Math #235 Notes

(Gautier) Cole Killian - 260910531

January 6, 2020

Contents

§1 Proof of $(A \cup B)' = A' \cap B'$

In order to prove $A = B$, prove that $A \subset B$ and $A \supset B$

§1.1 Proof of $(A \cup B)' \subset A' \cap B'$

$$\begin{aligned}\text{Proving that let } x \in (A \cup B)' \\ \to x \notin A \cup B \\ \to x \notin A \text{ and } \notin B \\ \to x \in A' \text{ and } x \in B' \\ \to x \in A' \cap B'\end{aligned}$$

§1.2 Proof of $(A \cup B)' \supset A' \cap B'$

$$\begin{aligned}\text{let } x \in A' \cap B' \\ \to x \in A \text{ and } x \in B' \\ \to x \notin A \text{ and } x \notin B \\ \to x \notin A \cup B \\ \to x \in (A \cup B)'\end{aligned}$$

§2 Product of Sets

$$\begin{aligned}A \times B = \{(a, b) : a \in A \text{ and } b \in B\} \\ \text{i.e. } A^n = A \times A \times A \ldots \\ \mathbb{R} = R \times R\end{aligned}$$

§3 Relations and Functions

A relation from A to B is a subset of $A \times B$

A map or funciton from A to B is a relation where $f \subset A \times B$ such that for each $a \in A$ there exists a unique $(a, b) \in f$

Notation: $f : A \to B$

Think of it as $f(a) = b$ instead of $(a, b) \in f$

A is domain of f, B is codomain or target of f

image of f is $f(A) = \{f(a) : a \in A\}$

Example: $f(A) = \{(1, y), (2, y), (3, y)\}$

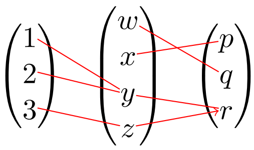
image $= f(A) = \{y, z\}$

Definition: $f : A \to B$ is subjective if $f(A) = B$

Definition: $f : A \to B$ is injective or one-to-one or "into" if there does not exist $a \in A$ and $b \in A$ such that $f(a) = f(b)$

§4 Composite Functions

$f : A \to B$
$g : B \to C$
Composition $g \circ f$ is a function. $g \circ f : A \to C$
$(g \circ f)(a) = g(f(a))$



$$g \circ f(1) = g(f(1)) = g(y) = r$$
$$g \circ f(2) = g(f(2)) = g(y) = r$$
$$g \circ f(3) = g(f(3)) = g(z) = r$$

Theorem 1.1.8: The quick brown fox jumps right over the lazy dog. the quick brown fox jumps right over the lazy dog. the quick brown fox jumps right over the lazy dog. the quick brown fox jumps right over the lazy dog. the quick brown fox jumps right over the lazy dog. the quick brown fox jumps right over the lazy dog. the quick brown fox jumps right over the lazy dog. the quick brown fox jumps right over the lazy dog.

§5 Lecture 2019-09-09

Theorem 5.1

Suppose $f : A \to B$ and $g : B \to C$ are surjective then $g \circ f : A \to C$ is surjective
Proof: $c \in C$
since $g : B \to C$ there exists $b \in B$ s.t. $g(b) = c$ since $f : A \to B$ is surjective, exists $a \in A$ s.t. $f(a) = b$
thus $(g \circ f)(a) = g(f(a)) = g(b) = c$

Definition 5.2. A function $g : b \to A$ is inverse to function $f : A \to B$ if:

$$f \circ g = 1_B$$
$$g \circ f = 1_A$$

$$A \to^f B \to^g C$$
$$A \to^f B \to^g A$$
$$g \circ f = 1_A$$

$$B \to^g A \to^f B$$
$$f \circ g = 1_B$$

Note 5.3. They say f and g are inverible, use notation f^-1 for inverse of f

Theorem 5.4
Let $f : A \to B$ be a map: f is invertible if and only if f is a bijection

$$P \Leftrightarrow Q$$
$$P \Leftarrow Q$$
$$P \Rightarrow Q$$

Proof that f is invertible means f is a bijection:

$$\text{let } g = f^{-1} \text{ f is surjective since for all } b \in B$$
$$\text{we have } \ f(g(b)) = f \circ g(b) = 1_B(b) = b$$

$$\text{f is injective since if } f(a_1) = f(a_2) \Rightarrow g(f(a_1)) = g(f(a_2))$$

injective: if $f(a_1) = f(a_2)$, then $a_1 = a_2$
Proof that f is a bijection means f is invertible define $f^{-1} : B \to A$ thus:
for each $b \in B$, there exists $a \in A$ s.t. $f(a) = b$ and a is unique with this property (by injectivity)
define $f^{-1}(b) = a$ then $f \circ f^{-1}(b) = f(f^{-1}(b)) = f(a) = b$ $f^{-1} \circ f(a) = f^{-1}(f(a)) = f^{-1}(b)$
so $f \circ f^{-1} = 1_B$

Definition 5.5 (Equivalence Relation)**.** Equivalence Relation on a set X is a relation $R \subset X \times X$

$$R \text{ is reflexive } (x, x) \in R \text{ for all } x \in X$$
$$\text{is symmetric } (x, y) \in R \to (y, x) \in R$$
$$\text{is transitive } (x, y) \in R \text{ and } (y, z) \in R \to (x, z) \in R$$

Note 5.6. Usually denote equiv relations by $x \sim y$ instead of $(x, y) \in R$

$$\text{or } x = y$$
$$x \equiv y$$

Definition 5.7. A partition of X is a collection of disjoint nonempty subsets of X whose union is X

Example 5.8
$\{X_k : k \in K\}$ $x_i \cap x_j = \varnothing$ for $i \neq j$
$\{1, 2, 3, 4, 5, 6, 7, 8, 9, 0\} = \{1, 4, 5\} \cup \{6\} \cup \{9\} \cap \{2, 3, 7, 9, 0\}$
$X = X_1 \cup X_2 \cup X_3 \cup X_4$

§5.1 Creating a partition

let x be a set with equivalence relation $\sim$ for $y \in X$, let $[y] = \{x \in X : x \sim y\}$
$[y]$ is the equivalence class represented by y

Theorem 5.9
Theorem 1.25: The equivalence classes of an equivalence relation ($\sim$) form a partition of X.

Proof:

$$1. \text{ each equiv class is nonempty since } \; y \in [y]$$
$$2. \text{ equiv classes are either disjoint or equal since if } \; y \in [a] \text{ and } y \in [b]$$
$$\text{then } \; [a] \subset [b] \text{ since } \; c \in [a] \Rightarrow c \sim a \Rightarrow^{transitivity} c \sim y \Rightarrow^{transitivity} c \sim b \Rightarrow c \in [b]$$
$$\text{similarly } [b] \subset [a]$$
$$3. X = \cup_{x \in X} [x]$$

Conversely, given a partition of X you can define an equivalence relation by declaring $x \sim y \Rightarrow x, y$ lie in the same part of the partition

Note 5.10. An equivalence relation is a disguised version of a partition

Definition 5.11. Definition: congruence modulo n equivalence relation on Z

$a \equiv_n b$ if n divides $(b - a)$ i.e. $b - a = mn$ for some $m \in Z$ do NOT use $(a \equiv b(modn)$
EX. $\equiv_2$ partition

$$\{, -4, -2, 0, 2, \cdot\}$$
$$\{, -3, -1, 1, 3, \cdot\}$$

Proof: $\equiv_n$ is equiv relation

$$1. a \equiv_n a \text{ since } n|(a - a)$$
$$2. (a \equiv_n b) \Rightarrow (b \equiv_n a) \text{ since } n|(b - a) \text{ then } n|(a - b)$$
$$3. a \equiv_n b \text{ and } b \equiv_n c \text{ then } a \equiv_n c$$

$n|(b - a)$ and $n|(c - b)$ so $n|(b - a) + (c - b)$

§6 Mathematical Induction

Suppose have sequence of statements: $S_1, S_2, \ldots \{S_n : n \in \mathbb{N}\}$
Principle of mathematical induction:
Suppose S_1 is true (base case)
Suppose $S_n \Rightarrow S_{n+1}$ for each n (the induction)
Then S_n is true for each $n \in \mathbb{N}$
ex. $\int_n = 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$
(base case) $S_1 : 1 = \frac{1(1+1)}{2}$
(induction) $S_n \Rightarrow S_{n+1}$
$S_n : 1 + 2 + \cdots + n = \frac{n(n+1)}{2}$
$+n + 1$
$S_n : 1 + 2 + \cdots + n + (n + 1) = \frac{n(n+1)}{2} + (n + 1)$

Theorem 6.1

For $a, b \in \mathbb{Z}$ with $a \neq 0$ say a divides b if $b = a \cdot k$ for some $k \in \mathbb{Z}$

in other words b is a multiple of a

notation: $a|b$

d is a common divisor of a and b if $d|a$ and $d|b$

Greatest common divisor if largest integer that is a common divisor. Denoted by gcd (a, b)

a, b are relatively prime if gcd $(a, b) = 1$

ex. gcd $(48, 40) = 8$

gcd $(49, 39) = 1$

Theorem 6.2

Theorem 2.10 - Let $a, b \in \mathbb{Z} : a, b \neq 0$

There exists $r, s \in \mathbb{Z}$ s.t. gcd $(a, b) = ra + sb$

Example 6.3

gcd $(12, 20) = 2 * 12 - 1 * 20$

gcd $(14, 20) = 3 * 14 - 2 * 20$

Proof. let $S = \{ma + nb : m, n \in \mathbb{Z}$ and $ma + nb > 0\}$

$S \neq 0$ since $a^2 + b^2 > 0$

by W.O.P (well ordering property), let $d = ra + sb$ be least element of S

Claim: gcd $(a, b) = d$

First show that $d|a$ and $d|b$

Second: if $d'|a$ and $d'|b$ then $d'|d$

□

Theorem 6.4

2.9 - Division Algorithm - Review

Theorem 6.5

Theorem There are infinitely many primes.

Proof: Argument by contradiction. Suppose finetly many primes - $P_1, P_2, \ldots, P_n$

let $p = p_1 p_2 p_3 \ldots p_n + 1$

$p > p_n$ which means that p is not prime

but every composite number has prime factor so $p = p_k r$ for some k

impossible!

