping of $gC(x) \mapsto gxg^{-1}$ is a kind of action as you'd see in the definition below).

Definition 5.1. Let S be a set and G be a group. Then, an **action** of G on S is a function

$$* : G \times S \to S, (g, s) \mapsto g * s \tag{5.1}$$

We say that G acts on S (or S is a $G-$set) such that

- $e_G * s = s \forall s \in S$
- $g_1 * (g_2 * s) = (g_1 g_2) * s \forall g_1, g_2 \in G$ and $s \in S$.

Example 5.0.1. Consider the following actions:

1. Let S be a set and consider $\text{sym}(S)$. We can see that $\text{sym}(S)$ acts on S since $\sigma \in \text{sym}(S), s \in S \implies \sigma * s = \sigma(s)$. To show that this is an action, let $s \in S$. Then, $\text{Id}_S * s = \text{Id}_S(s) = s$. Let $\sigma_1, \sigma_2 \in \text{sym}(S)$. Then,

$$\begin{aligned}\sigma_1 * (\sigma_2 * s) &= \sigma_1(\sigma_2 * s)\\ &= (\sigma_1 \circ \sigma_2)(s) = (\sigma_1\sigma_2) * s\end{aligned}$$

2. Let G be a group and et $S = G$. Define an action $G \times G \to G, (g, x) \mapsto gxg^{-1}$. To show that this is an action, let $x \in G : x * e_G = e_G x e_G = x$. Let $g_1, g_2 \in G$. Then,

$$\begin{aligned}g_1 * (g_2 * x) &= g_1 * (g_2 x g_2^{-1})\\ &= g_1(g_2 x g_2^{-1}) g_1^{-1}\\ &= (g_1 g_2) x (g_1 g_2)^{-1} = (g_1 g_2) * x\end{aligned}$$

Definition 5.2. Let $s \in S$. The **orbit** of S is denoted as

$$\text{orb}(s) = \{g * x, g \in G\} \tag{5.2}$$

Example 5.0.2. For conjugation, $\text{orb}(x) = \{g * x, g \in G\} = \{gxg^{-1}, g \in G\} =$ conjugacy class of x.

Example 5.0.3. More example on group actions.
Let $S = G$, define a group action as $G \times G \to G, g * x = gx$. This is a group action since $e_G * x = e_G x = x$ and $g_1 * (g_2 * x) = g_1 * (g_2 x) = g_1(g_2 x) = (g_1 g_2)x = (g_1 g_2) * x$.

Definition 5.3. Let $s \in S$. The **stabilizer** of S is the subset of G defined as

$$\text{stab}(s) = \{g \in G : g * s = s\} \tag{5.3}$$

Example 5.0.4. The stabilizer of the conjugacy class is defined as $\text{stab}(x) = \{g \in G : g * x = x = \{g \in G : gxg^{-1} = x\}\} = C(x)$.

Proposition 5.1. *stab$(x) < G$*

Proof. $e_G * s = s$ hence $e_G \in \text{stab}(s)$. Let $g_1, g_2 \in \text{stab}(s)$. Then, $(g_1 g_2) * s = g_1 * (g_2 * s) = g_1 * s = s \implies g_1 g_2 \in \text{stab}(s)$. Lastly, $g_1 * s = s \implies g_1^{-1} * (g_1 * s) = (g_1^{-1} g_1)s = g^{-1} * s = e_G * s = g_1^{-1} * s \implies s = g^{-1} * s \implies g_1^{-1} \in \text{stab}(s)$ hence $\text{stab}(s) < G$. □

End of Lecture

Lecture 23: October 25th, 2024.

5.1 The Orbit-Stabilizer Theorem

Definition 5.4. Let G be a group. Then, a **conjugation** of G acts on G is given as

$$(g, x) \mapsto g * x = gxg^{-1} \tag{5.4}$$

The equivalence class that contains $x \in G$ that follows conjugation is called **conjugacy class** and is given as

$$\{gxg^{-1} : g \in G\} \tag{5.5}$$

Though not mentioned in class, there are many way to notate the conjugacy class of x and here are 2 of the most common: cl(x) and C_x.

Definition 5.5. Let G be a group. Then, a **centralizer** of x in G is defined as

$$C(x) = \{g \in G : gx = xg\} \tag{5.6}$$

We've seen this from the previous class that this is a result from taking the stabilizer of the conjugacy class of x.

Theorem 5.2. ***(Orbit-Stabilizer).*** *Let $s \in S$, there exists a bijection defined as:*

$$f_s : G/\text{stab}(s) \to \text{orb}(s),\ g\text{stab}(s) \mapsto g * s \tag{5.7}$$

Proof. We first show that f_s is a well-defined function. Let $g_1, g_2 \in G$: $g_1\text{stab}(s) = g_2\text{stab}(s) \iff g_2^{-1}g_1 \in \text{stab}(s)$. Then,

$$\begin{aligned} &\iff (g_2^{-1}g_1) * s = s \\ &\implies g_2 * ((g_2^{-1}g_1) * s) = g_2 * s \\ &\implies (g_2g_2^{-1}g_1) * s = g_2 * s \\ &\implies g_1 * s = g_2 * s \implies f(g_1\text{stab}(s)) \qquad = f_s(g_2\text{stab}(s)) \end{aligned}$$

Now, we need to show that f_s is injective. Suppose that $f(g_1\text{stab}(s)) = f_s(g_2\text{stab}(s)) \implies g_1 * s = g_2 * s \implies$ we're just reversing the process above $\implies (g_2^{-1}g_1) * s = s \implies g_2^{-1}g_1 \in \text{stab}(s) \implies g_1\text{stab}(s) = g_2\text{stab}(s)$.
Now we need to show that f_s is surjective. Let $s' \in \text{orb}(s)$. Then, $\exists h \in G$: $s' = h * s = f_s(h\text{stab}(s))$.

Thus, f_s is well-defined and bijective. □

Proposition 5.2. *S can be partitioned into a disjoint union of orbits.*

Proof. Define the following relation on S. $s_1 \sim s_2 \iff \exists g \in G : g * s_1 = s_2$.

Claim: $\sim$ is an equivalence relation.

1. Reflexivity: Let $s \in S$. Then, $e_G * s = s$.
2. Symmetry: Let $s_1, s_2 \in S : s_1 \sim s_2$. Hence, $\exists g \in G : g * s_1 = s_2 \implies s_1 = g^{-1} * s_2 \implies s_2 \sim s_1$.
3. Transitivity: Let $s_1, s_2, s_3 \in S : s_1 \sim s_2, s_2 \sim s_3$. Hence, $\exists g, g' \in G : g * s_1 = s_2$ and $g' * s_2 = s_3$. Then, $g' * s_2 = s_3 \implies g' * (g * s_1) = s_3 \implies (g'g) * s_1 = s_3 \implies s_1 \sim s_3$

Thus, $\sim$ is an equivalence relation.

So, the equivalence class of $s \in S$ under $\sim$ is $\{s' \in S : s' \sim s\} = \{g \in G : g * s\} = \text{orb}(s)$. Hence S can be partitioned into disjoint union of orbits. In particular, 2 orbits are equal or disjoint. □

In fact, we can write proposition 5.2 as the following:

$$S = \bigsqcup_{s_i} \text{orb}(s) \tag{5.8}$$

where s_i are representatives of the distinct orbits.[1]

[1] $\sqcup$ means disjoint union.

Proposition 5.3. *Suppose that G is finite and G acts on S. Let $s \in S$, then $|\text{orb}(s)|$ divides $|G|$.*

Proof. $|\text{orb}(s)| = |G/\text{stab}(s)|$ which divides $|G|$ because $|G| = [G : \text{stab}(s)]\ |\text{stab}(s)|$. □

End of Lecture ——

5.2 Cauchy's Theorem

Theorem 5.3. ***(Cauchy).*** *Let G be a finite group and p be a prime number dividing $|G|$. Then, G has an element of order p.*

Proof. Let $\sigma = (123\cdots p)$ and let $H = \langle G\rangle$ so $|H| = p$. Let $S = \{(x_1,\dots,x_p) \in G\times G\times\cdots\times G = G^p : x_1x_2\cdots x_p = e_G\}$. Then, $|S| = |G|^{p-1}$. Define the following action of H on S: Let $\tau \in H$ and $(x_1,\dots,x_p) \in S$

$$H * S \to S, \qquad \tau * (x_1,\dots,x_p) \mapsto (x_{\tau(1)},\dots,x_{\tau(p)})$$

e.g. $(123) * (x_1,x_2,x_3) = (x_2,x_3,x_1)$.

Lecture 24: October 28th, 2024.

Let $\tau,\lambda \in H$. We need to show that $(\tau\lambda) * (x_1,\dots,x_p) = \tau * (\lambda * (x_1,\dots,x_p))$. Now, it's obvious that $(e_{s_p}) * (x_1,\dots,x_p) = (x_1,\dots,x_p)$. Then,

$$\begin{aligned}\tau * (\lambda * (x_1,\dots,x_p)) &= \tau * (x_{\lambda(1)},\dots,x_{\lambda(p)})\\ &= (x_{(\tau\lambda)(1)},\dots,x_{(\tau\lambda)(p)})\\ &= (\tau\lambda) * (x_1,\dots,x_p)\end{aligned}$$

We still need to show that $\tau * (x_1,\dots,x_p) \in S$ i.e. $x_{\tau(1)}\cdots x_{\tau(p)} = e_G \forall\tau \in H$. If $(x_1,\dots,x_p) \in S$. Then, $G * (x_1,\dots,x_p) = (x_2,x_3,\dots,x_p,x_1) \in S$ since

$$\begin{aligned}x_1x_2\cdots x_p &= e_G\\ \implies x_2x_3\cdots x_p &= x_1^{-1}\\ \implies x_2x_3\cdots x_px_1 &= x_1^{-1}x_1 = e_G\end{aligned}$$

Then, inductively, $G^k * (x_1,\dots,x_p) \in S, \forall k \in \{0,1,\dots,p-1\}$. Hence, $*$ defines a group action on S. We know that S is a disjoint union of H-orbits. Then,

$$S = \bigsqcup_{i=1}^{n} \text{orb}(s_i)$$

where $s_1,s_2,\dots s_n$ are representatives of the distinct orbits. Then, let $s_1,s_2,\dots s_k$ be representatives of **singleton**[2] orbits and $s_{k+1},\dots,s_n$ be representatives of

[2] Singletons are sets with 1 element.

non-singleton orbits. Note that $(e_G, \dots, e_G) \in G^p$ which satisfies $\operatorname{orb}(e_G, \dots, e_G) = \{(e_G, \dots, e_G)\}$. Then,

$$\begin{aligned} S = \left(\bigsqcup_{i=1}^{k} \operatorname{orb}(s_i) \right) &\bigsqcup \left(\bigsqcup_{i=k+1}^{n} \operatorname{orb}(s_i) \right) \\ \implies |S| &= k + qp && \text{for some } q \in \mathbb{N} \\ \implies |G|^{p-1} &= k + qp \end{aligned}$$

so $p \mid k$ and since $k \geq 1 \implies k \geq p$. Let $(x_1, \dots, x_p) \in S : \operatorname{orb}(x_1, \dots, x_p) = \{(x_1, \dots, x_p)\}$ Then,

$$\begin{aligned} &\iff \tau * (x_1, \dots, x_p) = (x_1, \dots, x_p)\ \forall \tau \in H, x_1 \cdots x_p = e_G \\ &\iff \sigma * (x_1, \dots, x_p) = (x_1, \dots, x_p) \text{ and } x_1 \cdots x_p = e_G && \text{since } H = \langle G \rangle \\ &\iff (x_2, x_3, \dots, x_p, x_1) = (x_1, x_2, \dots, x_p) \text{ and } x_1 \cdots x_p = e_G \\ &\iff x_1 = x_2 = x_3 = \cdots = x_p \text{ and } x_1 x_2 \cdots x_p = e_G \\ &\iff x_1^p = e_G, x_1 = x_2 = x_3 = \cdots = x_p \end{aligned}$$

Hence singleton orbits are of the form $(x, \dots, x)$ where $x^p = e_G$. Since, $k \geq p, \exists x \neq e_G : x^p = e_G$. Then, $\operatorname{ord}(x) \mid p$ is prime and $x \neq e_G$ so x has order p. □

Theorem 5.4. *Let G be a group and S a G−set. Then, there exists a homomorphism G → Sym(S)*

Proof. $G \times S \to S, (g, s) \mapsto g * s$. Let $g \in G$ and define $\lambda_g : S \to S, \lambda_g(s) = g * s$.