$p_k r = p_k(p_1 \ldots p_{k+1} \ldots p_n) + 1$

which would require that $p_k|1$ but this is impossible □

Theorem 6.6

Theorem Fundametnal theorem of arithmetic

let $n \in \mathbb{Z}$ with $n > 1$ Then $n = p_1 p_2 \dots p_k$ is a product of primes

This product is unique in a certain sense that:

if $n = q_1 q_2 \dots q_l$, then $k = l$ and sequences are actually the same after reording them

ex. $2 * 2 * 3 * 3 * 3 * 5 * 5$

$5 * 2 * 3 * 2 * 5 * 3 * 3$

Why is this true?

two things going on: exist and unique

proof of existence:

Show by (strong) induction that for $n \geq 2$, $S_n =$ "n is a product of primes"

(base case) n = 2

2 is a product of primes. 2 = 2 ✓

((strong) induction): Either n+1 is prime, or $n + 1 = ab$ where $2 \leq a, b, \leq n$

by (strong) induction, $a = p_1 p_2 \dots p_k, b = q_1 q_2 \dots q_l$ where a and b are a product of primes. Therefore n+1 is a product of primes.

Proof of uniqueness. Note, new discussion, dosen't realte to previous proof

§6.1 Review proof of uniqueness

suppose $p_1 \dots p_k =$ n $= q_1 \dots q_l$

assume $p_1 \leq p_2 \leq \dots \leq p_k$ and $q_1 \leq q_2 \leq \dots \leq q_l$

assume $p_1 \leq q_1$

then $p_1 | n$ so $p_1 | q_k$ for some k

so $p_1 = q_k$ thus $p_1 \leq q_1 \leq q_k$

so $p_1 = q_1$

now $(p_2 \dots p_k) = (q_2 \dots q_l)$ by induction $k = l$ and the sequence are the same. n/p has a unique prime factorization and so

§6.2 Definition and example of Groups

a binary operation on a set G is a function $f : G \times G \to G$

math world is built out of binary operation: multiplication, subtraction, addition...

denote $f(a, b)$ by $a \circ b$ or $a \cdot b$ or ab

Def: a group $(G, \circ)$ is a set G with a binary operation $(a, b) \to a \cdot b \in G$ such that

(1) the operation is associative. i.e. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

Review: associative, communative...

(2) there exists an identity element $e \in G$ s.t. $e \cdot x = x = x \cdot e$ for all $x \in G$

(3) Each element $x \in G$ has an inverse $y \in G$ s.t. $x \cdot y = e$

x^{-1} Often denotes inverse

We are blessed with a group theorist :)

example

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

(1) $(a+b)+c = a+(b+c)$

(2) $e = 0, a+0 = a = 0+a$

(3) inverse of x denoted by $-x$

idea

$(G, \circ)$ is <u>commutative</u> or <u>abelian</u> if $a \circ b = b \circ a$ for all $a, b \in G$

examples of commutative groups

ex. $(\mathbb{Z}, \cdot)$, $\cdot =$ "times"/multiplication is NOT a group

(1) yes associative $(a * b) * c = a * (b * c)$

(2) has identity element $e = 1$

(3) BUT inverses don't always exist. $2^{-1} = ?$. No integer inverse of 2

On the other hand: $(\mathbb{Q}*, \cdot)$ is a commutative group. Note: $\mathbb{Q}* = \mathbb{Q} - \{0\}$

identity (better word for e) is 1

ex. $(\mathbb{Q}, +)$ is a commutative group.

inverse of $\frac{2}{3}$ is $-\frac{2}{3}$

definition: $(G, \circ)$ is a finite group if G is a finite set.

otherwise we call G an infinite group.

What is more important when talking about a group. G or $\circ$? The $\circ$, everything is built into the $\circ$. i.e. $G \times G \to^f G$ and $(a, b) \to a \circ b$.

$|G|$ represents the number of elements in G

Let us now get familiar with Finite cyclic group $\mathbb{Z}_n$

Let $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$

Define binary operation $a + b = c$ where $a + b \equiv_n c$ (called addition modulo n)

Turns out that this is a commutative group. $(\mathbb{Z}_n, +)$ is a commutative group.

ex. in $\mathbb{Z}_n$

$2+2=4$, $3+3=1$, $4+1=0$, $4+4=3$

Requirements:

(1) associative $\checkmark$

(2) 0 is the identity element

(3) Inverse exists. i.e. inverse of $3 = 2$, inverse of $4 = 1$, inverse of $1 = 4$

Starting discussions on wednesday with Cayley table

I'm not gonna be able to type this lmao

Grid like a multiplication table, but more general. "The Cayley table of a group". Summary of a binary operation.

§6.3 Proposition 3.21

Proposition 3.21: Let G be a group, let $a, b \in G$.

Then the equations $ax = b$ and $xa = b$ have unique solutions.

§6.3.1 Proof of existence:

Let $x = a^{-1}b$. This is a solution for the first equation. $a * a^{-1}b = b = b$ ✓

Let $x = ba^{-1}$. This is a solution for the second equation.

§6.3.2 Proof of uniqueness:

To do this we will show that two solutions are always the same. Suppose c and d are solutions to $ax = b$. Therefore $a * c = b$ and $a * d = b$.

Therefore $a * c = a * d \Rightarrow a^{-1} * a * c = a^{-1} * a * d \Rightarrow c = d$ ✓. This is the proof for the first equation; the same steps can be used for the second equation.

§6.4 Proposition 3.22

Let G be a group. $(ba = ca) \Rightarrow (b = c)$. $(ab = ac) \Rightarrow b = c$. The idea behind this is <u>left right</u> cancellation.

$ba = ca \Rightarrow baa^{-1} = caa^{-1} \Rightarrow b = c$

§6.5 Notation

$g^n = g \circ g \circ g \circ \cdots \circ g$ where the number of g equals n - 1

$g^0 = e$

$g^{-1} = g^{-1} \circ g^{-1} \circ \cdots \circ g^{-1}$ where the number of g equals n - 1

From this: $g^m \circ g^n = g^{m+n}$ and $(g^m)^n = g^{m*n}$

Careful: $(ab)^m \neq a^m b^n$. Not necessarily commutative so you can't pass them through one another. Review a conceptually understanding of this.

For commutative $(G, +)$

$-g$ is notation for inverse of g.

§6.6 3.3 a <u>subgroup</u> H of group G is a subset of G

st $(H, \circ)$ is itself a group.

§6.6.1 ex. of the above.

${}_3\mathbb{Z} = \{\dots, -9, -6, -3, 0, 3, 6, \dots\}$

Perform checks. every element has an inverse. Review the group requirements. Every element has inverse. There is a unique identity element. Associative.

ex. The trivial subgroup $\{e\} \subset G$

ex. $(\mathbb{C}^*, \circ)$. Let $H = \{1, -1, i, -i\}$

ex. $SL_2(R) \subset GL_2(R)$.

Subgroup of 2×2 real invertible matricies but this time determ inent must equal 1. This works because determ inent of inverse of matrix is multiplicative inverse of determ inent; which in this case is also 1.

ex. $SL_2(Z) \subset SL_2(R) \subset GL_2(R)$.

§6.7 Proposition 3.30: Criterian for subgroup

A subset $H \subset G$ of a group $(G, \circ)$ is a subgroup iff:

(1) $e \in H$

(2) $h_1, h_2 \in H \Rightarrow h_1 h_2, \in H$

3) $h \in H \Rightarrow h^{-1} \in H$

§6.7.1 Proof that being a group gives these requirements

(1) Let e' be identity element of H. Then $e' = e'e = ee' = e \Rightarrow e = e'$
(2) Holds because H is a group. We like to say: H is "closed under multiplication".
(3) Since H is a group, h must have an inverse.

§6.7.2 Proof that these requirements means it must be a subgroup

Conditions (1), (2), (3), and associativity $\Rightarrow$ H is a group using operation of G. Must be associative because G is associative so any subset of G is also associative.

§6.8 Proposition 3.31

H is a subgroup $\Leftrightarrow H \neq \varnothing$
Easy to understand that $g, h \in H \Rightarrow gh^{-1} \in H$
A little harder to see that $gh^{-1} \in H$
$H \neq \varnothing \Rightarrow \exists x \in H$

§7 Cyclic Groups

§7.1 Cyclic Subgroup

Let $g \in (G, \circ)$. Notation: $< g >= \{g^n : n \in \mathbb{Z}\}$
Let $g \in (G, +)$. Notation: $< g >= \{ng : n \in \mathbb{Z}\}$

§7.2 Examples

$5 \in \mathbb{Z}$. $< 5 >= \{\dots, -10, -5, 0, 5, \dots\}$
$2 \in \mathbb{Z}$. $< 2 >= \{\text{even integers}\}$
$5 \in \mathbb{Z}_{10}$. $< 5 >= \{0, 5\}$
$6 \in \mathbb{Z}_{10}$. $< 6 >= \{6, 2, 8, 4, 0\}$
$2 \in \mathbb{Z}_{10}$. $< 2 >= \{2, 4, 6, 8, 0\}$
$3 \in \mathbb{Z}_{10}$. $< 3 >= \{3, 6, 9, 2, 5, 8, 1, 4, 7, 0\}$
Note: $< 1 >=< 3 >=< 7 >=< 9 >= \mathbb{Z}_{10}$. These capture the whole group.

> Theorem 4.3 - Let G be a group. Let $x \in G$, then $< x >$ is a subgroup of G. Another way of thinking about it: $< x >$ is the smallest subgroup containing x.

Definition / Notation: $< x >$ is the cyclic subgroup generated by x. If $G =< x >$, then G is a cyclic group and x is a generator of G.
Detecting whether or not a subset is a subgroup.
Criteria
(0) Identity element.
(1) Inverse of each element is inside.
(2) Two elements inside, their product is inside.

§7.3 Proof

(0) $x^0 \in< x >$ so $e \in< x >$.
(1) If $g \in< x >$ then $g = x^m$ for some $m \in \mathbb{Z}$. $g^{-1} = x^{-m}$ because $x^{-m} * x^m = x^0 = e$. Therefore $g^{-1} \in< x >$
(2) Let $g, k \in< x >$, then $g = x^m$ and $k = x^n$ for some $m, n \in \mathbb{Z}$so $g \circ h = x^m \circ x^n = x^{m+n} \in< x >$.
Note: Finite groups are really complicated.

The order of x in G equals the smallest $n > 0$ such that $x^n = e$. If $x^n \neq e$ for all $n > 0$ we declare x in G to have infinite order.

Definition / Notation: $|x|$ represents the order of x.

§7.4 Examples

In $\mathbb{Z}_{10}$: $|5| = 2$, $|3| = 10$, $|0| = 1$

3 in $\mathbb{Z}$ has infinite order. All x in Z have infinite order except the identity element.

$2 \in \mathbb{R}^*$. $< 2 >= \{2^n : n \in \mathbb{Z}\} = \{\dots, \frac{1}{8}, \frac{1}{4}, \frac{1}{2}, 1, 2, \dots\}$. Infinite order.