Claim: $\lambda_g \in \operatorname{Sym}(s)$.
$\lambda_g \circ \lambda_{g^{-1}} = \operatorname{Id}_s$. Since $(\lambda_g \circ \lambda_{g^{-1}})(s) = g * (g^{-1} * s) = (gg^{-1}) * s = s$. Similarly, $\lambda_{g^{-1}} \circ \lambda_g = \operatorname{Id}_s$.

Now, define $\rho : G \to \operatorname{Sym}(S),\ g \mapsto \lambda_g$ where ρ is a homomorphism. We need to show that $\rho(g_1 g_2) = \rho(g_1) \circ \rho(g_2)$ i.e. $\lambda_{g_1} \circ \lambda_{g_2} = \lambda_{g_1 g_2}$. Let $s \in S$, then

$$\begin{aligned} (\lambda_{g_1} \circ \lambda_{g_2})(s) &= \lambda_{g_1}(\lambda_{g_2}(s)) \\ &= g_1 * (g_2 * s) \\ &= (g_1 g_2) * s = \lambda_{g_1 g_2}(s) \end{aligned}$$

hence $\rho(g_1 g_2) = \lambda_{g_1 g_2} = \lambda_{g_1} \circ \lambda_{g_2} = \rho(g_1) \circ \rho(g_2)$. Thus, there's a homomorphism from G to $\operatorname{Sym}(S)$. □

End of Lecture

We can check for the kernel of this homomorphism too. $\ker\rho = \{g \in G : \lambda_g = \mathrm{Id}_S\}$ then,

$$\begin{aligned} g \in \ker &\iff g * s = s \forall s \in S \\ &\iff g \in \mathrm{stab}(s) \forall s \in S \\ &\iff g \in \bigcap_{s \in S} \mathrm{stab}(s) \end{aligned}$$

so $\ker\rho = \bigcap_{s\in S} \mathrm{stab}(s)$.

Lecture 25: November 1st, 2024.

5.3 Coset Representations

Definition 5.6. Let G be a group and $H < G$ of finite index n. Define G acts on $G/H = \{xH : x \in G\}$ as

$$\begin{aligned} * : G \times G/H \to G/H \\ g * xh = gxh \end{aligned}$$

Then, $*$ is a group action.

We can evidently tell that this is a group action. Let $x, g_1, g_2 \in G$. Then,

1. $e_G * xh = e_G xh = xh \in G/H$.
2. $g_1 * (g_2 * xH) = g_1 * (g_2 xH) = (g_1 g_2)xH = (g_1 g_2) * xH$.

One thing you'd realize from this action is that it induces a homomorphism $\rho : G \to \mathrm{Sym}(G/H) \cong S_n$. So now you can ask, what is $\ker\rho$? Well...we need to find $\mathrm{stab}(s) \forall s \in G/H$.

Claim: Let $x \in$, then $\mathrm{stab}(xH) = xHx^{-1}$.
proof. $g \in \mathrm{stab}(xH)$. Then,

$$\begin{aligned} &\iff gxH = xH \\ &\iff x^{-1}gx = H \\ &\iff x^{-1}gx \in H \\ &\iff g \in xHx^{-1} \end{aligned}$$

Hence $\ker\rho = \bigcap_{x\in G} xHx^{-1}$. Then, by the first isomorphism theorem, $G/\ker\rho \cong \rho(G) < \mathrm{Sym}(G/H)$, so $|G/\ker\rho| = |\rho(G)|$ divides n. Then,

$$\ker\rho = \bigcap_{x \in G} xHx^{-1} \subseteq e_G H e_G^{-1} = H$$

Thus, $\ker\rho < H$. Interestingly, index of $\ker\rho$ is finite even if G is infinite.

Proposition 5.4. *Let G be a group and $H < G$. Then, there exists a normal subgroup $N \lhd G : N \subseteq H$ and $[G:N] \mid n!$*

Proposition 5.5. *Let G be a finite group and H a subgroup of G of index p where p is the smallest prime division of $|G|$. Then, $H \lhd G$*

Proof. (Outline). Let N be the kernel of the coset representation of the group action G on G/H. $N < H$ and $[G:N]$ divides $p! \implies [G:N]$ divides $|G| = [G:N]|N|$. Hence, $[G:N]$ divides $\gcd(|G|, p!)$. Since p is the smallest prime divisor of G, then $\gcd(|G|, p!) = p$. Hence $[G:N] \mid p \implies [G:N] = 1$ or p. If $[G:N] = 1$, then $N = G$ but $N \subseteq H \subsetneq G$ which is a contradiction. Hence, $[G:N] = p$ and $N \subseteq H \subseteq G$, then

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

This means $p = p[H:N]$ so $[H:N] = 1$ so $H = N$. Now, $N \lhd G$ and $H = N \implies H \lhd G$. □

5.4 P-Groups

Definition 5.7. Let G be a group and S be a $G-$set. We say that G acts **transitively** on S (i.e. the action of G on S is transitive) if S is the only orbit.

Proposition 5.6. *Let S be a finite group with n elements. Then, G acts transitively on $S \iff G$ has a subgroup of index n.*

Definition 5.8. A subgroup of S_n is said to be **transitive** if for all $i, j \in \{1, \dots, n\}$, there exists $\sigma \in H : \sigma(i) = j$.

Example 5.4.1. Consider the following examples:

- $H = \{1, (12)\}$ is not a transitive subgroup in S_3.
- $H = \{1, (123), (132)\}$ is a transitive subgroup in S_3.

Definition 5.9. Let p be prime. A finite group G is said to be a ***p*-group** if $|G| = p^k$ for some $k \in \mathbb{N}$[3]

[3] In certain textbooks, we they includes trivial group as $p-$group but here we will not do that.

Here are some properties that we've previously done about $p-$group in homeworks 4 and 6: If G is a finite $p-$group, then

1. $|Z(G)| \geq p$ with
$$|G| = |Z(G)| + \sum_{i=k}^{n} [G : C(x_i)] \tag{5.9}$$
where $x_k, \ldots, x_n$ are representatives.

2. If G has order p^2 then it is abelian.

End of Lecture ———

Lecture 26: November 4th, 2024.

Definition 5.10. (better definition). Let S be a $G-$set. We say that the action of G on s is **transitive** if there is only 1 orbit.

Proposition 5.7. *Let G be a $p-$group ($|G| = p^k, k \in \mathbb{N}$ and p is prime). Then, if $i \in \{0, 1, \ldots, k\}$, G has a normal subgroup of order p^i.*

Proof. We will prove by induction:

- <u>$k = 1$:</u> $|G| = p \implies$ only $\{e_G\}$ and G are normal subgroup of G.

- <u>Induction:</u> Suppose the result holds for groups of size p^{k-1} and let G be a group of size p^k. WE know from homework 4, $|Z(G)| = p^\alpha$ for some $\alpha \in \mathbb{N}$, hence $p \big| |Z(G)|$. Hence, by Cauchy's theorem, $Z(G)$ has an element x of order p. Let $H = \langle x \rangle, H \lhd G$ (let $y \in \langle x \rangle \subseteq Z(G)$ and $g \in G, gyg^{-1} = ygg^{-1} = y \in \langle x \rangle$). So, G/H is a group of size $\frac{p^k}{p} = p^{k-1}$. Let $\Pi_H : G \to G/H$ denote the projection $g \mapsto gH$. By the induction hypothesis, if $i \in \{0, 1, \ldots, k-1\}$, there eixsts a normal subgroup $\tilde{H}$ of G/H of size p^i. $\Pi_H^{-1}(\tilde{H})$ is a normal subgroup of G, then
$$|\Pi_H^{-1}(\tilde{H})| = |H| \cdot |\tilde{H}| = p \cdot p^k = p^{k+1}$$

Hence, if $i \in \{0, 1, \ldots, k\}$, G has a normal subgroup of order p^i. Hence G has normal subgroups of size $p, p^2, \ldots, p^k$ and of size 1 which is $\{e_G\}$. □

Definition 5.11. Let G be a group and S a $G-$set. Define $S_G = \{s \in S : g * s = s \forall g \in G\}$. We say that an element $s_0 \in S_G$ is a **fixed point** of the action G on S.

Example 5.4.2. Consider G acting on G by conjugation, $(g,x) \mapsto g * x = gxg^{-1}$. Then,

$$\begin{aligned} G_G &= \{x \in G : g * x = x \forall g \in G\} \\ &= \{x \in G : gxg^{-1} = x \forall g \in G\} \\ &= \{x \in G : gx = xg \forall g \in G\} = Z(G) \end{aligned}$$

Remark 5.1. *$Z(G)$ is the center of a group.*

Proposition 5.8. $s_0 \in S_G \iff \operatorname{orb}(s_0) = \{s_0\}$

Proof. $s_o \in S_G \iff g * s_0 = s_0 \forall g \in G \iff \operatorname{orb}(s_0) = \{s_0\}$. □

Remark 5.2. *S_G is the union of singleton orbits.*

Theorem 5.5. *Let G be a $p-$group*[4] *and S a finite $G-$set. Then, $|S| \equiv |S_G| \mod p$*

Proof. Homework. □

Theorem 5.6. *Let G be a finite group and p be prime. Suppose that G has size $p^k m$ where $k \in \mathbb{N} \cup \{0\}$ and $\gcd(m,p) = 1$. Then, G has a subgroup of order p^k*

Proof. We will prove by induction:

- $\underline{|G| = 1:}$ Then $|G| = p^0 \times 1$ so $\{e_G\} < G$ of order p^0.

- Induction: Suppose that G is a group size $p^k m$, where $k \in \mathbb{N} \cup \{0\}$ and $\gcd(m,p) = 1$ and that the statement statement is true for all groups of size $< |G|$. If $p \nmid |G|, k = 0$. Then, $\{e_G\} < G$ of order $p^0 = 1$.
  If $p \mid G$, then
  $$|G| = |Z(G)| + \sum_{i=a}^{n} [G : C(x_i)] \tag{5.10}$$
  where $x_a, \ldots, x_n$ are representatives of non-singleton conjugacy classes and $C(x_i)$ are its centralizer. Assume that p does not divided $[G : C(x_{i_0})]$ for some $i_0 \in \{a, \ldots, n\}$. Then,
  $$|G| = [G : C(x_{i_0})]|C(x_{i_0})|$$
  So $p^k \Big| |C(x_{i_0})|$ and hence $|C(x_{i_0})| = p^k l$ where $\gcd(p,l) = 1$. So,
  $$[G : C(x_{i_0})] = |\text{conjugacy class of } x_{i_0}| > 1$$

[4] In this class, we consider $p-$group is finite.

Hence, $|C(x_{i_0})| < |G|$. Hence, by induction hypothesis, $C(x_{i_0})$ has a subgroup of size p^k. So G has a subgroup of size p^k. Now we need to look at if $p\Big|[G:C(x_i)]$. Suppose that $p\Big|[G:C(x_i)], \forall i\{a,\dots,n\}$. So p divides $\sum_{i=a}^{n}[G:C(x_i)]$. But we know that

$$|G| = [G:C(x_{i_0})]|C(x_{i_0})|$$

Hence, $|Z(G)|$ is divisible by p. So $Z(G)$ has an element x of order p. By Cauchy's theorem, since $\langle x\rangle \subseteq Z(G)$. Then, $H = \langle x\rangle \lhd G$ and G/H is a group of order $p^{k-1}m < p^k m$. By the induction hypothesis, G/H has a subgroup $\tilde{H}$ of order p^{k-1}. Hence $\Pi^P{-1}(\tilde{H})$ is a subgroup of order $|\tilde{H}||H| = p^{k-1}p = p^k$.

□

End of Lecture

Lecture 27: November 6th, 2024.

5.5 Sylow's Theorems

Theorem 5.7. ***(Sylow's First Theorem).*** *Let G be a finite group and p be a primber number dividing* $|G|$*. Then, if* $|G| = p^k m$ *where* $\gcd(p,m) = 1$ *and* $k \in \mathbb{N}$*. Then G has a subgroup of order* p^k

Definition 5.12. Any such subgroup that satisfies the Sylow's first theorem, it's called a **Sylow** $p-$subgroup of G.

Example 5.5.1. $|S_3| = 6 = 2 \times 3$. Since, $S_3 = \{(),(12),(13),(23),(123),(132)\}$, then, $\{(),(12)\}$, $\{(),(13)\}$ and $\{(),(23)\}$ are Sylow $2-$subgroup of S_3. $A_3 = \{(),(123),(132)\}$ is a Sylow $3-$subgroup.

Recall: Let G be a $p-$group ($|G| = p^k, k \in \mathbb{N}$) and S a finite $G-$set. Then, $|S| \equiv |S_G| \bmod p$ where S_G is the set of fixed points.

Proof. We know that S is a disjoint union of orbits. Let $s_1,\dots,s_k$ be representatives of singleton orbits and $s_{k+1},\dots,s_n$ be representatives of non-singleton orbits. Then,

$$\begin{aligned} S &= \bigsqcup_{i=1}^{n} \operatorname{orb}(s_i) \\ &= \left(\bigsqcup_{i=1}^{k} \operatorname{orb}(s_i)\right) \bigsqcup \left(\bigsqcup_{i=k+1}^{n} \operatorname{orb}(s_i)\right) \\ \implies |S| &= \left(\bigsqcup_{i=1}^{k} |\operatorname{orb}(s_i)|\right) + \left(\bigsqcup_{i=k+1}^{n} |\operatorname{orb}(s_i)|\right) \\ &= |S_G| + \sum_{i=k+1}^{n} [G : \operatorname{stab}(s_i)] \end{aligned}$$

$\forall k+1 \le 1 \le n$, $[G : \operatorname{stab}(s_i)]$ divides $|G| = p^k$, then $[G : \operatorname{stab}(s_i)] \in \{1, p, p^2, \ldots, p^k\}$. $|\operatorname{orb}(s_i)| = [G : \operatorname{stab}(s_i)] > 1 \implies |\operatorname{orb}(s_i)|$ is divisible by p for all $i \in \{k+1, \ldots, n\}$. Hence $|S| \equiv |S_G| \mod p$ (if there's no fixed points, the result is clear). □

Definition 5.13. Let G be a group and H a subgroup of G. A subgroup K of G is said to be **conjugated** to H if there exists $g \in G$ such that $gKg^{-1} = H$. **Conjugacy** is an equivalence relation on the set of subgroups of G.

Proposition 5.9. *Let G be a group and $g \in G$. Let $\phi_g : G \to G, x \mapsto gxg^{-1}$. ϕ_g is an isomorphism from G to G.*

Proof. Let $x_1, x_2 \in G$. Then, $\phi_g(x_1, x_2) = g(x_1x_2)g^{-1} = gx_1g^{-1}gx_2g^{-1} = (gx_1g^{-1})(gx_2g^{-1}) = \phi_g(x_1)\phi_g(x_2)$. So, it's a homomorphism. $(\phi_{g^{-1}} \circ \phi_g)(x) = g^{-1}(\phi_g(x))g = g^{-1}(gxg^{-1})g = x$. Similarly, $(\phi_g \circ \phi_{g^{-1}})(x) = x$. Hence $\phi_{g^{-1}}$ is the inverse of ϕ_g and hence ϕ_g is bijective and hence an isomorphism. □

Corollary 5.1. *Any conjugate subgroups of G are isomorphic. Let H and K be conjugate subgroups. Then, for some $g \in G, K = gHg^{-1} = \phi_g(H)$, ϕ_g is an isomorphism. So $H \cong gHg^{-1} = K$.*

Theorem 5.8. ***(Sylow's Second Theorem).*** *Let G be a finite group and p a prime dividing $|G|$ such that $|G| = p^k m$ where $k \in \mathbb{N}$ and $\gcd(p, m) = 1$. Then, If K and P are two Sylow $p-$subgroup of G, then K is conjugate to P.*

Proof. Define the following action of K on G/P as $y * xp = kxp$ where $y \in K$ and $x \in G$. Now, $|K| = p^k$ so K is a $p-$group and $|G/P| = m$. Let n be the number of fixed points of this action. Then, $|G/P| \equiv n \mod p$ so $n \not\equiv 0 \mod p$ since $\gcd(p, m) = 1$. Hence, $n \neq 0$ and $n \ge 1$. Hence, this action has a fixed point. Let x_0p be a fixed point, then $\operatorname{orb}(x_0p) = \{x_0p\}$. Hence, $\forall y \in$

$K, y * x_0 p = x_0 p \implies y x_0 p = x_0 p \implies x_0^{-1} y x_0 p = p$, so $\forall y \in K, x_0^{-1} y x_0 \in P$. This also means $y \in x_0 P x_0^{-1} \implies K \subseteq x_0 P x_0^{-1}$.
Now, $|K| = p^k, |x_0 P x_0^{-1}| = |P| = p^k$ hence $K = x_0 P x_0^{-1}$. □

Theorem 5.9. ***(Sylow's Third Theorem).*** *Let G be a finite group $|G| = p^k m$ where $k \in \mathbb{N}$, $\gcd(p, m) = 1$ and p is prime. Then, the n_p of Sylow $p-$subgroups satisfies $n_p \equiv 1 \mod p$ and n_p divides m.*

Proof. Let P be a Sylow $p-$subgroup of G and consider the set $S = \{xPx^{-1}, x \in G\}$. Note that by Sylow's second theorem, S is the set of all subgroups of size p^k. Let P act on S defined as $*P \times S \to S, y * xPx^{-1} \mapsto (yx)P(yx)^{-1}$. If $x = e_G, xPx^{-1} = P$. So $P \in S$, if $y \in P, yPy^{-1} = P$. So, $P \in S$ is a fixed point of this action. Suppose P' is a fixed point of this action. Then, $y * P' = P' \ \forall y \in P$ hence $yP'y^{-1} = P' \ \forall y \in P$, hence for any $y \in P, yP' = P'y$. Therefore $y \in N_G(P') = \{g \in G : gP' = P'g\}$ ($N_G(P')$ is the normalizer of P' in G, $N_G(P') < G$ and $P' \subseteq N_G(P')$ by Homework 7). □

End of Lecture

Lecture 28: November 8th, 2024.

Proof. *(Continuation from previous lecture).* We got that $y \in N_G(P')$ hence $P \subseteq N_G(P')$. We also have that $P' \subseteq N_G(P')$ since if $x \in P', xP'x^{-1} = P' \implies N_G(P')$. P' and P are subgroups of $N_G(P')$ then,

$$P' \text{ and } P < N_G(P') < G$$

We know that $|P| = |P'| = p^k, |G| = p^k m$ hence $N_G(P') = p^k l$ where $\gcd(l, p) = 1$. Hence, P and P' are Sylow $p-$subgroup of $N_G(P')$. Therefore, by Sylow's Second Theorem, P and P' must be conjugate in $N_G(P')$. Hence $\exists z \in N_G(P') : zP'z^{-1} = P \implies P' = P$. P is a $p-$group and S is a $P-$set, and the action of P on S has only one fixed point so

$$|S| \equiv \text{ number of fixed points } \mod p$$
$$\implies n_p \equiv 1 \text{ mod } p$$

$n_p \mid m$, by proposition 5.10. (next page), $n_p = [G : N_G(P)]$. $P < N_G(P)$ so $[G : P] = [G : N_G(P)][N_G(P) : P] \implies m = n_p[N_G(P)] \implies n_p \mid m$. □

NOTE: The final exam has 7 questions: 4 questions on groups and 3 questions on ring. Most questions are post-midterm materials. As the professor emphasized: "this final is way easier than the original". Every homeworks post-midterm are important. Remember to prove first and second Sylow's Theorem.

Proposition 5.10. *Let G be a group and H a subgroup of G. Let $S = \{xHx^{-1}, x \in G\}$ which is the set of conjugate of H. Then, if G is finite, $|S| = [G : N_G(H)]$ where $N_G(H) = \{g \in G : gHg^{-1} = H\}$.*

Proof. G acts transitively on S by $G \times S \to$, $g * xHx^{-1} \mapsto gxHx^{-1}$. The proof that $*$ defines an action on S has been done in the homework. This action is transitive since,

$$\begin{aligned} \text{orb}(H) &= \{g * H, g \in G\} \\ &= \{gHg^{-1}, g \in G\} = S \end{aligned}$$

Thus, S is a transitive $G-$set. Now let's look at the stabilizer:

$$\begin{aligned} \text{stab}(H) &= \{g \in G : g * H = H\} \\ &= \{g \in G : gHg^{-1} = H\} = N_G(H) \end{aligned}$$

So $N_G(H) < G$. If G is finite then,

$$\begin{aligned} &[G : \text{stab}(H)] = |\text{orb}(H)| \\ \implies &[G : N_G(H)] = |S| \end{aligned}$$

□

End of Lecture

Review of Coset Representation

Theorem 5.10. *Let G be a group and $H < G$ of index n where $n \in \mathbb{N}$. Then, $\exists N \lhd G : N \subseteq H$ and G/N is isomorphic to a subgroup of S_n.*
Note that $N = \bigcap_{x \in G} xHx^{-1}$ and $[G : N]$ divides n.

Example 5.5.2. Let's apply this to $G = S_4$ which has $|S_4| = 24 = 2^3 \times 3$. We first look symmetry of a square can be defined as (dihedral group K) Id $=$ $()$, $r = (1234)$, $r^2 = (13)(24)$, $r^3 = (1432) = (4321)$, $V = (12)(34)$, $H = (14)(23)$, $D_1 = (24)$ and $D_2 = (13)$ i.e. $K = \{\text{Id}, r, r^2, r^3, V, H, D_1, D_2\}$. So, we can see that $K < S_4$ but is not normal in S_4 since $(12)(13)(12) = (23) \in K$. There exists a normal subgroup N of S_4, $N \subseteq K$ such that G/N is isomorphic to a subgroup of S_3.

6 Ring and Fields

Lecture 29: November 11^{th}, 2024.