Theorem 4.9 - Every cyclic group is abelian (commutative).

§7.5 Proof

Suppose G $= < x >$. For each $g, k \in G$ there exist $m, n \in \mathbb{Z}$ such that $g = x^m$ and $k = x^n$

$g \circ k = x^m * x^n = x^{m+n} = x^{n+m} = x^n + x^m = k \circ g$

§7.6 Practice

$\mathbb{Q}_8$. Quaternians. I'm not sure what the "8" is for.

$< i >= \{1, i, -1, -i\}$

$< -i >= \{1, -i, -1, i\}$

$< 1 >= \{1\}$

$< -1 >= \{-1, 1\}$

$< j >= \{1, j, -1, -j\}$

Note to self: Groups are not necessarily commutative, but cyclic groups are always commutative. Review: Abelian.

§7.7 The group of units modulo n

$U_n = \{m : 1 \leq m < n, \gcd(m, n) = 1\}$

Binary operation: Multiply elements of U_n by computing remainder of xy modulo n.

§7.8 Examples

$U_{10} = \{1, 3, 7, 9\}$

Cayley Table: Can't make the table fast enough. Notes: each element appears once per row.

Changin to U_{15} :

$U_{15} = \{1, 2, 4, 7, 8, 11, 13, 14\}$

$U_8 = \{1, 3, 5, 7\}$

$< 1 >= \{1\}$

$< 3 >= \{1, 3\}$

$< 5 >= \{1, 5\}$

$< 7 >= \{1, 7\}$

U_8 is not cyclic. It is commutative because the cayley table is symmetric across $y = -x$.

Remember: U_n is abelian because xy mod n equals yx mod n ((because multiplication in integers is commutative)).

$U_3 = \{1, 2\}$. Is it cyclic. Yes because $< 2 >$ generates it. $< 2 >= \{1, 2\}$

$U_4 = \{1, 3\} =< 3 >$

$U_5 = \{1, 2, 3, 4\} =< 2 >= \{1, 2, 4, 3\} = \{2^0, 2^1, 2^2, 2^3\}$

Theorem 7.1
Every subgroup of a cyclic group G is cyclic

§7.9 Proof

Let $G = \langle x \rangle$. Let $H \subset G$ be a subgroup.
Show that $H = \langle y \rangle$ for some y.
If $H = \{e\}$ then $H = \langle e \rangle$ ✓.
Wha t is H contains an element $g \neq e$
Let $S = \{n > 0 : x^n \in H\}$
$S \neq \varnothing$ because it at least must include (review this proof that $S \neq \varnothing$.
Next step:
By W.O.P, let m be the least element of S.
Claim: $H = \langle y \rangle$ where $y = x^m$
Proof of claim: Let $h \in H$ Show that $h \in \langle y \rangle$ which means $h = y^q$ for some q.
Since $h \in G = \langle x \rangle$, $h = x^a$ for some $a \in \mathbb{Z}$
By the division algorithm: $a = mq + r$ where $0 \leq r < m$
If $r = 0$ then $h = x^a = x^{mq} = x^{m^q} = y^q$ ✓
If $r > 0$ the $hy^{-q} = x^{mq+r}x^{m^{-q}} = x^{mq+r}x^{-mq} = x^r$, but this would contradict that m is least element of S because... i'm not sure why review this
Cor 4.11. Subgroups of $\mathbb{Z}$ are $\langle n \rangle = n\mathbb{Z}$ (notation)
Prop 4.12. Let G by cyclic of order n $\Rightarrow x^n = e$. Suppose $G = \langle x \rangle$. This means that $(x^k = e) \Leftrightarrow n|k$.
Proof "$\Leftarrow$" If $k = n * l$, then x^k

§8 Cyclic Subgroups

Note 8.1 (Generator Group Notation)**.**
Let $g \in (G, \circ)$. Notation: $\langle g \rangle = \{g^n : n \in \mathbb{Z}\}$
Let $g \in (G, +)$. Notation: $\langle g \rangle = \{ng : n \in \mathbb{Z}\}$

Example 8.2 (Generator Groups)

$$\begin{aligned}
5 \in \mathbb{Z}. \quad & \langle 5 \rangle = \{\dots, -10, -5, 0, 5, \dots\} \\
2 \in \mathbb{Z}. \quad & \langle 2 \rangle = \{\text{Even integers.}\} \\
5 \in \mathbb{Z}_{10}. \quad & \langle 5 \rangle = \{0, 5\} \\
6 \in \mathbb{Z}_{10}. \quad & \langle 6 \rangle = \{6, 2, 8, 4, 0\}
\end{aligned}$$

Note: $\mathbb{Z}_{10} = \langle 1 \rangle = \langle 3 \rangle = \langle 7 \rangle = \langle 9 \rangle$

Theorem 8.3
Let G be a group. Let $x \in G$, then $\langle x \rangle$ is a subgroup of G. Also, $\langle x \rangle$ is the smallest subgroup containing x.

Definition 8.4. $\langle x \rangle$ is the cyclic subgroup generated by x. If $G = \langle x \rangle$, then G is a cyclic group and x is a generator of G.

Definition 8.5. Detecting wheter or not a subset is a subgroup.

1. The identity Element is in the subgroup.
2. Inverse of each element is inside.
3. If two elements are inside, their product is inside as well.

§9 Chapter 5 09-27

Definition 9.1. A permutation of set X is a bijection $f : X \to X$.

Example 9.2

$x = \{1, 2, 3, 4\} \to \{3, 1, 4, 3\}$

I'm not fast enough to write this

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 3 \end{bmatrix}$$

$$\text{General notation:} \begin{bmatrix} 1 & 2 \dots\dots\dots\dots n \\ f(1) & f(2) \dots f(\dots) \dots f(n) \end{bmatrix}$$

Definition 9.3. The symmetric group of degree n (on n objects) is group S_N consisting of all permutations of $X = \{1, 2, \dots n\}$

Theorem 9.4

S_n is a group whose binary operation is composition of functions.

Proof.

1. Composition of functions is associative.
2. Inverses exist because inverses of bijections are bijections. f^{-1} is inverse of f.

□

Example 9.5

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{bmatrix}$$

Note 9.6. S_n has $n!$ elements.

Example 9.7

Consider the following function.

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

Definition 9.8. A cycle is a permutation with property that there is a subset $\{a_1, a_2, \ldots, a_m\} \subset \{1, 2, \ldots, n\}$ such that $f(a_i) = a_{i+1}$ for $1 \leq i < m$, and $f(a_m) = a_1$, and $f(x) = x$ when $x \notin \{a_1, \ldots, a_m\}$.

Example 9.9

Consider the following function.

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 2 & 3 & 7 & 5 & 6 & 1 \end{bmatrix}$$

$1 \to 4 \to 7 \to 1.$ $\quad (1, 4, 7)$ are being cycled.
$(2, 3, 5, 6)$ are fixed.

Note 9.10. Use notation $(a_1, a_2, \ldots, a_m)$ for the cycle. All other elements are fixed.

Example 9.11

$(3\ 7\ 5\ 1) \in S_7$ contains the same information as:

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 7 & 4 & 1 & 6 & 5 \end{bmatrix}$$

But the former is easier to understand.

Note 9.12. $(a_1, a_2, \ldots, a_m)$ and $(b_1, b_2, \ldots, b_l)$ are disjoint if $a_i \neq b_j$ for i, j.

Example 9.13

$(3\ 7\ 5\ 1)$ is disjoint from (64), but note that there are multiple ways of representing the same cycle.
For example. $(3\ 7\ 5\ 1) = (5\ 1\ 3\ 7) = (7\ 5\ 1\ 3)$

Theorem 9.14

Disjoint cycles commute.

$$(a_1\ \ldots\ a_m)(b_1\ \ldots\ b_l) = (b_1\ \ldots\ b_l)(a_1\ \ldots\ a_m)$$

if $c \notin \{a_1\ \ldots\ a_m, b_1\ \ldots\ b_l\}$

Theorem 9.15

Every permutation is a product of disjoint cycles.

Example 9.16

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 6 & 5 & 9 & 8 & 2 & 4 & 1 & 7 \end{bmatrix} = (3\ 5\ 8)(2\ 6)(7\ 4\ 9) \in S_9$$

More Practice:

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 7 & 8 & 2 & 1 & 5 & 3 & 6 & 10 & 9 & 4 \end{bmatrix} = (1\ 7\ 6\ 3\ 2\ 8\ 10\ 4)(5)(9) \in S_{10}$$

Practice in the other direction:

$$((1\ 3\ 5)(2\ 7\ 6\ 4))((1\ 2)(3\ 4)(5\ 6\ 7)) = (1\ 7)(2\ 3)(4\ 5)(6)$$

The (6) at the end is unnecessary because it is an identity element.

He just drew a pictorial circle on the board. I am just going to watch and absorb.

Theorem 9.17
Every permutation is a product of transpositions because:

> **Theorem 9.18**
> Every n-cycle is a product of $(n-1)$ transpositions.

Proof. $(a_1\ a_2\ \ldots\ a_m) = (a_1\ a_m)(a_1\ a_{m-1})\ldots(a_1\ a_3)(a_1\ a_2)$ □

§10 Lecture 09-30

§10.1 Review Complex Numbers

Recall $\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$
Come equipped with:

1. Addition: $(a_1 + b_1 i) + (a_2 + b_2 i) = (a_1 + a_2) + (b_1 + b_2)i$
2. Multiplication:

Complex numbers are associative and commutative under these operations.
There exists a complex conjugate.

Example 10.1
Complex conjugate of $(a + bi) = (a - bi)$

Note 10.2. $(a + bi)(a - bi) = a^2 + b^2$

$\mathbb{C}^*$ is a multiplicative group of complex numbers. All imaginary numbers have an inverse.
Rectangular and Polar coordinates.
Rectangular: x axis is real component, y axis is imaginary component.
Polar: radius is $\sqrt{a^2 + b^2}$
$\sqrt{a^2+b^2}\cos\theta + \sqrt{a^2+b^2}\sin\theta i = \sqrt{a^2+b^2}cis\theta = re^{i\theta}$

We have that $(r_1 cis\theta_1)(r_2 cis\theta_2) = r_1 r_2 cis(\theta_1 + \theta_2)$.
r is the "scale factor"
$cis\theta$ is the "rotation"
When $r = 1$, we get the subgroup of unit length com plex numbers.
$cis\theta = 1 =$ identity. $(cis\theta)^{-1} = cis(\theta)$ $cis\theta_1(cis\theta_2) = cis(\theta_1 + \theta_2)$
The nth roots of unity are the solutions to $x^n = 1$ in $\mathbb{C}^*$.
They form a cyclic subgroup of order n. Form verticies of a polygon with n verticies.
Recall. Given a geometric object X, its group of isometries or symmetries Isom(X) is a group with multiplication as composition of functions.
Recall. An isometry $f : X \to X$ is a distance preserving function.
dist $(p, q) =$ dist $(f(p), f(q)\forall p, q \in X$.