6.1 Rings

Definition 6.1. A **ring (R)** is a non-empty set with two binary operations:

$$+ : R \times R \to R \qquad \text{(Addition)}$$
$$\times : R \times R \to R \qquad \text{(Mutliplication)}$$

Such that

1. $(R, +)$ is an abelian group and the neutral element for $+$ is denoted by 0_R.
2. There exists an element $1_R \in R : \forall a \in R, a \times 1_R = 1_R \times a = a$.
3. $\times$ is associative i.e. $\forall a, b, c \in R, (a \times b) \times c = a \times (b \times c)$.
4. Closed under distributivity i.e. $a \times (b + c) = a \times b + a \times c$

Example 6.1.1. Consider the following examples:

- $(\mathbb{Z}, +, \times)$ is a ring.
- $(\mathbb{Q}, +, \times)$ is a ring.
- $(\mathbb{R}, +, \times)$ is a ring.
- $M_n(\mathbb{R})$, which is the set of $n \times n$ matrices, is a ring.
- $(\mathbb{Z}/n\mathbb{Z})$ is a ring with addition and multiplication $\bmod n$.

Remark 6.1. *The additive inverse of $a \in R$ is denoted by $-a$, specifically, $a + (-a) = 0_R$.*

Remark 6.2. *$\times$ can somtimes be notated as $\cdot$. In somes cases, multiplication won't be denoted at all e.g. $a \times b = a \cdot b = ab$.*

Proposition 6.1. *Let R be a ring. Then,*

1. $0_R \cdot a = 0_R$
2. $a \cdot 0_R = 0_R$

Proof. 1) $0_R \cdot a = (0_R + 0_R) \cdot a = 0_R \cdot a + 0_R \cdot a \implies 0_R = 0_R \cdot a$. 2) will follows the same argument. □

Proposition 6.2. *Let R be a ring and $a \in R$. Then, $(-1_R) \cdot a = -a$*

Proof. $0_R = 0_R \cdot a = (1_R + (-1_R)) \cdot a = 1_R \cdot a + (-1_R) \cdot a = a + (-1_R) \cdot a \implies (-1_R) \cdot a = -a$ (by the uniqueness of inverses in a group). □

Proposition 6.3. *Let R be a ring and suppose that $1_R = 0_R$. Then, $R = \{0_R\}$ (zero ring).*

Proof. Let $a \in R$. Then, $a = 1_R \cdot a = 0_R \cdot a = 0_R$ so $R = \{0_R\}$. □

Remark 6.3. *From now on, $1_R \neq 0_R$ unless it's stated that they're equal.*

Definition 6.2. A ring $(R, +, \times)$ os said to be **commutative** if × is commutative such that

$$a \times b = b \times a, \ \forall a, b \in R$$

Example 6.1.2. $\mathbb{R}, \mathbb{Z}, \mathbb{Q}, \mathbb{Z}/n\mathbb{Z}$ are commutative rings. $M_n(\mathbb{R})$ where $n \geq 2$ is non-commutative.

6.2 Integral Domain and Field

Definition 6.3. Let R be a commutative ring. A non-zero element $a \in R$ is said to be a **zero divisor** if there exists a non-zero $b \in R : ab = 0_R$.

Example 6.2.1. In $\mathbb{Z}/4\mathbb{Z}$, 2 is a zero divisor as $2 \cdot 2 = 0$. In $\mathbb{Z}/6\mathbb{Z}$, $2, 3$ are zero divisor as $2 \cdot 3 = 0$. In $\mathbb{Z}/8\mathbb{Z}$, $2, 4$ are zero divisor as $2 \cdot 4 = 0$.

Definition 6.4. Let R be a commutative ring, R is said to be an **integral domain** if R has no zero divisors.

Example 6.2.2. $\mathbb{R}, \mathbb{Q}, \mathbb{Z}$ are integral domains.

Theorem 6.1. *$\mathbb{Z}/n\mathbb{Z}$ is an integral domain iff n is prime.*

Proof. If n is not prime, write $n = ab$ where $2 \leq a, b < n$. So $[a]_n$ and $[b]_n$ are non-zero in $\mathbb{Z}/n\mathbb{Z}$ and $[a]_n \cdot [b]_n = [ab]_n = [0]_n$ so $[a]_n$ and $[b]_n$ are zero divisors.
Suppose that n is prime. Let $n = p$. Let $a, b \in \mathbb{Z}/n\mathbb{Z}$ be non-zero. Then, $a, b \in U(p)$ hence $ab \in U(p)$ and hence $ab \neq 0_p$. Hence $\mathbb{Z}/n\mathbb{Z}$ is an integral domain if n is prime. □

Remark 6.4. *Let R be a commutative ring. Then the following are equivalent:*

1. *R is an integral domain.*
2. *If $a, b \in R$ and $ab = 0_R \implies a = 0_R$ or $b = 0_R$.*

Definition 6.5. A commutative ring R is said to be a **field** if for all $a \neq 0_R$, there exists non-zero $b \in R : ab = 1_R$. (Every non-zero element has a multiplicative inverse)

Example 6.2.3. $\mathbb{R}$ and $\mathbb{Q}$ are fields. $\mathbb{Z}$ is not a field.

Proposition 6.4. *Let $\mathbb{F}$ be an field. Then, $\mathbb{F}$ is an integral domain.*

Proof. Let $a, b \in \mathbb{F}$ be such that $ab = 0_{\mathbb{F}}$. If $ab = 0_{\mathbb{F}}$, we're done. Suppose that $a \neq 0_{\mathbb{F}}$. There exists $c \in \mathbb{F}$ such that $ca = ac = 1_{\mathbb{F}}$. Then,

$$\begin{aligned} ab &= 0_{\mathbb{F}} \\ c(ab) &= c \cdot 0_{\mathbb{F}} = 0_{\mathbb{F}} \\ (ca)b &= 0_{\mathbb{F}} \\ 1_{\mathbb{F}} b &= 0_{\mathbb{F}} \\ b &= 0_{\mathbb{F}} \end{aligned}$$

Hence, $\mathbb{F}$ is an integral domain. □

End of Lecture

Lecture 30: November 13th, 2024.

Theorem 6.2. *Let R be a finite integral domain. Then, R is a field.*

Proof. Let $a \in R, a \neq 0_R$ and $f : R \to R$ be the function $x \mapsto ax$. We will show that f is injective. Suppose that $x, y \in R : f(x) = f(y)$. Then, $ax = ay \implies ax - ay = 0_R \implies a(x - y) = 0_R \implies x - y = 0_R$ since $a \neq 0_R$. R is an integral domain, hence $x = y$ and f is injective. $f : R \to R$ is injective while R is finite hence f is surjective therefore, $\exists x_0 \in R : f(x_0) = 1_R \implies ax_0 = 1_R$. Hence a has a multiplicative inverse in $R \implies R$ is a field. □

Corollary 6.1. *Let p be a prime number, $\mathbb{Z}/p\mathbb{Z}$ is a field.*

6.3 Unit in a Ring

Definition 6.6. Let R be a ring. An element $a \in R$ is said to be a **unit** in R if $\exists b \in R : ab = ba = 1_R$. The set of units in R is denoted as $R^{\times}$.

Proposition 6.5. $(R^\times, \times)$ *is a group (under multiplication).*

Proof. First, let $x, y \in R^\times$. Then,

$$\begin{aligned} x \in R^\times &\implies \exists x' \in R^\times : xx' = x'x = 1_R \\ y \in R^\times &\implies \exists y' \in R^\times : y' = y'y = 1_R \end{aligned}$$

We also have

$$\begin{aligned} (xy)(y'x') = x(yy')x' = x1_Rx' = xx' = 1_R \\ (y'x')(xy) = y'(x'x)y = y'1_Ry = y'y = 1_R \end{aligned}$$

$1_R \in R^\times$ since $1_R \cdot 1_R = 1_R$. Associativity follows from properties of $\times$. $x' \in R$ since $xx' = x'x = 1_R$. Thus, $(R^\times, \times)$ is a group. □

Corollary 6.2. *Let R be a commutative ring.* $(R^\times, \times)$ *is an abelian group.*

Proposition 6.6. *Let R be a commutative ring. Then, any non-zero element is either a unit or a zero divisor.*

Proof. Let $a \in R$ and $a \neq 0_R$. If a is not a zero-divisor, we'll show that a is a unit. Let $f : R \to R, x \mapsto ax$. We'll prove that it's bijective:

- Injectivity: If $f(x) = f(y)$ for some $x, y \in R$. Then, $ax = ay \implies a(x - y) = 0_R$. Since a is not a zero divisor, $x - y = 0_R \implies x = y$.
- Surjectivity: R is finite and f is injective hence f is surjective.

Since f is surjective, $\exists x_0 \in R : f(x_0) = 1_r \implies ax_0 = 1_R \implies a$ is a unit. □

Example 6.3.1. Let $n \geq 2$. Then, $(\mathbb{Z}/n\mathbb{Z})^\times = U(n)$ where $U(n) = \{[a]_n; \gcd(a, n) = 1\}$.

Proof. Let $a \in \mathbb{Z} : \gcd(a, n) = 1, [a]_n \in U(n)$. Then, $\exists u, v \in \mathbb{Z} : au + nv = 1 \implies au \equiv 1 \mod n$. So, $[a]_n[u]_n = [1]_n$ so $a \in (\mathbb{Z}/n\mathbb{Z})^\times \implies U(n) \subseteq (\mathbb{Z}/n\mathbb{Z})^\times$.
Suppose $[a]_n \in (\mathbb{Z}/n\mathbb{Z})^\times$. Then, $\exists [b]_n : [ab]_n = [1]_n \implies \exists k \in \mathbb{Z} : ab = 1 + kn \implies ab - kn = 1$. Hence, $\gcd(a, n) \mid 1 \implies \gcd(a, n) = 1$. So $[a]_n \in U(n)$.
Hence, $(\mathbb{Z}/n\mathbb{Z})^\times = U(n)$. □

Proposition 6.7. *A unit is never a zero divisor.*

Proof. Suppose a is a unit and let b be such that $ab = 0_R$. Let $u : au = 1_R$. Then, $uab = u0_R = 0_R \implies b = 0_R$. □

6.4 Complex Numbers

Definition 6.7. Let i be such that $i^2 = -1$. Then, a **complex number** is an element of the form

$$x + iy \qquad \text{where } x, y \in \mathbb{R} \tag{6.1}$$

Proposition 6.8.

$(x + iy) + (x' + iy') = (x + x') + i(y + y')$

$(x + iy) \times (x' + iy') = (xx' - yy') + i(x'y + y'x)$

Example 6.4.1. $(2 + 3i)(7 + 5i) =?$

$$\begin{aligned}(2+3i)(7+5i) &= 14 + 10i + 21i + 15i^2 \\ &= 14 + 31i - 15 \\ &= -1 + 31i\end{aligned}$$

End of Lecture

Lecture 31: November 15th, 2024.

Definition 6.8. Define the set, $\mathbb{C}$ of complex numbers such that

$$\mathbb{C} = \{x + iy : x, y \in \mathbb{R}, i^2 = -1\} \tag{6.2}$$

Proposition 6.9. *$\mathbb{C}$ is a field*

Definition 6.9. Let R and S be rings. Then, $R \times S$ is a **ring** with operations:

$$\begin{aligned}(r,s) + (r',s') &= (r+s, r'+s') \\ (r,s) \cdot (r',s') &= (r \times_R s, r' \times_R s')\end{aligned}$$

and $(0_R, 0_R)$ is the neutral element for $+$ and $(1_R, 1_R)$ is the neutral element for $\times$.

Proposition 6.10. *$R \times S$ is not an integral domain*

Proof. $(1_R, 0_R) \times (0_R, 1_R) = (0_R, 0_R)$. □

6.5 Ideals

Definition 6.10. Let R be a commutative ring. A non-empty subset I of R is called an **ideal** if

1. $(I, +)$ is a subgroup of $(R, +)$.
2. $r \in R$ and $a \in I \implies ra \in I$.

6.5.1 Ideals of $\mathbb{Z}$

Lemma 6.1. *Consider the followings:*

1. *$n\mathbb{Z}$ is an ideal of $\mathbb{Z}$ for any $n \in \mathbb{N} \cup \{0\}$.*
2. *If I is an ideal of $\mathbb{Z}$. Then, $I = n\mathbb{Z}$ for some $n \in \mathbb{N} \cup \{0\}$.*

Proof. 1) Let $n \in \mathbb{N} \cup \{0\}$. Then, $n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$ ($n = 0, n\mathbb{Z} = \{0\}, n = 1 \implies n\mathbb{Z} = \mathbb{Z}$). Let $r \in \mathbb{Z}$ and $a \in n\mathbb{Z}$, then $a = nq$ for some $q \in \mathbb{Z}$ and $ra = rnq = n(qr)$ where $qr \in \mathbb{Z}$ so $ra \in n\mathbb{Z}$. Hence, $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$.
2) Let I be an ideal in $\mathbb{Z}$. Then I is a subgroup of $\mathbb{Z}$. Hence $I = n\mathbb{Z}$ for some $n \in \mathbb{N} \cup \{0\}$. (See HW5 and Sessions 1). □

Note: $\{0_R\}$ is always an ideal of R and R is always an ideal of R.

Proposition 6.11. *Let R be a commutative ring. R is a field $\iff$ The only ideals of R are $\{0_R\}$ and R.*

Proof. ($\implies$) Suppose that R is a field and let I be a non-zero ideal of R. Then, $\exists a \in R, a \neq 0_R : a \in I$. Let $b \in R : ab = 1_R$ (R is a field , $a \neq 0_R$). Now, $b \in R$ and $a \in I \implies ab \in I \implies 1_R \in I$. Let $r \in R, r = r1_R \in I$. Then, $R \subseteq I \subseteq R \implies R = I$.
($\impliedby$) Suppose that the only ideals of R are $\{0_R\}$ and R. Let $a \in R : a \neq 0_R$. Let $I = \{ar, r \in R\}$. Then, I is an ideal of R. $0_R \in I$ since $0_R = 0_R \cdot a$. If $x, y \in I$, then $x = r_1 a$ and $y = r_2 a$ for some $r_1, r_2 \in R$. Then, $x + y = r_1 a + r_2 a = a(r_1 + r_2) \implies (x + y \in I)$. $-x \in I$ since $-x = (-r_1)a$. So $(I, +) < (R, +)$.

Now, if $r \in R, rx = \overbrace{rr_1}^{\in R} a$ hence $rx \in I$. So I is an ideal of R. $I \neq \{0_R\}$ since $a \in I \implies I = R$ by assumption. Hence, $1_R \in I, \exists r_0 \in R : r_0 a = 1_R \iff ar_0 = 1_R$ (since R is commutative). So R is a field since every non-zero element is invertible. □

6.5.2 Quotient Rings

Let R be a commutative ring and I be an ideal of R. Define the following relation on R: We say $x \sim_I y$ iff $x - y \in I$, we write ($x \equiv y \bmod I$). $\sim_I$ is an equivalence relation since, $(I, +) < (R, +)$.

Now, the equivalence class of $x \in R$ is the coset $x + I$ and $x + I = y + I \iff x - y \in I$. This is denoted by R/I, the set of left cosets of I. Additionally, R/I is a ring under the following operations:

- $(r_1 + I) + (r_2 + I) = (r_1 + r_2) + I$

- $(r_1 + I) \times (r_2 + I) = (r_1 r_2) + I$

$+$ on R/I is well-defined since $(I,+)$ is a normal subgroup of $(R,+)$.

Claim: × is well-defined

Proof. Suppose that $r_1 \equiv r_1' \bmod I$ and $r_2 \equiv r_2' \bmod I$. We need to show that $r_1 r_2 - r_1' r_2' \in I$ i.e. $r_1 r_2 \equiv r_1' r_2' \bmod I$. Notice that

$$\begin{aligned} r_1 &= r_1' + k \text{ for some } k \in I \\ r_2 &= r_2' + q \text{ for some } q \in I \\ \implies r_1 r_2 - r_1' r_2' &= (r_1' + k)(r_2' + q) - r_1' r_2' \\ &= r_1' r_2' + k r_2' + q r_1' + kq - r_1' r_2' \\ &= \underbrace{r_2' k}_{\in I} + \underbrace{r_1' q}_{\in I} + \underbrace{kq}_{\in I} \in I \end{aligned}$$

Hence $r_1 r_2 + I = r_1' r_2' + I \implies \times$ is well-defined. □

End of Lecture

Lecture 32: November 18th, 2024.

Notice that $(1_R + I)$ and $(0_R + I)$ are the neutral element under × and + respectively. Associativity of $+, \times$ and the distributive laws follow easily from properties of R.

Claim: R/I is a commutative ring.

Proof. Since $(r_1 + I) \cdot (r_2 + I) = r_1 r_2 + I = r_2 r_1 + I = (r_2 + I) \cdot (r_1 + I)$. □

Example 6.5.1. $R = \mathbb{Z}$, $I = n\mathbb{Z}$ fpr some $n \in \mathbb{N}$. Then,

$$\mathbb{Z}/I = \begin{cases} \mathbb{Z}, & n = 0 \\ \{0_R\} & n = 1 \\ \mathbb{Z}/n\mathbb{Z}, & n > 1 \end{cases}$$

Definition 6.11. The set of equivalence classes denoted by R/I (and its properties shown above) is called the **quotient ring**.

Definition 6.12. Let R be a ring. A subset S of R is said to be a **subring** of R if

1. $(R,+)$ is a subgroup of $(R,+)$.

2. $1_R \in S$

3. $a, b \in S \implies ab \in S$.

N.B. $S \subseteq R$ is a subring $\iff$ S is a ring on its own.

Example 6.5.2. $\mathbb{Z}$ is a subring of $\mathbb{Q}$, $\mathbb{Q}$ is a subring of $\mathbb{R}$ and $\mathbb{R}$ is a subring of $\mathbb{C}$.

6.6 Ring Homomorphisms

Definition 6.13. Let R and S be rings. A **ring homomorphism** is a function $\varphi : R \to S$ such that:

- $\varphi(r_1 +_R r_2) = \varphi(r_1) +_S \varphi(r_2)$
- $\varphi(r_1 \times_R r_2) = \varphi(r_1) \times_S \varphi(r_2)$
- $\varphi(1_R) = 1_S$

Proposition 6.12. *Let φ be a ring homomorphism from R to S. Then,*

1. $\varphi(0_R) = 0_S$.
2. $\varphi(-r) = -\varphi(r)$

Proof. Follows immediately from the definition. □

Definition 6.14. The **kernel** of a ring homomorphism $\varphi : R \to S$ is denoted by $\ker\varphi$ and is defined as:

$$\ker\varphi = \{r \in R : \varphi(r) = 0_S\} = \varphi^{-1}(\{0_S\}) \tag{6.3}$$

Proposition 6.13. *$\varphi : R \to S$ is an injective ring homomorphism iff* $\ker\varphi = \{0_R\}$.

Proof. Follows from the fact that $\varphi : R \to S$ is a group homomorphism. □

Proposition 6.14. *Let R be a commutative ring and $\varphi : R \to S$ be a ring homomorphism. Then,* $\ker\varphi$ *is an ideal in R.*

Proof. $\ker\varphi < (R, +)$. Let $r \in R, x \in \ker\varphi$. Then, $\varphi(r \times_R a) = \varphi(r) \times_S \varphi(a) = \varphi(r) \times_S 0_S = 0_S \implies ra \in \ker\varphi$. □

Definition 6.15. A ring homomorphism $\varphi : R \to S$ is said to be an **isomorphism** of rings if it is bijective. In such case, we also say R and S are *isomorphic*, notated as: $R \cong S$.

Remark 6.5. *Being isomorphic is an equivalence relation on rings. Additionally, any ideals I of a commutative ring R is the kernel of a ring homomorphism.*

Theorem 6.3. ***(First Isomorphism for Ring).*** *Let R be a commutative ring and $\varphi : R \to S$ be a surjective group homomorphism. Then, $R/\ker\varphi \cong S$. ($S = \varphi(R)$)*

Proof. Let $I = \ker\phi$, define $\overline{\varphi} : R/I \to S = \varphi(R),\ r + I \mapsto \varphi(r)$. $\overline{\varphi}$ is a well-defined and bijective function and is a group homomorphism from R/I to S. All we have to check are:

1. $\overline{\varphi}(1_R + I) = \varphi(1_R) = 1_S$.

2. $\overline{\varphi}((r_1 + I)(r_2 + I)) = \overline{\phi}(r_1 + I)\overline{\phi}(r_2 + I)$

Then, $\overline{\varphi} : R/I \to S$ is a bijective homomorphism of rings, and thus $R/I = R/\ker\varphi \cong S$. □

Example 6.6.1. Show that there exists no ring homomorphism from $\mathbb{Q}$ to $\mathbb{Z}$.

Proof. If $\varphi : \mathbb{Q} \to \mathbb{Z}$ os a ring homomorphism. Then, $\varphi(2(1/2)-1) = \varphi(0) = 0$. Then, $\varphi(2)\varphi(1/2) - \varphi(1) = 0 \implies 2\varphi(1/2) - 1 = 0$, now $\varphi(1/2) \in \mathbb{Z}$ by definition $\implies 2\varphi(1/2) \neq 1$. Thus, there's no ring homomorphism from $\mathbb{Q} \to \mathbb{Z}$. □

Example 6.6.2. Is there a ring homomorphism from $\mathbb{C}$ to $\mathbb{R}$? Well...if $\varphi : \mathbb{C} \to \mathbb{R}$ is a ring homomorphism. Then, $\varphi(-1) = -1 \implies \varphi(i^2) = -1 \implies \varphi(i)\varphi(i) = -1$ however, there's no such real number $r : r^2 = -1$. Thus, there's no ring homomorphism from $\mathbb{C}$ to $\mathbb{R}$.

End of Lecture ———

Theorem 6.4. *Let R and S be commutative rings and $\varphi : R \to S$ a ring homomorphism. Then,*

1. *$\varphi(R)$ is a subring of S.*

2. *If x is a unit in R. Then, $\varphi(x)$ is a unit in S.*

3. *If J is an ideal in S. Then, $\varphi^{-1}(J)$ is an ideal of R containing $\ker\varphi$.*

4. *If φ is surjective and I is an ideal of R. Then, $\varphi(I)$ is an ideal of S.*

5. *If φ is an isomorphism of rings. Then,*

Lecture 33: November 20$^{\text{th}}$, 2024.