Definition 10.3. Dinedral group - D_n is the group of isometries of regular n-gon.

Example 10.4

$|D_n| = 2n$. It has n reflections and n rotations (counting the identity).

Consider $n = 3$. This gives a regular triangle. There are three reflections and three rotations. In this example, reflections fix 1 vertex and midpoing of opposite edge. Rotations fix the center. Group of isometries is not abelian because if you do the same thing in different orders you get different results.

Lemma. The set of rotations forms a subgroup.
Remark. Each reflection is its own inverse. Remark. Product of two reflections is a rotation.Generally it is by twice the angle between the axes of reflection.
When n is even, reflections occur in two ways.

1. Fix two vertices
2. Fix two midpopints of opposite edges.

Interpretation for $n = 1$ and $n = 2$.

1. $n = 2$ represented by isometry of "bigon" (looks like a lemon).
2. $n = 1$ represented by isometry of a water droplet. $reflection, identity$.

These two groups are the only abelian dinedral groups.
Let X be a rigid object. Its group of rigit motions consists of isometries that can be "physically realised". They are all rotations.

Example 10.5

Let X be a "brick". Dimensions: $2 \times 3 \times 5$

1. Isom X consists of 16 elements. We have 3 π rotations, the identity, and reflections.
2. Rigid motions of X consists of 8 elements.

§11 Math 235 Tutorial — 09-27

§11.1 Groups & Subgroups

Definition 11.1. A group $(G, \circ)$ is a set G together with an operation $\circ$ such that:

1. The elements are associative: $(a \circ b) \circ c = a \circ (b \circ c)$
2. There exists an identity element: $\exists e \in G$ such that $\forall g \in G$, $ge = eg = g$.
3. All elements contain an inverse within the group. $\forall g \in G \;\; \exists g^{-1}$ such that $g \circ g^{-1} = g^{-1}g = e$

Example 11.2

1. $(\mathbb{Z}, +)$. It is associative. Identity element is 0. $a^{-1} = -a$.
2. $(\mathbb{R} \setminus \{0\}, *)$. Is is associatve. Identity element is 1. All elements have an inverse (we removed 0 because 0 doesn't have an inverse).
3. $(\mathbb{Z}_n, +)$. It is associative. Identity element is 0. $a^{-1} = -a = n - a$.
4. $(\mathbb{Z}, *)$ is <u>NOT</u> a group because many integers do not have inverses that belong to the integers. $5^{-1} = \frac{1}{5} \notin \mathbb{Z}$
5. $(\mathbb{R}, *)$ is <u>NOT</u> a group because 0 does not have an inverse.

Note 11.3.

1. Multiplicative Notation: g^n means use the operation n times. $(G, \cdot)$
2. Additive Notation: ng means use the operation n times. $(G, +)$

Example 11.4

$$\begin{aligned} 11x + 2 &\equiv 16 \pmod{26} \\ 11x &\equiv 14 \pmod{26} \\ 11^{-1}11x &\equiv 11^{-1}14 \pmod{26} \\ x &\equiv 11^{-1}14 \pmod{26} \end{aligned}$$

If we were in $\mathbb{R}$, $(11)^{-1} = \frac{1}{11}$, but $\frac{1}{11} \notin \mathbb{Z}_{26}$ We need to find $(11)^{-1} \in \mathbb{Z}_{26}$. We know it exists because $\gcd(11, 26) = 1$

Euclidean Algorithm

$$\begin{aligned} 26 &= 2 * 11 + 4 \\ 11 &= 2 * 4 + 3 \\ 4 &= 1 * 3 + 1 \\ 3 &= 3 * 1 + 0 \end{aligned}$$

$$\begin{aligned} 1 &= 4 - 3 \\ &= 4 - (11 - 24) \\ &= 3 * 4 - 11 \\ &= 3(26 - 2 * 11) - 11 \\ &= 3 * 26 - 7 * 11 \end{aligned}$$

$\gcd(11, 26) = 1$ means there is a linear combination of 11 and 26 that equals 1. Taking the mod of both sides, mod of 26 is 0 and mod of 1 is 1 so it means that there is a multiple of 11 equal to 1 in mod 26. This means that it has an inverse. It's inverse is $-7 = 26 - 7 = 19$.

Back to equation:

$$\begin{aligned} 11x &= 14 \\ 19 \cdot 11x &= 19 \cdot 14 \\ x &= 266 \\ x &= 6 \end{aligned}$$

Solution: $\{x \in \mathbb{Z} : 26 \cdot n + 6 \quad n \in \mathbb{Z}\}$

Example 11.5

When presented with a Cayley table, how can we tell whether or not we are looking at a group.

$$\begin{bmatrix} a & b & c & d \\ b & b & c & d \\ c & d & a & b \\ d & a & b & c \end{bmatrix}$$

We must check identity element, inverses, and associativity,.

1. Identity element is a. ✓
2. b doesn't have an inverse so this is not a group.
3. Whether or not associativity fails, this is not a group. In order to see associativity in a cayley table, it must by symmetric along the line $y = -x$.

Advice: When checking if two groups are the same with cayley tables, look at the inverses and see if they match perfectly.

Exercise 11.6. Let G be a group such that $g^2 = e \quad \forall g \in G$. Show that G is abelian. In other words, $\forall a, b \in G \quad ab = ba$.

Solution. Let $a, b \in G$. We want to show that $ab = ba$. Note: $e = a^2 = b^2 = (ab)^2 = (ba)^2$

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

□

Advice: when proving that a group is abelian, play around with the identity matrix.

Definition 11.7. H is a subgroup of G if $H \subset G$ and H is a group with the inherited operation from G.

Example 11.8

$(\mathbb{Z}, +)$. Even integers are a subgroup of $\mathbb{Z}$ with the $+$ operation.
$(\mathbb{Z}, +)$. Odd integers are NOT a subgroup of $\mathbb{Z}$ with the $+$ operation because they don't have closure. $1 + 3 = 4$ and 4 is not an element of the odd integers.

Exercise 11.9. H_1 and H_2 are subgroups of G. Prove or disprove the following:

1. $H_1 \cap H_2$ is a subgroup of G.

   This is TRUE because it has the identity element, it has the inverses, and there is closure. There is no need to prove associativity because it is inherited from the binary operation.

   a) (Identity) $e \in H_1$ and $e \in H_2$ because H_1 and H_2 are subgroups.

   b) (Inverses) $a \in H_1 \cap H_2$. In particular, $a \in H_1 \Rightarrow a^{-1} \in H_1$ and $a \in H_2 \Rightarrow a^{-1} \in H_2$. So $a^{-1} \in H_1 \cap H_2$. Note: This works because inverses are unique.
   c) (Closure) $a, b \in H_1 \cap H_2$. $a, b \in H_1 \Rightarrow ab \in H_1$. Same for H_2. Therefore $ab \in H_1 \cap H_2$.

2. $H_1 \cup H_2$ is a subgroup of G?

   This is FALSE. Counter example: Let $A = \{n \in \mathbb{Z} : \text{n is a multiple of } 2\}$. Let $B = \{n \in \mathbb{Z} : \text{n is a multiple of } 5\}$.
   a) Identity ✓
   b) Inverses ✓
   c) Closure ✗

§12 10-02

Theorem 12.1

Any n-cycle is the product of $(n-1)$ transpositions.

Proof.

$$(a_1\ a_2\ \dots\ a_n) = (a_1\ a_n)(a_1\ a_{n-1})\dots(a_1\ a_3)(a_1\ a_2)$$

An alternative proof:

$$(a_1\ a_2\ \dots\ a_n) = (a_1\ a_2)(a_2\ a_3)\dots(a_{n-1}\ a_n)$$

□

Definition 12.2. An element $\sigma \in S_n$ is:

1. Even if σ is the product of an even number of transpositions
2. Odd if σ is the product of an odd number of transpositions.

Theorem 12.3

No $\sigma \in S_n$ is both even and odd.

Note 12.4. This means that any odd σ can only be expressed as a product of an odd number of transpositions.

Proof. Matricies over $\mathbb{R}$ have det positive or negative. Positive determinent maintains orientation. Negative determinent inverses orientation. An even element can be likened to a matrix with a positive determinent, while an odd element can be likened to a matrix with a negative determinent. □

Example 12.5

(2 3 5 7 9) is even because it is the product of four transpositions $(n-1)$.
(1 8 6 2) is odd because it is the product of three transpositions $(n-1)$.

Theorem 12.6

The set of even permutations of S_n is a subgroup. $A_n \subset S_n$, alternating group.

Proof. Identity Element: $() = (1\ 2)(1\ 2)$

Inverse: $() \in A_n$. Need to prove that $\sigma \in A_n \Rightarrow \sigma^{-1} \in A_n$.Indeed:

$$\sigma = (a_1\ b_1)(a_2\ b_2)\ldots(a_k\ b_k)$$

$$\sigma = (a_k\ b_k)\ldots(a_2\ b_2)(a_1\ b_1)$$

Closure: $\sigma, \phi \in A_n \Rightarrow \sigma \cdot \phi \in A_n$. Even number of permutations times even number of permutations gives an even number of permuatations which is in A_n.

Note 12.7. $|A_n| = \frac{1}{2}|S_n|$.

□

Understanding $A_4 \subset S_4$.

Listing elements in S_4. $S_4 =$

$$\{()\}$$
$$\{(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

$$\begin{gathered}\{(1\ 2\ 3), (1\ 3\ 2)\\ (1\ 2\ 4), (1\ 4\ 2)\\ (1\ 3\ 4), (1\ 4\ 3)\\ (2\ 3\ 4), (2\ 4\ 3)\}\end{gathered}$$

Note 12.8. S_4 "is" an isometry group of tetrahedron.

A_4 "is" the subgroup of its rigit motions.

§12.1 Cosets and Lagrange's Theorem

Let $H \subset G$ be a subgroup.

Let $g \in G$.

The left coset of H represented by g is $gH = \{gh : h \in H\}$.

The right coset of H represented by g is $Hg = \{hg : h \in H\}$.

Usually $gH \neq Hg$. (If equal just call them cosets if you'd like).

Example 12.9

Misleading but simple example.

$G = \mathbb{Z}_{12}, H = \langle 4 \rangle = \{0, 4, 8\}$.

$$0 + H = 4 + H = 8 + H = \{0, 4, 8\}$$
$$1 + H = 5 + H = 9 + H = \{1, 5, 9\}$$
$$2 + H = 6 + H = 10 + H = \{2, 6, 10\}$$
$$3 + H = 7 + H = 11 + H = \{3, 7, 11\}$$

Note 12.10. Notation can be confusing. gh means binary operation between g and h so when binary operation is + it means $g + h$.

Cosets formed a partition of the group.

Review: What is a partition? Disjoint subsets that unionize to form a set.

Example 12.11

$$H = \{1, -1, i, -i\} \subset \mathbb{Q}_8$$
$$1 \cdot H = \{1 * 1, 1 * -1, 1 * i, 1 * -i\}$$
$$jH = \{j * 1, j * -1, j * i, j * -i\} = \{j, -j, -k, k\} = Hj$$

Note 12.12. These form a partition of the quaternions.

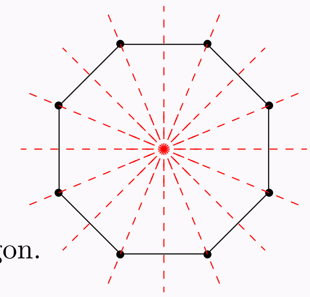
Example 12.13

$$K \subset \mathbb{Q}_8$$
$$K = \{1, -1\}$$

$$1K = \{1, -1\}$$
$$iK = \{i, -i\}$$
$$jK = \{j, -j\}$$
$$kK = \{k, -k\}$$

Note 12.14. For all of these, a left coset is a right coset.

Example 12.15



D_8. Symmetries of a regular octogon.

$$D_8 = \{r_i, \frac{i}{8}2\pi : 0 \leq i \leq 7\}$$

Subgroup (Same as the isometry of a rectangle living inside):

$$H = \{r_1, r_5, 0, \pi\}$$

Note 12.16. Product of rotation with rotation is a rotation. Product of a rotation with a reflection is a reflection. Product of a reflection with a reflection is a rotation.

$$0H = H$$
$$\frac{\pi}{8}H = \{r_2, r_6, \frac{\pi}{8}, \frac{5\pi}{8}\}$$
$$\frac{2\pi}{8}H = \{r_3, r_7, \frac{2\pi}{8}, \frac{6\pi}{8}\}$$
$$\frac{3\pi}{8}H = \{r_4, r_0, \frac{3\pi}{8}, \frac{7\pi}{8}\}$$
$$H\frac{\pi}{8} = \{r_0, r_4, \frac{\pi}{8}, \frac{5\pi}{8}\}$$

Note 12.17. Finding the product of a reflection and a rotation can be tricky. See how the composition affects a single point, and then identity a single rotation that affects the point in the same way.

Theorem 12.18

Lem 6.2. Let $g_1, g_2 \in G$ and $H \subset G$ be a group.
TFAE (similar for right cosets)

1. $g_1 H = g_2 H$
2. $H g_1^{-1} = H g_2^{-1}$. There is a bijection from a group to itself. Most obvious is identity bijection, but another one is every element to its inverse. In order to prove that statements 1 and 2 imply one another, use $\phi : G \to G, \phi(g) = g^{-1}.\phi$ is a bijection.$\phi(g_1 h) = h^{-1} g_1^{-1} \Rightarrow \phi(gH) \subset Hg^{-1}$.
3. $g_1 H \subset g_2 H$
4. $g_2 \in g_1 H$
5. $g_1^{-1} g \in H$. Reading this statement: "The difference between g_1 and g_2 lies in H.

Proof. $1 \Leftrightarrow 5$.
$\Rightarrow$. Suppose $g_1^{-1} g_2 \in H$, then $g_2^{-1} g_1 = (g_1^{-1} g_2)^{-1} \in H$.
Therefore $g_1 H \subset g_2 H$ because $g_1 h = (g_2 g_2^{-1}) g_1 h = g_2 (g_2^{-1} g_1) h \in g_2 H$. ($g_2 h'$ with $h' \in H$).
$\Leftarrow$. ($g_1 H = g_2 H$) $\Rightarrow$ ($g_1 e \in g_2 H$) $\Leftrightarrow$ ($g_1 \in g_2 H$) $\Rightarrow$ ($g_1 = g_2 h$ for some $h \in H$) $\Rightarrow g_2^{-1} g_1 = h \in H$. □

Theorem 12.19

Lem 6.4. Let $H \subset G$ be a subgroup. The left (or right) cosets of H form a partition of G.

Proof. Look:

$$G = \bigcup_{g \in G} gH \text{ because } g = ge \in gH$$

If $g_1 H \cap g_2 H \neq \varnothing$, then $g_1 H = g_2 H$ because if $g_1 h_1 = g_2 h_2$, then $g_1^{-1} g_2 = h_1 h_2^{-1} \in H$, hence $g_1 H = g_2 H$. □

Definition 12.20. Let $[G : H]$ be the index of H in G denote the number of left cosets of H in G.

Example 12.21

$$[D_8 : \{r_1, r_5, 0, \pi\}] = 4$$
$$[\mathbb{Z}_{12} : \{0, 4, 8\}] = 4$$
$$[\mathbb{Q}_8 : \{-1, 1\}] = 4$$
$$[\mathbb{Q}_8 : \{-1, 1, i, -i\}] = 2$$
$$[\mathbb{Z} : n\mathbb{Z}] = n$$
$$[G : G] = 1$$
$$[G : \{e\}] = |G|$$

Theorem 12.22
6.4. Let $H \subset G$. The number of left cosets equals the number of right cosets.

Proof. The inversion map on G sends left cosets to right cosets and right cosets to left cosets.

Let L be the collection of left cosets and R be the collection of right cosets.

Define bijection $\phi : L \to R$ by $\phi(gH) = Hg^{-1}$. Now to check that this function is well defined

Definition 12.23. . Well defined: independent of choice of representative.

Check that if $gH = kH \Rightarrow \phi(gH) = \phi(kH)$.

$$gH = kH \Rightarrow Hg^{-1} = Hk^{-1} \Rightarrow \phi(gH) = \phi(kH).$$

Now check that ϕ is injective.

$$[\phi(gH) = \phi(kH)] \Rightarrow [Hg^{-1} = Hk^{-1}] \Rightarrow [gH = kH]$$

Now check that ϕ is surjective.
$Hx = H(x^{-1})^{-1} = \phi(x^{-1}H)$ □

§13 Tutorial 5: Cyclic Groups - 10-04

Theorem 13.1
Every cyclic group is abelian.

Theorem 13.2
Every subgroup of a cyclic group is cyclic.

Let G be a cyclic group and let $a \in G$ be of order n.

Theorem 13.3
$a^m = e \Leftrightarrow n|m$

Theorem 13.4

$b = a^k \in G$, then $|b| = \frac{n}{\gcd(n,k)}$

Corollary: In additive notation

- $\mathbb{Z}_n = \langle 1 \rangle$ with $|1| = n$.
- $k = k \cdot 1$, then $|k| = \frac{n}{\gcd(n,k)}$
- Generators of $\mathbb{Z}_n$ are the integers k such that $1 \leq k < n$ and $\gcd(k, n) = 1$.

Example 13.5

Subgroups of $(\mathbb{Z}_8, +)$. Observe that $1, 2, 4, 8$ divide 8. We have to find $k \in \mathbb{Z}_8$ such that:

- $\gcd(8, k) = 1$

  $\{1, 3, 5, 7\}$. These generate subgroups of order $\frac{8}{\gcd} = 8$. There is only one such subgroup of $\mathbb{Z}_8$ so they must all be the same.

- $\gcd(8, k) = 2$

  $\{2, 6\}$. These generate subgroups of order 4: $\{0, 2, 4, 6\}$

  A question arises: Do 2 and 6 generate the same subgroup? $\langle 2 \rangle = \{0, 2, 4, 6\}$. $6 \in \langle 2 \rangle$ so $\langle 2 \rangle = \langle 6 \rangle$.

- $\gcd(8, k) = 4$

  $\{4\}$. Generates a group of order 2: $\{0, 4\}$

- $\gcd(8, k) = 8$

  $\{0\}$. Generates a sugroup of order 1: $\{0\}$

$$\begin{tikzcd}[arrows=dash]
 & \mathbb{Z}_8{=}\langle 1\rangle{=}\langle 3\rangle{=}\langle 5\rangle{=}\langle 7\rangle \arrow[dl] \arrow[dr] & \\
\langle 4\rangle \arrow[d] & & \langle 2\rangle{=}\langle 6\rangle \arrow[d] \\
\{0\} & & \{0\}
\end{tikzcd}$$

Example 13.6

List all the subgroups of $\mathbb{Z}_{10}$. Observe that 1, 2, 5, and 10 divide 10. Find $k \in \mathbb{Z}_{10}$ such that:

- $\gcd(k, 10) = 1$.

  $k = 1, 3, 7, 9$. $\mathbb{Z}_{10} = \langle 1 \rangle = \langle 3 \rangle = \langle 7 \rangle = \langle 9 \rangle$

- $\gcd(k, 10) = 2$.

  $k = 2, 4, 6, 8$. These generate subgroups of order 5.

  $\langle 2 \rangle = \langle 4 \rangle = \langle 6 \rangle = \langle 8 \rangle = \{0, 2, 4, 6, 8\}$

- $\gcd(k, 10) = 5$.

  $k = 5$. $\langle 5 \rangle = \{0, 5\}$.

- $\gcd(k, 10) = 10$.

  $k = 0$. $\langle 0 \rangle = \{0\}$

$$\begin{tikzcd}[column sep=small]
& \mathbb{Z}_{10}=\langle 1\rangle=\langle 3\rangle=\langle 7\rangle=\langle 9\rangle \arrow[dl, dash] \arrow[dr, dash] & \\
\langle 5\rangle \arrow[d, dash] & & \langle 2\rangle=\langle 4\rangle=\langle 6\rangle=\langle 8\rangle \arrow[d, dash] \\
\{0\} & & \{0\}
\end{tikzcd}$$

Example 13.7

Let G be a group. Assume $a \in G$ such that $a^{24} = e$. What are the possible orders of a?

Recall that when $a^n = e$, the possible orders of a are those which divide n. Possible orders are therefore 1, 2, 3, 4, 6, 8, 12, 24.