- *R is a field $\iff$ S is a field.*
- *R is an integral domain $\iff$ S is an integral domain.*
- $(R^\times, \times_R) \cong (S^\times, \times_S)$ *and* $(R, \times_R) \cong (S, \times_S)$ *as groups*

Proof. Left as an exercise. □

Proposition 6.15. *Let R be a ring. Then, there exists a unique ring homomorphism $\phi : \mathbb{Z} \to R$, defined as:*

$$\phi(n) = n \cdot 1_R = \begin{cases} \underbrace{1_R + \cdots + 1_R}_{n \text{ times}} & \text{if } n > 0 \\ 0 & \text{if } n = 0 \\ \underbrace{-(1_R + \cdots + 1_R)}_{-n=|n| \text{ times}} & \text{if } n < 0 \end{cases} \tag{6.4}$$

Proof. The fact that ϕ is a ring homomorphism is left as an exercise. To prove uniqueness, if $\phi, \psi : \mathbb{Z} \to R$ is a ring homomorphism. Then, they're group homomorphism from $\mathbb{Z}$ to R satisfying $\phi(1) = \psi(1) = 1_R$. Since $\mathbb{Z}$ is cyclic and generated by 1, $\phi, \psi : \mathbb{Z} \to R$ are group homomorphisms and $\phi(1) = \psi(1)$ then $\phi(n) = \psi(n)\ \forall n \in \mathbb{Z} \implies \phi = \psi$ and thus it's unique. □

6.7 Characteristic of Ring

Definition 6.16. (Characteristic of a Ring). Let R be a ring and ϕ denote the unique ring homomorphism from $\mathbb{Z}$ to R. Then, $\ker\phi = n\mathbb{Z}$ for some $n \geq 2$ or $n = 0$.[1] The **characteristic** of R is the non-negative integer n ($n \neq 1$) such that $\ker\phi = n\mathbb{Z}$.[2]

Example 6.7.1. Consider the following examples:

1. Let $R = \mathbb{Z}$ and $\phi : \mathbb{Z} \to \mathbb{Z}$ be the unique ring homomorphism. Then, $\ker\phi = n$ and $\phi(n) = n \implies \mathbb{Z}$ has characteristic 0.

2. Let $R = \mathbb{Z}/7\mathbb{Z}$ and $\phi : \mathbb{Z} \to R$. Then, $1 \mapsto [1]_7$, $2 \mapsto [2]_7, \ldots, 7 \mapsto [7]_7 = [0]_7$. Then, $\mathbb{Z}/7\mathbb{Z}$ has characteristic 7.

3. Let $R = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ then, $\text{Char}(R) = 4$.

[1] Proof: $\ker\phi$ is an ideal of $\mathbb{Z}$ so there exists $n \in \mathbb{N} \cup \{0\} : \ker\phi = n\mathbb{Z}$. $1 \notin \ker\phi$ since $\phi(1) = 1_R \neq 0_R \implies \ker\phi \neq \mathbb{Z}$. So, $n \neq 1 \implies \ker\phi = \{0\}$ or $n\mathbb{Z}$ for some $n \geq 2$. □

[2] Though not mentioned, some texts denote the characteristic of R as $\text{Char}(R)$. We will use this for simplicity.

Proposition 6.16. *Let R be a ring of characteristic $n \geq 2$. Then, the additive order of 1_R in $(R,+)$ is n.*

Proof. First, note that if $\text{Char}(R) = n$. Then, $\underbrace{1_R + \cdots + 1_R}_{n \text{ times}} = n1_R$, so 1_R has finite order in $(R,+)$. If $m \in \mathbb{N} : m \cdot 1_R = 0_R \implies \phi(m) = 0_R \implies m \in \ker\phi = n\mathbb{Z}$ and hence n divides m. Hence, the order of 1_R in $(R,+)$ is n. □

Proposition 6.17. *Let R be a ring where 1 has finite order $n \geq 2$. Then,* $\text{Char}(R) = n$.

Proof. Obvious. □

Proposition 6.18. *Let p be a prime number and R a ring with p elements. Then, $R \cong \mathbb{Z}/p\mathbb{Z}$ (and R is a field).*

Proof. Consider 1_R in $(R,+)$. $|R| = p$ so the order of 1_R in $(R,+)$ divides $|R| = p$, but $1_R \neq 0_R$ so 1_R has order p since p is prime. Let ϕ denote the unique ring homomorphism from $\mathbb{Z}$ to R. By the previous proposition (6.17), $\ker\phi = p\mathbb{Z}$. By the first isomorphism theorem for ring, $\mathbb{Z}/\ker\phi$ is isomorphic to a subring of R. Since $|\mathbb{Z}/p\mathbb{Z}| = p$ and $|R| = p \implies \mathbb{Z}/p\mathbb{Z} \cong R$. □

Notation: We denote the "field with p elements" as $\mathbb{F}_p$ i.e. you can assume $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Remark 6.6. *A subring of an integral domain is an integral domain.*

Theorem 6.5. *Let $\mathbb{F}$ be a finite field and let $\phi : \mathbb{Z} \to \mathbb{F}$ denote the unique ring homomorphism. Then,* $\ker\phi = p\mathbb{Z}$ *for some prime number p.*

Proof. $\phi : \mathbb{Z} \to \mathbb{F}$ is the unique ring homomorphism from $\mathbb{Z}$ to $\mathbb{F}$. We know that $\ker\phi = n\mathbb{Z}$ for some $n \geq 2$ or $n = 0$. By the first isomorphism theorem for rings, $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to a subring of $\mathbb{F}$. Since $\mathbb{F}$ is a finite field hence $\mathbb{Z}/n\mathbb{Z}$ is a finite integral domain. Hence $\mathbb{Z}/n\mathbb{Z}$ is a field and thus $n = p$ for some prime number p. □

End of Lecture ——

Proposition 6.19. *Let $n \geq 2$ and let R be a ring.* $\text{Char}(R) = n \iff 1_R$ *has order n in $(R,+)$.*

(This follows from proposition 6.16 and 6.17)

Proposition 6.20. *Let R be a ring with* $\text{Char}(R) = n \geq 2$ *and let $x \in R$. The order of x in $(R,+)$ divides n*

Lecture 34: November 22nd, 2024.

Proof. $n \cdot x = \overbrace{x + \cdots + x}^{n \text{ times}} = x\overbrace{(1_R + \cdots + 1_R)}^{n \text{ times}} = x \cdot 0_R = 0_R$ (by previous proposition). □

Proposition 6.21. *Let p be a prime number and R a finite ring with* $\mathrm{Char}(R) = p$*. Then $|R| = p^m$ for some $m \in \mathbb{N}$.*

Proof. By proposition 6.20, let $x \in R$ and $x \neq 0_R$. Then, x has order dividing p in $(R,+)$. Since p is prime and $x \neq 0_R$ then x has order p in $(R,+)$. Suppose that q is a prime dividing $|R|$. Then, by Cauchy's theorem, $\exists y \neq 0_R$ in R such that the order of y in $(R,+)$ is q. And since any non-zero element has order p in $(R,+)$ then $p = q \implies$ the only prime dividing $|R|$ is $p \implies |R| = p^m$ for some $m \in \mathbb{N}$ where $m > 0$ since $|R| \geq 2$. □

6.7.1 Chinese Remainder Theorem For Rings

Theorem 6.6. ***(Chinese Remainder For Rings).*** *Let $m, n \geq 2$ and* $\gcd(m,n) = 1$*. Then, $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$*

Proof. Let $\phi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ denote the unique ring homomorphism from $\mathbb{Z}$ to $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. The order of $([1]_n, [1]_m)$ in $(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}, +)$ is $\mathrm{lcm}(m,n) = \frac{mn}{\gcd(m,n)} = mn \geq 2$. Hence $\ker\phi = mn\mathbb{Z}$. By the first isomorphism theorem for rings, $\mathbb{Z}/\ker\phi = \mathbb{Z}/mn\mathbb{Z}$ is isomorphic to a subring of $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. Hence, $\phi(\mathbb{Z})$ is a subring of $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ and $|\phi(\mathbb{Z})| = mn = |\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}|$ hence ϕ is surjective so $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ as rings. □

Remark 6.7. *If* $\gcd(m,n) \neq 1$ *then $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ is not isomorphic to $\mathbb{Z}/mn\mathbb{Z}$ as groups. Hence, $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ as rings iff* $\gcd(m,n) = 1$.

End of Lecture —

Exercises. Let R be a ring. Then, $\mathrm{Char}(R) = 0 \iff 1_R$ does not have a finite order in $(R,+)$

Proposition 6.22. *Let R be a ring with* $\mathrm{Char}(R) = n \geq 2$*. Then, $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to a subring of R.*

Proposition 6.23. *Let R be an integral domain. Then,* $\mathrm{Char}(R) = 0$ *or prime number.*

Proposition 6.24. *Let $\mathbb{F}$ be a finite field. Then $|\mathbb{F}| = p^m$ for some prime p and for some $m \in \mathbb{N}$.*

Lecture 35: November 25th, 2024.

Proof. Let ϕ be the unique homomorphism from $\mathbb{Z}$ to $\mathbb{F}$. We've seen before that $\ker\phi = p\mathbb{Z}$ for some prime p. Hence, $\mathbb{F}$ is a finite ring with $\mathrm{Char}(\mathbb{F}) = p$ and thus $|\mathbb{F}| = p^m$ for some $m \in \mathbb{N}$ □

6.8 Rings of Polynomials

Definition 6.17. Let R be a commutative ring. The **ring of polynomials** $R[x]$ is defined by

$$R[x] = \{a_n x^n + \cdots + a_1 x + a_0, n \in \mathbb{N} \cup \{0\} \text{ and } a_n, \ldots, a_0 \in \mathbb{R}\} \tag{6.5}$$

x is called the **indeterminate** and $a_n, \ldots, a_0$ are called the coefficients.

Definition 6.18. We defined the sum of two polynomials as:

$$\begin{aligned}&(a_n x^n + \cdots + a_1 x + a_0) + (b_m x^m + \cdots + b_1 x + b_0)\\ &= a_n x + \cdots + (a_m + b_m)x^m + \cdots + (a_1 + b_1)x + (a_0 + b_0)\end{aligned}$$

for $n \geq m$. Their multiplication as:

$$\begin{aligned}&(a_n x^n + \cdots + a_1 x + a_0) \cdot (b_m x^m + \cdots + b_1 x + b_0)\\ &= c_{n+m} x^{n+m} + \cdots + c_1 x + c_0\end{aligned}$$

where $c_i = a_0 b_i + a_1 b_{i-1} + \cdots + a_i b_0$. In c_i, some a_i or b_i may not be defined. We consider these as 0.

Proposition 6.25. *$R[x]$ is a ring under the above operations.*

Proof. Left as an exercise. □

6.8.1 Degree of a Polynomial

Definition 6.19. Let R be a commutative ring and $f(x) \in R[x]$. Then, the **degree** of $f(x)$ is defined as

$$\deg f(x) = \begin{cases} -\infty & \text{if } f(x) = 0 \\ \max\{n \in \mathbb{N} \cup \{0\} : a_n \neq 0\} & \text{otherwise} \end{cases} \tag{6.6}$$

Proposition 6.26. *If R is an integral domain, then so is $R[x]$. If $f(x), g(x) \in R[x]$ and are non-zero, then* $\deg(f(x)g(x)) = \deg f(x) + \deg g(x)$.

Proof. Let $f(x)$ have degree $m \geq 0$ and $g(x)$ has degree $n \geq 0$. Let $f(x) = a_m x^m + \cdots + a_0$ and $g(x) = b_n x^n + \cdots + b_n$ where $a_m, b_n \neq 0$. Then, $f(x)g(x) = a_m b_n x^{m+n} +$ some lower order/degree term. Since, R is an integral domain, $a_m \neq 0$ and $b_n \neq 0$ so $a_m b_n \neq 0$. Thus, $\deg(f(x)g(x)) = m + n = \deg f(x) + \deg g(x)$. Hence if $f(x), g(x)$ are non-zero then $f(x)g(x)$ is also non-zero. □

End of Lecture

Remark 6.8. *If R is not an integral domain, then $R[x]$ is not an integral domain.*

Example 6.8.1. Let $R = \mathbb{Z}/4\mathbb{Z}$ and $2x + 1 \in R[x]$. Then,

$$(2x+1)(2x+1) = 4x^2 + 4x + 1 = 1$$

Then, $\deg f(x) f(x) = \deg f(x) + \deg f(x)$ does not hold necessarily if R is not an integral domain.

Lecture 36: November 27th, 2024.