$|a| = n \Rightarrow a^n = e$. NOT $\Leftarrow$

Example 13.8

Let $a, b \in G$. Prove the following statements:

(a) $|a| = |a^{-1}|$

Proof. $|a| = n$. $|a^{-1}| = m$

$$\begin{aligned} a^n &= e \\ \Rightarrow (a^n)^{-1} \cdot a^n &= (a^n)^{-1} \cdot e \\ \Rightarrow e &= (a^n)^{-1} \\ \Rightarrow e &= (a^{-1})^n \Rightarrow m|n \end{aligned}$$

You can show similarly that $n|m$. By proving that $m|n$ and that $n|m$, we have proven that $n = m$. □

(b) $\forall g \in G, |a| = |g^{-1}ag|$

Proof. Let $g \in G$, $|a| = n$, $|g^{-1}ag| = m$. Observe that:

$$\begin{aligned} (g^{-1}ag)^m &= e \\ \Rightarrow (g^{-1}ag)(g^{-1}ag)\dots(g^{-1}ag) &= e \\ \Rightarrow g^{-1}a^m g &= e \\ \Rightarrow g \cdot g^{-1}a^m g \cdot g^{-1} &= g \cdot e \cdot g^{-1} \\ \Rightarrow a^m &= e \end{aligned}$$

Therefore $n|m$ because $|a| = n$. Similarly $m|n$. Therefore $m = n$. □

(c) $|ab| = |ba|$

Proof. By (b), $|ab| = |a^{-1}(ab)a| = |a^{-1}aba| = |ba|$ □

Exercise 13.9. Show that if G has no proper non-trivial subgroups, then G is a cyclic group of prime orders.

Proof.

(a) Showing that G is cyclic. Let $g \in G : g \neq e$. $\langle g \rangle$ is a non-trivial subgroup of G because $g \in \langle g \rangle$ and $g \neq e$. By assumption that G has no proper non-trivial subgroups, $\langle g \rangle = G$.

(b) Showing that G must be of prime order.

a) Case where $|G| = \infty$. Let G

Observe that $\langle g^2 \rangle$ is a non-trivial subgroup of G. Observe that $\langle g^2 \rangle \neq G$ because $g \notin \langle g^2 \rangle$. "If the order of a group is infinity, we will always be able to generate non-trivial proper subgroups."

b) Case where $|G| = n < \infty$

Assume that $n = d \cdot m$ for some d, m. Since $d|n$, then G must have a subgroup H of order d. This would mean that H is non-trivial and $H \neq G$. This is a contradiction $\Rightarrow |G| = p$ for some prime number.

□

Exercise 13.10. An infinite cyclic group G has exactly 2 generators.
$G = \langle a \rangle = \langle b \rangle$. This would mean that $a = b^k$ for some k, and that $b = a^l$ for some l.

$$a = b^k = (a^l)^k = a^{lk}$$
$$\Rightarrow a^{-1} \cdot a = a^{-1} a^{lk}$$
$$\Rightarrow e = a^{lk-1}$$

We know that $|a| = \infty$, therefore $lk - 1 = 0 \Rightarrow lk = 1$. This gives two possible cases: $l = k = 1$ or $l = k = -1$ because l and k must be integers. Therefore either $b = a$ or $b = a^{-1}$. This means that the only generators of G are a and a^{-1}.

§14 Lecture 10-07

Theorem 14.1
Proposition 6.9. Let $H \subset G$ and $g \in G$.
There is a bijection $\phi : H \to gH$ defined by $\phi(h) = gh$

Proof. This is injective because $(gh_1 = gh_2) \Rightarrow h_1 = h_2$
This is surjective because $gH = \{gh : h \in H\}$
$\{\phi(h) : h \in H\} = \phi(H)$ □

Theorem 14.2
Lagrange's Theorem
Let G be a finite group and $H \subset G$ a subgroup.
Then $\frac{|G|}{|H|} = [G : H]$

Proof. $G = g_1 H \cup g_2 H \ldots g_h H$ by theorem 6.4
Each of $|g_i H| = |H|$ by proposition 6.9
$|G| = n|H| = [G : H]\,|H| \Rightarrow \frac{|G|}{|H|} = [G : H]$ □

Theorem 14.3
Corollary 6.11.
Let G be finite and $g \in G$. Then $|g|$ divides $|G|$.

Proof. $|g| = |\langle g \rangle|$ which represents a subgroup of G which divides $|G|$ by Lagrange's Theorem. □

Theorem 14.4
Corollary. If $g \in G$ is finite, then $g^{|G|} = e$. Intuitively this makes sense because the order of g divides the order of G.
$g^{|G|} = g^{|g| \cdot [G:\langle g \rangle]} = g^{|g|^{[G:\langle g \rangle]}} = e^{[G:\langle g \rangle]} = e$

Example 14.5
For $\sigma \in S_n, \sigma^{n!} = e$. But this is very inefficient.

Theorem 14.6
Corollary. If $|G| = p$ with p prime, then $G = \langle g \rangle$ for each $g \in G - \{e\}$.

Proof. $1 \neq |g|$ Nd $|g|$ divides $|G| = p(by6.11)$. Therefore $|\langle g \rangle| = p$ so $\langle g \rangle = G$. □

Theorem 14.7
Corollary. If $K \subset H \subset G$ is a finite group, then $[G : K] = [G : H] [H : K]$

Proof. $[G : K] = \frac{|G|}{|K|} = \frac{|G|}{|H|} \cdot \frac{|H|}{|K|} = [G : H] [H : K]$. □

Definition 14.8. Euler ϕ function. $\phi : \mathbb{N} \to \mathbb{N}$
$|U_n| = \phi(n)$

Example 14.9
$\phi(1) = 1$
$\phi(9) = |\{1, 2, 4, 7, 8\}| = 5$
$\phi(8) = |\{1, 3, 5, 7\}| = 4$

Theorem 14.10
6.18. Euler's Theorem
Let $a, n \in \mathbb{Z}$ with $n > 0$ and $\gcd(a, n) = 1$, then $a^{\phi(n)} = 1$ (mod n)

Proof. Regard $a \in U_n$.
$a^{\phi(n)} = a^{|U_n|} = 1$ (mod n)
i.e. $g^{|G|} = e$
At the time of righting this it makes perfect sense, but we will see how it goes when I revisit it haha. □

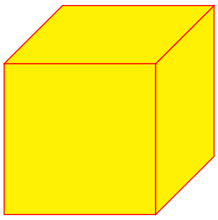
Theorem 14.11
6.19. Fermat Little Theorem.
Let p be prime and p does not divide a. (If p divided a, then a wouldn't be in the group of units U_p.)
Then $a^{p-1} = 1$ (mod p)

Proof. with $p = n$ prime, $a^{p-1} = a^{\phi(p)} \equiv_p 1$. This works because when p is prime, $\phi(n) = p - 1$.
moreover, for any a, $a^p \equiv_p a$. If $p|a$ this is $0 \equiv 0$. □

Definition 14.12. Conjugacy: Let $x, y \in G$. x is conjugate to y if there exists $g \in G$ such that $x = gyg^{-1}$. We use the notation $x \sim y$.
Lem: Conjugacy is an equivalence relation. Transitivity, Reflexivity, Symmetry.

Proof. Reflexivity: $x \sim x$ because $x = exe^{-1}$.
Symmetry: $(x \sim y) \Rightarrow (x = gyg^{-1}) \Rightarrow y = g^{-1}xg \Rightarrow y = gg^{-1}xg^{-1}g^{-1}$
Transitivity: □

§15 Case Study: The Cube



8 vertices, 6 faces, 12 edges.

Let G denote the symmetry group of the cube (the same as the isometry or motion group).

This group has 48 elements.

Indeed, there are 8 isometries that map each

§16 Tutorial 6: Permutation Groups

Recall 16.1.

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

Note 16.2. What is the order of a cycle σ of length r?

Answer: $|\sigma| = r$

Reasoning: $\sigma = (x_0\ x_1\ \ldots\ x_{r-1})$

$\sigma^m(x_i) = x_{i+m \pmod r}$

So if $m = r$, $\sigma^m(x_i) = x_i$ ✓

Example 16.3

Show that A_{10} contains an element of order 15.

Recall 16.4. A_n = even permutations of S_n

Every permutation σ can be written as a product of transpositions.

$(14356) = (16)(15)(13)(14)$.

There are an even number of transpositions. So $(14356) \in A_n$

First trying with A_{15}. $(1\ 2\ \ldots\ 14\ 15)$ is an example of an element with order 15. This is easy because we have access to 15 elements.

What about A_{10}?

$\sigma = (1\ 2\ 3)(4\ 5\ 6\ 7\ 8)$

$\sigma^m = ((1\ 2\ 3)(4\ 5\ 6\ 7\ 8))^m$

Note 16.5. $((1\ 2)(3\ 4))^2 = ((1\ 2)(3\ 4)(1\ 2)(3\ 4)) = (1\ 2)^2(3\ 4)^2$

Only because the cycles are disjoint do they have this property.

Therefore $\sigma^m = ((1\ 2\ 3)(4\ 5\ 6\ 7\ 8))^m = (1\ 2\ 3)^m(4\ 5\ 6\ 7\ 8)^m$

When does $(1\ 2\ 3)^m = (1)$? So long as $3 \mid m$

When does $(4\ 5\ 6\ 7\ 8)^m = (1)$? So long as $5 \mid m$

Therefore $\sigma^m = (1) \Leftrightarrow\ 5 \mid m$ and $3 \mid m$

Smallest such m is $m = 15$. Therefore $|\sigma| = 15$.

$\sigma = (1\ 3)(1\ 2)(4\ 8)(4\ 7)(4\ 6)(4\ 5)$

Exercise 16.6. Find $(a_1\ a_2\ \ldots\ a_n)^{-1}$

Answer 16.7. $(a_1\ a_2\ \ldots\ a_n)^{-1} = (a_n\ a_{n-1}\ \ldots\ a_1)$

Example 16.8

1. $(1\ 7\ 5\ 4\ 3)^{-1} = (34571)$
2. $[(1\ 4\ 2\ 3)(5\ 6)(1\ 3\ 2)]^{-1} = (1\ 3\ 2)^{-1} \cdot (5\ 6)^{-1} \cdot (1\ 4\ 2\ 3)^{-1}$
3. $(1\ 3\ 5\ 4\ 7)^{702} = (1\ 3\ 5\ 4\ 7)^{700} \cdot (1\ 3\ 5\ 4\ 7)^2 = (1) \cdot (1\ 3\ 5\ 4\ 7)^2 = (1\ 5\ 7\ 3\ 4)$

Exercise 16.9. $t = (a_1\ a_2\ \cdots\ a_k)$ is a cycle of length k

1. Show that for any permutation σ, $\sigma t \sigma^{-1} = (\sigma(a_1)\ \sigma(a_2)\ \cdots\ \sigma(a_k))$

   This is equivalent to showing that $\sigma t = (\sigma(a_1)\ \sigma(a_2)\ \cdots\ \sigma(a_k))\sigma$

   a) Case where $x \notin \{a_1, \cdots, a_k\}$

      $\sigma t(x) = \sigma(x)$ because t fixes x

      On the other hand, $(\sigma(a_1)\ \sigma(a_2)\ \cdots\ \sigma(a_k))\sigma(x) = \sigma(x)$ because $\sigma(x) \neq \sigma(a_i)$ for all i.