6.9 Ideal Quotient and Principal

Definition 6.20. Let I be an ideal in R. We say that I is a **principal ideal** if $\exists a \in R : I = (a) = Ra.$ [3]

Definition 6.21. Let $a \in R$. Then, the set $(a) = \{ra : r \in R\} = Ra$ is called the **ideal quotient** by a on the *principal ideal.*

Definition 6.22. Let $a_1, \ldots, a_n \in R$. Then, the set $(a_1, \ldots, a_n) = \{r_1 a_1 + r_2 a_2 + \cdots + r_n a_n : r_1, \ldots, r_n \in R\}$ is an ideal, in particular, it's called the **ideal quotient generated by** $a_1, \ldots, a_n$.

Definition 6.23. An integral domain R where every ideal is principal is called a **principal ideal domain (PID)**.

Example 6.9.1. $\mathbb{Z}$ is a PID. Though, not every ring is a PID such as $\mathbb{Z}[x], I = (2, x) = \{2f(x) + xg(x) : f, g \in \mathbb{Z}\}$. $\mathbb{Z}[\sqrt{5}] = \{a + b\sqrt{5} : a, b \in \mathbb{Z}\}$ has ideal $I = (2, 1 + \sqrt{5})$ is not principal.

Definition 6.24. Let R be a commutative ring. We say that a and b are **associated** if $\exists u \in R : a = ub$ and u is a unit in R.

[3] If an ideal is a principal ideal, we simply call it principal.

Proposition 6.27. *Being associated is an equivalence relation i.e. $a \sim b$ if $\exists u \in R^\times : a = ub$ is an equivalence relation.*

Proof. Left as an exercise. □

Definition 6.25. If R is a commutative ring and $a = 0_R$. We say *a divides b* if $b = ac$ for some $c \in R$. This is denoted as $a \mid b$.

Proposition 6.28. *If $a \neq 0_R$, $a \mid b$ and $a \mid d \implies a \mid b + d$. Similarly, if $a \neq 0_R$ and $a \mid b \implies a \mid bd \; \forall d \in R$.*

Proof. Left as an exercise. □

Proposition 6.29. *Let $\mathbb{F}$ be a field, $\mathbb{F}[x]$ is a ring of polynomial with coefficient in $\mathbb{F}$. Then, units of $\mathbb{F}[x]$ are the elements of $\mathbb{F}^\times = \mathbb{F} \setminus \{0_\mathbb{F}\}$ (or $\mathbb{F} - \{0_\mathbb{F}\}$).*

Proof. Let a be a unit and $a \neq 0_\mathbb{F} \implies \exists b \in \mathbb{F} : ab = 1\mathbb{F}$ so a is a unit in $\mathbb{F} \subseteq \mathbb{F}[x]$.
Now, Let $f(x) \in \mathbb{F}[x]$ where $\deg f(x) \geq 1$, and suppose $f(x)$ is a unit $\implies \exists g(x) \in \mathbb{F}[x] : f(x)g(x) = 1$. Then, $g(x) \neq 0 \implies \deg f(x)g(x) = 0$. We also know that $\mathbb{F}$ is a field, thus $\deg f(x)g(x) \geq \deg f(x) + \deg g(x) \geq 1$. This is a contradiction. Thus, $\deg f(x) \implies f(x)$ is not a unit and $0_\mathbb{F}$ is not a unit $\implies$ the units of $\mathbb{F}[x]$ are the constant non-zero polynomials i.e. $\mathbb{F} - \{0_\mathbb{F}\}$. □

Example 6.9.2. For $\mathbb{Z}/4\mathbb{Z}[x], 2x+1$ is a unit since $(2x+1)^2 = 4x^2 + 4x + 1 = 1$. Similarly, $(2x+3)^2 = 4x^2 + 12x + 9 = 1$.

6.10 Division Algorithm

Definition 6.26. Let $\mathbb{F}$ be a field and $\mathbb{F}[x]$ be the ring of polynomials with coefficients in $\mathbb{F}$. Then, a non-zero polynomial $f(x) \in \mathbb{F}[x]$ is **monic** if the coefficient of its highest degree term is 1

Example 6.10.1. In $\mathbb{F}_3[x]$, $2x^2 + x + 1$ is not monic.

Theorem 6.7. ***(Division Algorithm).*** *Let $f(x), g(x) \in \mathbb{F}[x]$ and $g(x) \neq 0$. Then, $\exists! q(x), r(x) : f(x) = q(x)g(x) + r(x)$ with $\deg r(x) < \deg g(x)$*

Theorem 6.8. ***(GCD of Polynomials).*** *Let $f, g \in \mathbb{F}[x]$. Then, the $\gcd(f, g)$ is the monic polynomial of largest degree that divides both f and g. Such polynomial exists and is unique, moreover, $\exists u, v \in \mathbb{F}[x] : \gcd(f, g) = uf + vg$.*

Proof. (Division Algorithm). Let $f, g \in \mathbb{F}[x]$ and $g \neq 0$. Let $S = \{f(x) - k(x)g(x) : k(x) \in \mathbb{F}[x]\} \implies$ if $0 \in S$ then $\exists q(x) : f(x)q(x) \implies r(x) = 0$. If $0 \notin S \implies$ takes a polynomial of minimal degree $r(x) \in S$. Then, show that $\deg r(x) < \deg g(x)$ and uniqueness (exercise.) □

End of Lecture

6.11 Irreducible Polynomials

Lecture 37: November 29th, 2024.

Definition 6.27. Let $\mathbb{F}$ be a field, $\mathbb{F}[x]$ is a ring of polynomial with coefficient in $\mathbb{F}$. Let $f(x)$ be a polynomial in $\mathbb{F}[x]$. We say that $\alpha \in \mathbb{F}$ is a **root** of $f(x)$ if $f(\alpha) = 0$

Proposition 6.30. *Let $f(x) \in \mathbb{F}[x]$ α is a root of $f(x) \iff x - \alpha \mid f(x)$.*

Proof. ($\implies$) Suppose α is a root of $f(x)$. Then, $f(\alpha) = 0$. Write $f(x)$ as $f(x) = q(x)(x-\alpha) + r(x)$ where $r(x) = 0$ or $\deg r(x) < 1$. So, $f(x) = (x-\alpha)q(x) + r$ where $r \in \mathbb{F}$. Then, $f(\alpha) = (\alpha-\alpha)q(\alpha) + r \implies 0 = 0 + r \implies r = 0$. Thus, $f(x) = (x-\alpha)q(x)$ so $x - \alpha \mid f(x) \in \mathbb{F}[x]$.
($\impliedby$) Suppose that $x - \alpha \mid f(x)$ Then, $f(x) = (x-\alpha)q(x)$ for some $q(x) \in \mathbb{F}[x]$. Then, $f(\alpha) = (\alpha-\alpha)q(x) = 0$ so α is a root of $f(x)$. □

Definition 6.28. A non-constant polynomial $f(x) \in \mathbb{F}[x]$ is said to be **irreducible** in $\mathbb{F}[x]$ if $f(x)$ cannot be expressed as a product of 2 polynomials $g(x)$ and $h(x) \in \mathbb{F}[x]$ of strictly smaller degree than $f(x)$. i.e. if $f(x)$ is irreducible in $\mathbb{F}[x]$ and $f(x) = g(x)h(x)$, then $g(x)$ is a unit or $h(x)$ is a unit.

Example 6.11.1. Consider the following examples:

1. Let $a \neq 0$. Then, $f(x) = ax + b$ is irreducible in $\mathbb{F}[x]$.

   Proof. If $f(x) = g(x)h(x)$ for some $g(x), h(x) \in \mathbb{F}[x]$. Then, $\deg f = \deg g + \deg h$ (since $\mathbb{F}$ is a field). This means, $1 = \deg g + \deg h \implies$ either $\deg g = 0$ or $\deg h = 0 \implies$ either $g(x)$ is a unit or $h(x)$ is a unit. Thus, $f(x)$ is irreducible. □

2. Let $f(x) \in \mathbb{F}[x]$ with $\deg f = 3$. Then, $f(x)$ is irreducible in $\mathbb{F}[x] \iff f(x)$ has no roots.

   Proof. ($\implies$) Suppose that $f(x)$ has root α. Then, $f(x)$ is divisible by $x - \alpha$ and $f(x) = (\alpha - x)q(x)$ for some $q(x) \in \mathbb{F}[x]$ and f is not irreducible.
   ($\impliedby$) Suppose that f has no roots in $\mathbb{F}$ and let $h(x), g(x) \in \mathbb{F}[x]$: $f(x) = g(x)h(x)$. We have $\deg f(x) = 2 \implies \deg g = \deg h = 1$ or $\deg g = 0 \wedge \deg h = 2$ or $\deg g = 2 \wedge \deg h = 0$. But, if $\deg g = \deg h = 1 \implies f(x)$ has a root in $\mathbb{F}$. So, we must have that $\deg g = 0$ or $\deg g = 2$. Hence, $f(x)$ is irreducible in $\mathbb{F}[x]$. □

Theorem 6.9. [4]*Let $\mathbb{F}$ be a field and $f(x) \in \mathbb{F}[x]$ be a non-constant polynomial. Then, $\mathbb{F}[x]/(f(x))$ is a field $\iff$ $f(x)$ is irreducible in $\mathbb{F}[x]$.*

Example 6.11.2. Let $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ be the field with 2 elements. Let $f(x) = x^2+x+1$. Then, $f(1) = 1$ and $f(0) = 1$. Then, $\deg f(x) = 2$ and has no roots in the field $\mathbb{F}_2$. So, $f(x)$ is irreducible in $\mathbb{F}_2[x]$. Then, $\mathbb{F}_2[x]/(x^2+x+1)$ is a field. Write $f(x) = (x^2+x+1)q(x)+r(x)$ with $\deg r < 2$ and let $I = (x^2+x+1)$. Then, $f(x)+I = (x^2+x+1)q(x)+r(x) \implies f(x)+I = r(x)+I \implies (x^2+x+1)q(x) \in I$.

$$\mathbb{F}_2[x]/(x^2+x+1) = \{0+I, 1+I, x+I, x+1+I\}$$

e.g. $(x+I)(x+1+I) = x(x+1)+I = x^2+x+I = 1+I$. Notice too that $\text{Char}(\mathbb{F}_2[x]/(x^2+x+1)) = 2$.

Example 6.11.3. Construct a field with 25 element.
To do so, we first know that $25 = 5^2 \implies \deg f(x) = 2$. Then, let $f(x) = x^2+2$ in $\mathbb{F}_5[x]$. We will have residue in the form of $a+bx$ where you have 5 choices for a and b, each $\implies$ 25 elements. Thus, we construct the field $\mathbb{F}_5[x]/(x^2+2)$ which has 25 elements.

Example 6.11.4. Find a field with p^2 element where $p \equiv 3 \bmod 4$. Well...We know that x^2+1 will have no root in $\mathbb{F}_p$ (check subsection of 4.2.2 Isomorphism Theorem, frequently asked question). Thus, we can construct the field is $\mathbb{F}_p/(x^2+1)$ which will have p^2 elements.

End of Lecture ——

Lecture 38: December 2nd, 2024.