      $\sigma(x) = \sigma(x)$ ✓

   b) Case where $x = a_i$ for some i.

      If $i \neq k$,

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

      $(\sigma(a_1)\ \sigma(a_2)\ \cdots\ \sigma(a_k))\sigma(a_i) = \sigma(a_{i+1})$

      If $i = k$,

      $\sigma t(a_k) = \sigma(a_1)$

      $(\sigma(a_1)\ \sigma(a_2)\ \cdots\ \sigma(a_k))\sigma(a_k) = \sigma(a_1)$

2. Let μ be a cycle of length k.

   $t = (a_1\ a_2\ \cdots\ a_k)$

   Show that $\exists \sigma \in S_n$ such that $\sigma t \sigma^{-1} = \mu$

   We just showed that $\sigma t \sigma^{-1} = (\sigma(a_1)\ \sigma(a_2, \cdots \sigma(a_k))$

   Assume that $\mu = (b_1\ b_2\ \cdots\ b_k)$

   Let σ be such that $\sigma(a_i) = b_i$ and $\sigma(x) = x$ if $x \neq a_i$ for all i, then the result follows.

Exercise 16.10. Let there be group G and fix $g \in G$. Define $\lambda_g : G \to G$ where $\lambda(a) = ga$. Show that λ_g is a permutation.

Definition 16.11. A permutation of a set S is a bijection $\pi : S \to S$

1. Showing that λ_g is injective.

   Let $a, b \in G$ such that $\lambda_g(a) = \lambda_g(b)$.

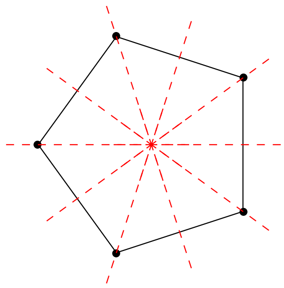
   $\Rightarrow ga = gb \Rightarrow a = b$ ✓

2. Showing that λ_g is surjective.

   For all $b \in G$, let $a = g^{-1}b \in G$. $\lambda_g(a) = gg^{-1}b = b$.

   Therefore the image of λ_g is G so λ_g is surjective. ✓

Exercise 16.12 (Dihedral Group)**.** Using the cyclic notation, list the elements in D_5.
$r = (1\ 5\ 4\ 3\ 2)$ $\quad r^2 = (1\ 4\ 2\ 5\ 3)$ $\quad r^3 = \ldots$
$s = (2\ 5)(3\ 4)$ $\quad sr = \ldots$



Exercise 16.13. Show that S_n is non-abelian for $n \geq 3$. We need to find $\sigma, \tau \in S_n$ such that $\sigma\tau \neq \tau\sigma$
$\sigma = (1\ 2)$ $\quad \sigma = (1\ 3)$
$\sigma\tau = (1\ 3\ 2)$ $\quad \tau\sigma = (1\ 2\ 3)$
$(1\ 3\ 2) \neq (1\ 2\ 3)$

§17 10-11

Lemma 17.1

Conjugacy is an equivalence relation.
$x \sim y$ if $x = gyg^{-1}$ for some $g \in G$

Theorem 17.2

Any two k-cycles in S_n are conugate. Moreover, any conjugate of a k-cycle is a k-cycle.

Proof. $\alpha = (a_1 a_2 \ldots a_k)$ $\quad \beta = (b_1 b_2 \ldots b_k)$
Let σ be a bijection with $\sigma(b_i) = a_i$ for $1 \leq i \leq k$
Then $\sigma\beta\sigma^{-1} = \alpha$. Claiming that β and α are conjugate to one another.
If $x \notin \{a_1 \ \ldots \ a_k\}$, then $\sigma\alpha\sigma^{-1}(x) = x$

Example 17.3

$\sigma\beta\sigma^{-1}(a_i) = \sigma\beta b_i = \sigma b_{i+1} = a_{i+1} = \alpha(a)$

□

§17.1 A_4 is the group of rigid motions of a tetrahedron

Note 17.4. A_4 is the subgroup of even elements in S_4.

$$\text{identity: } [e] = \{()\}$$
$$[(12)(34)] = \{(12)(34), (13)(24), (14)(23)\}$$
$$\text{Clockwise rotations about a face: } [(123)] = \{(123), (134), (142), (243)\}$$
$$\text{Counter clockwise rotations about a face: } [(132)] = \{(132), (143), (124), (234)\}$$

Note 17.5. A_4 has no 6 element subgroup even though 6 divides $|A_4|$

§18 Isomorphisms

Definition 18.1. $(G, \cdot)$ and $(H, \circ)$ are isomorphic if there exists a bijection $\phi : G \to H$ such that $\phi(a \cdot b) = \phi(a) \circ \phi(b)$ for all $a, b \in G$.

This would make ϕ an isomorphism.

$G"equalsignwithsimontop"H$

Note 18.2. Let $H \subset G$ be a subgroup. It is possible for $x \not\sim y$ in H while $x \sim y$ in G. This is a distinguishing between $\sim_H$ and $\sim_G$.

Example 18.3

$H \subset S_{17}$

$H = \langle (1\ 2 \dots 17) \rangle$

H is cyclic and abelian.

It has 17 conjugacy classes.

All nontrivial elements of H are conjugate in S_{17}.

Note 18.4. In an abelian group, two elements are conjugate iff they are equal.

If H is abelian, then $(x \sim y) \Leftrightarrow x = aya^{-1} = y$

§19 Isomorphisms

Definition 19.1. $(G, \cdot)$ and $(H, \circ)$ are <u>isomorphic</u> if there exists a bijection $\phi : G \to H$ such that $\phi(a \cdot b) = \phi(a) \circ \phi(b)$ for all $a, b \in G$.

Then ϕ is an <u>isomorphism</u> and we write $G \equiv\sim H$

Example 19.2

$\phi : \mathbb{Z}_4 \to U_5$

$$\begin{aligned} 0 &\to 1 \\ 1 &\to 2 \\ 2 &\to 4 \\ 3 &\to 3 \end{aligned}$$

$$\phi(3+2) = \phi(1) = 2 = \phi(3)\cdot\phi(2) = 3 \cdot 4 = 2 \checkmark$$

$$(\mathbb{Z}_4, +) : \begin{array}{c|cccc} \circ & 0 & 1 & 2 & 3 \\ \hline 0 & 0 & 1 & 2 & 3 \\ 1 & 1 & 2 & 3 & 0 \\ 2 & 2 & 3 & 0 & 1 \\ 3 & 3 & 0 & 1 & 2 \end{array}$$

$$(U_5, \cdot) : \begin{array}{c|cccc} \circ & 1 & 2 & 4 & 3 \\ \hline 1 & 1 & 2 & 4 & 3 \\ 2 & 2 & 4 & 3 & 1 \\ 4 & 4 & 3 & 1 & 2 \\ 3 & 3 & 1 & 2 & 4 \end{array}$$

Note 19.3. G and H are isomorphic if by "reordering the elements of H", they have the same caylety table - the only difference is notation.

"bijection between groups extends to a bijection between multiplication tables. Multiplication tables are the same, the difference being notation. A different language"

Example 19.4

$\phi : \mathbb{Z}_4 \to \{\pm 1, \pm i\} \subset \mathbb{C}^*$

$$\begin{aligned} 0 &\to 1 \\ 1 &\to i \\ 2 &\to -1 \\ 3 &\to -i \end{aligned}$$

$$\phi(n) = i^n$$
$$\phi(a+b) = i^{a+b} = i^a \cdot i^b = \phi(a) \cdot \phi(b)$$

$$(\{\pm 1, \pm i\} \subset \mathbb{C}^*, \cdot) : \begin{array}{c|llll} \circ & 1 & i & -1 & -i \\ \hline 1 & 1 & i & -1 & -i \\ i & i & -1 & -i & 1 \\ -1 & -1 & -i & 1 & i \\ -i & -i & 1 & i & -i \end{array}$$

Example 19.5

$\phi : \mathbb{Z}_4 \to \mathbb{Z}_4$

$$\begin{aligned} 0 &\to 0 \\ 1 &\to 3 \\ 2 &\to 2 \\ 3 &\to 1 \end{aligned}$$

This is an isomorphism.

Theorem 19.6

G is abelian if and only if the map $\phi : G \to G$ given by $\phi(a) = a^{-1}$ for all $a \in G$ is an isomorphism.

Proof. .

($\Leftarrow$)

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

($\Rightarrow$)

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

□

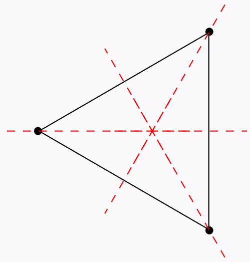
Example 19.7

$$Q_8 \equiv\sim \left\{ \pm\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pm\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \pm\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \pm\begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix} \right\}$$
$$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$$

These two representations of the quaternions are isomorphic to one another.

Example 19.8

$D_3 \equiv\sim S_3$



$$0 \to ()$$
$$\frac{2\pi}{3} \to \{1\ 3\ 2\}$$
$$\frac{4\pi}{3} \to \{1\ 2\ 3\}$$
$$\alpha \to \{2\ 3\}$$
$$\beta \to \{1\ 2\}$$
$$\gamma \to \{1\ 3\}$$

There are many isomorphisms from D_3 to S_3.

Theorem 19.9

If $\phi : G \to H$ is an isomorphism, then $\phi^{-1} : H \to G$ is an isomorphism.

Proof. phi^{-1} is a bijection since ϕ is (ϕ^{-1} exists because ϕ is a bijection)

$$\phi^{-1}(a \cdot b) = \phi^{-1}\Big(\phi(\phi^{-1}(a))\phi(\phi^{-1}(b))\Big) = \phi^{-1}\Big(\phi(\phi^{-1}(a)\phi^{-1}(b))\Big) = \phi^{-1}(a)\phi^{-1}(b)$$

$\square$

Theorem 19.10

Any "property" of G is a "property" of H.