6.11.1 Finite Fields and Polynomials Rings

Proposition 6.31. *Let $\mathbb{F}$ be a field and let $g(x) \in \mathbb{F}[x]$ and suppose that $\deg g(x) \geq 1$. Then, for any $h(x) \in \mathbb{F}[x]$, $\exists! r(x) \in \mathbb{F}[x] : h(x)+I = r(x)+I$ where I is the ideal generated by $g(x)$ in $\mathbb{F}[x]$, and $\deg r(x) < \deg g(x)$ or $\deg r(x) = 0$.*

Proof. Write $h(x) = g(x)q(x)+r(x)$ where $\deg r(x) < \deg g(x)$, then $h(x)+I = g(x)q(x)+r(x)+I = r(x)+I$. Suppose that $r'(x) \in \mathbb{F}[x] : h(x)+I = r'(x)+I$ where $\deg r'(x) < \deg g(x)$ or $\deg r'(x) = 0$. Then, $r(x)+I = r'(x)+I$. Hence, $r(x)-r'(x) = I \implies r(x)-r'(x) \in (g(x)) \implies g(x) \mid r(x)-r'(x)$. Therefore, $\exists k(x) : g(x) = k(x)(r(x)-r'(x))$.
If $r(x)-r'(x) \neq 0$, then $k(x) \neq 0$, and since $\mathbb{F}$ is a field, $\deg(r-r') = \deg k + \deg g$ but $\deg(r-r') < \deg g$ which is a contradiction. Thus, $r(x) = r'(x)$. □

[4] IMPORTANT: This will be used in the final exam

Corollary 6.3. *Consider the followings:*

1. *If* $\mathbb{F}$ *is a field and* $g(x) \in \mathbb{F}[x]$ *with* $\deg g(x) = n \geq 1$. *Then,* $\mathbb{F}[x]/(g(x)) = \{a_0 x^{n-1} + \cdots + a_1 x + a_0 + I : a_n, \ldots, a_0 \in \mathbb{F}\}$

2. *If* $|\mathbb{F}| < \infty$. *Then,* $\mathbb{F}[x]/(g(x))$ *is finite and has size* $|\mathbb{F}|^n$.

Proof. (Theorem 6.9). ($\implies$) Suppose $f(x)$ is not irreducible. Then, $\exists h(x)$, $g(x) \in \mathbb{F}[x] : f(x) = g(x)h(x)$ and $1 \leq \deg g, \deg h < \deg f$. Let $I = (f(x))$, $f(x) + I = g(x)h(x) + I \implies 0 + I = (g(x) + I)(h(x) + I) \implies g(x) + I \neq 0 + I$ and $h(x) + I \neq 0 + I$. Then, $\mathbb{F}[x]/(f(x))$ is not an integral domain and hence not a field.
($\impliedby$) Suppose $f(x)$ is irreducible and let $g(x) \in \mathbb{F}[x] : g(x) \notin I = (f(x))$. So $f(x) \nmid g(x) \implies \gcd(f, g) \mid f(x)$ and since $f(x)$ is irreducible. Then, $\gcd(f, g) = 1$ or $f(x)$. Since $f(x) \nmid \gcd(f, g) \implies \gcd(f, g) = 1$. Hence, $\exists u(x), v(x) \in \mathbb{F}[x] : f(x)u(x) + g(x)v(x) = 1 \implies f(x)u(x) + g(x)v(x) + I = 1 + I \implies g(x)v(x) + I = 1 + I$ and thus $(g(x) + I)(v(x) + I) = 1$ so $g(x) + I$ has a multiplicative inverse in $\mathbb{F}[x]/(f(x)) \implies \mathbb{F}[x]/(f(x))$ is a field. □

Example 6.11.5. Construct a field with 8 elements. Let $\mathbb{F}_2$ be the field with 2 elements. Let $f(x) = x^3 + x^2 + 1$, $f(x)$ has no roots in $\mathbb{F}_2$ since $f(0) = 1, f(1) = 1$. Since $\deg f(x) = 3 \implies f(x)$ is irreducible in $\mathbb{F}[x]$ and hence $\mathbb{F}[x]/(f(x))$ is a field with $2^3 = 8$ elements.

Is $\mathbb{F}_2[x]/(x^3)$ isomorphic to $\mathbb{F}_2[x]/(x^3 + x^2 + 1)$? Well...no since x^3 is not irreducible in $\mathbb{F}_2[x]$ so $\mathbb{F}_2[x]/(x^3)$ is not a field and is thus not isomorphic to $\mathbb{F}_2[x]/(x^3 + x^2 + 1)$.

Example 6.11.6. Construct a field with 25 elements. Let $\mathbb{F}_5$ be a field with 5 element and $f(x) = x^2 - 3 = x^2 + 2 \in \mathbb{F}_5$ which has no root. Hence, since $\deg f(x) = 2$, it's irreducible in $\mathbb{F}_5[x]$. Then, $\mathbb{F}_5[x]/(x^2 + 2)$ is a field with 25 elements.

Example 6.11.7. Let $K = \mathbb{F}_5[x]/(x^2 + 2)$ and let $g(y) = y^{25} - y$. How many roots does $g(y)$ have in K? K is a field and so $K^\times = K - \{0\}$ is a group and thus $|K^\times| = 25 - 1 = 24$. By Lagrange's theorem, if $a \in K^\times$, $a^{24} = 1$ and $a^{25} = a$. So any $a \in K^\times$ is a root of $g(y)$ and $g(0) = 0$ hence any $x \in K$ is a root of g.

End of Lecture

Lecture 39: December 4th, 2024.

6.12 Prime Ideals and Chinese Remainder Theorem

Proposition 6.32. *Let $f(x) \in \mathbb{F}[x]$ with $\deg f(x) = n \geq 2$. Then, $f(x)$ has at most n roots in $\mathbb{F}$.*

Proof. If $f(x)$ has no roots then the result hold true. Suppose $f(x)$ has a root $\alpha \in \mathbb{F}$. Then, we can write $f(x) = (x-\alpha)k(x)$ for some $k(x) \in \mathbb{F}[x]$ where $\deg k(x)$ is $n-1$. We can proceed by inductive on n. If β is a root of $f(x)$ and $\beta \neq \alpha$. Then, $(\beta-\alpha)k(\beta) = 0$. Since $\beta - \alpha \neq 0$ and $\mathbb{F}$ is a field, $(\beta) = 0$ so β is a root of k. By induction, $k(x)$ has at most $n-1$ distinct roots so $f(x)$ has at most $n-1$ distinct roots □

Example 6.12.1. $\mathbb{Z}/6\mathbb{Z}$ where $f(x) = x^2 - x$. It has at most 2 roots.

Proposition 6.33. *Let $f(x) \in \mathbb{F}[x]$ be irreducible. Then, if $f(x) \mid a(x)b(x)$ where $a(x), b(x) \in \mathbb{F}[x]$. Then, $f(x) \mid a(x)$ or $f(x) \mid b(x)$*

Proof. Let $f(x)$ be irreducible and let $f(x)|a(x)b(x)$. If $f(x) \mid a(x)$, we're done. If $f(x) \nmid a(x)$, then $\gcd(f(x), a(x)) = 1$. Then, $\exists u(x), v(x) \in \mathbb{F}[x]$: $1 = f(x)u(x) + a(x)v(x) \implies b(x) = f(x)u(x)b(x) + a(x)v(x)b(x)$. Noticer that $k(x)f(x) = a(x)b(x)$ for some $k(x) \in \mathbb{F}[x]$. Then, $b(x) = f(x)(u(x)b(x) + k(x)v(x)) \implies f(x) \mid b(x)$. □

Theorem 6.10. *Let $f(x) \in \mathbb{F}[x]$ and $\deg f(x) = n \geq 1$. Then,*

1. *$f(x)$ has irreducible factor.*
2. *There exists monic irreducible polynomials $f_1(x), f_2(x), \ldots, f_l(x) \in \mathbb{F}[x]$ and positive integer $a_1, a_2, \ldots, a_l \in \mathbb{N}$ and $a \in \mathbb{F}^{\times}$ such that*

$$f(x) = af_1^{a_1}(x)f_2^{a_2}(x)\cdots f_l^{a_l}(x) \tag{6.7}$$

Moreover, if $g_1(x), \ldots, g_k(x)$ are monic irreducible polynomials in $\mathbb{F}[x]$ and $b_1, \ldots, b_k \in \mathbb{N}$ and $b \in \mathbb{F}^{\times}$ such that $f(x) = bg_2^{b_1}(x)g_2^{b_2}(x)\cdots g_k^{b_k}(x)$. Then, $k = l$ and $b = a$ and after arranging $g_i(x) = f_i(x)$ and $a_i = b_i$.

Proof. Left as an exercise. □

Theorem 6.11. *Let R be a commutative ring and let I be an ideal in R. Then,*

1. *$I \cap J$ is an ideal of R and $R/(I \cap J)$ is isomorphic to a subring of $R/I \times R/J$.*

2. *$I+J=\{a+b : a \in I, b \in J\}$ is an ideal of R and if $I \neq J = R$. Then, $R/(I \cap J) \cong R/I \times R/J$.*

Corollary 6.4. *Let $R=\mathbb{Z}$ and $\gcd(m,n)=1$ where $m,n \in \mathbb{N}$. Let $I=(m)$ and $J=(n), I+J=R$. Then, $I \cap J = (m) \cap (n) = (\operatorname{lcm}(m,n)) = (mn)$. Then, $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.*

Proof. 1. Let $f : R \to R/I \times R \times J, f(r) = (r+I, r+J)$. Then, f is a ring homomorphism since

$$f(1_R) = (1_R + I, 1_R + J)$$

$$\begin{aligned} f(r+r') &= ((r+r')+I, (r+r')+J) \\ &= ((r+I)+(r'+I), (r+J)+(r'+J)) \\ &= (r+I, r+J) + (r'+I, r'+J) = f(r)+f(r') \end{aligned}$$

$$\begin{aligned} f(rr') &= (rr'+I, rr'+J) \\ &= ((r+I)(r'+I), (r+J)(r'+J)) \\ &= (r+I, r+J)(r'+I, r'+J) = f(r)f(r') \end{aligned}$$

Its kernel is given as

$$\begin{aligned} \ker f &= \left\{ r \in R : f(r) = (0+I, 0+J) \right\} \\ &= \{ r \in R : r+I = I \text{ and } r+J = J \} \\ &= \{ r \in R : r \in I \text{ and } r \in J \} = I \cap J \end{aligned}$$

2. The proof that $I+J$ is an ideal is left as an exercise. If $I+J=R$, we'll show that f is surjective. First, if $I+J=R$, then $1_R \in I+J$ hence $\exists a \in I, b \in J : 1 = a+b$. Then,

$$f(a) = (a+I, a+J) = (I, 1-b+J) = (0+I, 1+J)$$

Similarly, $f(b) = (1+I, 0+J)$. Let $x, y \in R$. We'll find $r \in R : f(x) = (x+I, y+J)$. Let $r = bx+ay$ then $f(r) = (bx+ay+I, bx+ay+J) = (bx+I, ax+J)$ since $ay \in I$ and $bx \in J$. Then,

$$\begin{aligned} f(r) = (bx+I, ay+J) &= ((b+I)(x+I), (a+I)(y+I)) \\ &= ((1+I)(x+I), (1+J)(y+J)) = (x+I, y+J) \end{aligned}$$

Thus, f is surjective and hence $R/(I \cap J) \cong R/I \times R/J$. □

6.12.1 Prime Ideal

Definition 6.29. Let R be a commutative ring. An ideal $P \subsetneq R$ is said to be a **prime ideal** if the following holds: if $a, b \in R$ such that $ab \in P \implies a \in P$ or $b \in P$.

Proposition 6.34. *P is a prime ideal in R iff R/P is an integral domain.*

Proof. ($\implies$) Let P be a prime ideal. Let $x+P, y+P \in R/P$ be such that $(x+P)(y+P) = 0_R + P$, we'll show that $x+P = 0_R + P$ or $y+P = 0_R + P$. Now, $(x+P)(y+P) = xy + P = 0_R + P \implies xy \in P \implies x \in P$ or $y \in P \implies x+P = 0_R + P$ or $y+P = 0_R + P$ so R/P is an integral domain.
($\impliedby$) Left as a Christmas exercise. □

End of Lecture