Example 19.11

$|G| = |H|$
G is abelian $\Leftrightarrow$ H is abelian
G is cyclic $\Leftrightarrow$ H is cyclic
$G = \langle g \rangle \Leftrightarrow H = \langle \phi(g) \rangle$

Theorem 19.12

If G is cyclic and $|G| = \infty$ the $G \equiv\sim \mathbb{Z}$
If G is cyclic and $|G| = n$ the $G \equiv\sim \mathbb{Z}_n$

Proof. Let $G = \langle g \rangle$. Consider map $\phi : \mathbb{Z} \to G$ given by $\phi(i) = g^i$
Claim that ϕ is a bijection.
Surjective because each $x \in G$ is $g = g^i$ for some i so $\phi(i) = x$ where x is arbitrary.
Injective because $\phi(i) = \phi(j) \Rightarrow g^i = g^j \Rightarrow g^i g^{-j} = e \Rightarrow g^{i-j} = e \Rightarrow i = j = 0 \Rightarrow i = j$
Therefore ϕ is an isomorphism because $\phi(i + j) = g^{i+j} = g^i g^j = \phi(i)\phi(j)$ □

§20 Cosets

Definition 20.1. Let G be a group. Let H be a subgroup of G. $g \in G$
$gH = \{gh : h \in H\}$ (left coset)
$Hg = \{hg : h \in H\}$ (right coset)

Theorem 20.2

Left (or right) cosets of H in G partition G.

Theorem 20.3 (Lagrange-theorem)

Let G be a finite group. Let H be a subgroup of G.

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

Note 20.4. $[G : H]$ is the number of cosets of H in G.

Remark 20.5. Right and left cosets are not necessarily equal.

Example 20.6

Let $H = \{id, (1\ 2)\}$ be a subgroup of S_3.

$$(1\ 2\ 3)H = \{(1\ 2\ 3), (1\ 2\ 3)(1\ 2)\} = \{(1\ 2\ 3), (1\ 3)\}$$
$$H(1\ 2\ 3) = \{(1\ 2\ 3), (1\ 2)(1\ 2\ 3)\} = \{(1\ 2\ 3), (2\ 3)\}$$

Exercise 20.7.

(a) What is the index of $\langle 6\rangle$ in $\mathbb{Z}_{24}$.

By lagrange:

$$[\mathbb{Z}_{24}, \langle 6\rangle] = \frac{|\mathbb{Z}_{24}|}{|\langle 6\rangle|} = \frac{24}{4} = 6$$
$$\langle 6\rangle = \{0, 6, 12, 18\} \qquad |\langle 6\rangle| = 4$$

(b) Let $\sigma = (1\,2\,5\,4)(2\,3)$ in S_5. What is the index of $\langle\sigma\rangle$ in S_5?

$$\sigma = (1\,2\,5\,4)(2\,3) = (2\,3\,5\,4\,1) \text{ because sigma is not disjoint}$$
$$|\sigma| = 5 \qquad |\langle\sigma\rangle| = 5$$
$$[S_5 : \langle\sigma\rangle] = \frac{5!}{5} = 4! = 24$$

Exercise 20.8. Find the left cosets of $H = \{id, \mu\}$ in D_4. (D_4 is the symmetries of a square.)

Recall 20.9. $\mu = (1\,2)(3\,4)$

$D_4 = \{id, (1\,2\,3\,4), (1\,3)(2\,4), (1\,2)(3\,4), (1\,4\,3\,2), (1\,4)(2\,3), (1\,3), (2\,4)\}$
By lagrange: $[D_4, H] = \frac{|D_4|}{|H|} = \frac{8}{2} = 4$

Example 20.10

Let $H = \{id, (1\,2)(3\,4)\}$

$$(1\,3)H = \{(1\,3), (1\,3)(1\,2)(3\,4)\} = \{(1\,3), (1\,2\,3\,4)\}$$
$$(2\,4)H = \{(2\,2), (2\,4)(1\,2)(3\,4)\} = \{(2\,4), (1\,4\,3\,2)\}$$
$$(1\,3)(2\,4)H = \{(1\,3)(2\,4), (1\,3)(2\,4)(1\,2)(3\,4)\} = \{(1\,3)(2\,4), (1\,4)(2\,3)\}$$

Conceptually it makes sense that the size of a subgroup must divide the size of the group so that the cosets of the subgroup can partition the group into subgroups of equal sizes.

Recall 20.11. S_n represents all possible bijections between $\mathbb{N}_n$ and $\mathbb{N}_n$

Exercise 20.12. Let G be a group and H a subgroup of G such that $[G : H] = 2$ and $a, b \in G \setminus H$. Show that $ab \in H$.
We know that $a^{-1} \notin H$. Therefore $a^{-1}H \neq H$.

Recall 20.13. $g_1H = g_2H \Leftrightarrow g_1 \in g_2H$. This implies that $g_1 \notin g_2H \Leftrightarrow g_1H \neq g_2H$.

Similarly $b \notin H$ implies that $bH \neq H$.

There are only two cosets, so $a^{-1}H = bH$. Therefore

$$a^{-1}h = bh'$$

for some $h, h' \in H$. Reordering we get that $ab = h(h')^{-1} \in H$

Exercise 20.14. Is it possible to have a group G of order 6 such that all of its elements have order 1 or 2? NO

Proof by contradiction. $G = \{e, g_1, g_2, g_3, g_4, g_5\}$ such that $|g_i| = 2$ for all $i \in \{1, 2, 3, 4, 5\}$

Claim: With this construction, G must be abelian.

$$a, b \in G$$
$$ab = id \cdot ab = (ba)^2 ab \text{ because } ba \in G \Rightarrow (ba)^2 = e$$
$$\text{Expanding: } ab = babaab = bab^2 = ba$$

Consider the subgroup $H = \{1, g_1, g_2, g_1g_2\}$. This is a subgroup because G is abelian and all its elements have order 2.

By lagrange: $[G : H] = \frac{|G|}{4}$. This is a contradiction because $|G| = 6$ and 4 does not divide 6.

Basically, with the assumption that G is of order 6 with all elements being of order 1 or 2, we can build a subgroup of order 4 which doesn't make sense because 4 doesn't divide 6.

Exercise 20.15. Let H, K be subgroups of G. Show that for $x, y \in G$, either $xH \cap yK = \varnothing$, or $xH \cap yK$ is a coset of $H \cap K$. (Recall that $H \cap K$ is a subgroup).

Pick $x, y \in G$. If $xH \cap yK = \varnothing$, we are done with this case.

Assume that $xH \cap yK \neq \varnothing$. Pick $g \in xH \cap yK$. Then $g \in xH \Rightarrow xH = gH$ and $g \in yK \Rightarrow yK = gK$.

Therefore $xH \cap yK = gH \cap gK$.

Claim: $gH \cap hK = g(H \cap K)$

Proof. $(\subseteq)$. Pick $z \in gH \cap gK$.

$$\Rightarrow z = gh = gk \text{ for some } \ h \in H, k \in K$$
$$\Rightarrow h = k \text{ so } h \in H \cap K$$
$$\text{So } z = gh \quad h \in H \cap K$$
$$\text{Then } z \in g(H \cap K)$$

$$(\supseteq)\text{Let } z \in g(H \cap K)$$
$$\Rightarrow z = gl \text{ for some } l \in H \cap K$$
$$l \in H \Rightarrow z \in gH$$
$$l \in K \Rightarrow z \in gK$$
$$z \in gH \cap gK$$

Therefore $gH \cap hK = g(H \cap K)$ □

§21 Isomorphisms Continued

Theorem 21.1

If G is cyclic and $|G| = n$, then $G \equiv \mathbb{Z}_n$.

Proof. Consider $\phi : \mathbb{Z}_n \to G$ given by $\phi(i) = g^i$, then ϕ is a bijection.
Injective: $\phi(i) = \phi(j) \Rightarrow g^i = g^j \Rightarrow g^{i-j} = g^0 \Rightarrow i - j \equiv_n = 0 \Rightarrow i = j$
Surjective: Let $G = \langle g \rangle$.
$\{g^0, g^1, \ldots, g^{n-1}\} = G$
$\{0, 1, \ldots, n-1\} = \mathbb{Z}_n$ $\square$

Theorem 21.2

Cor 9.9.
If $|G| = p$ and p is prime, then $G \equiv\sim \mathbb{Z}_p$

Proof. We showed that $G = \langle g \rangle$ for any $g \neq e$.
My understanding: if prime order, it must be cyclic. $\square$

Theorem 21.3

Isomorphism is an equivalence relation on a set of groups.
Reflexive: $G \equiv\sim G$ because $1_G : G \to G$ is isomorphism.

$$1_G(ab) = ab = 1_G(a) \cdot 1_G(b)$$

Symmetrical: $G \equiv\sim K \Rightarrow K \equiv\sim G$ because $\phi : G \to K$ isomorphism then $\phi^{-1} : K \to G$ is isomorphism.
Transitive: $f : G \to K$ and $h : K \to J$ are isomorphisms then $h \circ f : G \to J$ is ismorphism.

Theorem 21.4 (Cayley's Theorem)
Every group is isomorphic to a permutation group.

Recall 21.5. A permutation group is a subgroup of S_n

Proof. G is isomorphic to a subgroup of the group of bijections of the set G. You could think of this as S_G.

For $g \in G$, let $\lambda_g : G \to G$ be permutation "left multiply by g" i.e. $\lambda_g(x) = gx$ for all $x \in G$.

Let $\overline{G} = \{\lambda_g : g \in G\}$

Claim: $G \cong \overline{G}$ with $\phi(g) = \lambda_g$

Injectivity: if $\phi(x) = \phi(y)$ then λ_x and λ_y are some bijection of G.

$$x = xe = \lambda_x(e) = \lambda_y(e) = ye = y$$

Surjectivity (immediate). $\overline{G} = \{\lambda_g : g \in G\} = \{\phi(g) : g \in G\} = \phi(G)$

Homomorphism:

$$\begin{gathered} \phi(xy) = \lambda_{xy} \\ \phi(x)\phi(y) = \lambda_x\lambda_y \\ \lambda_{xy}(z) = (xy)z \text{ for all } z \in G \\ \lambda_x(\lambda_y(z)) = \lambda_x(yz) = x(yz) \\ (xy)z = x(yz) \checkmark \end{gathered}$$

□

Example 21.6

$$\begin{gathered} G = \{\pm 1, \pm i\} \\ G \cong \overline{G} \subset S_G \cong S_4 \\ 1 \to \lambda_1 = \begin{bmatrix} 1 & -1 & i & -i \\ 1 & -1 & i & -i \end{bmatrix} = () \\ -1 \to \lambda_{-1} = \begin{bmatrix} 1 & -1 & i & -i \\ -1 & 1 & -i & i \end{bmatrix} = (1\ \ -1)(i\ \ -i) \\ i \to \lambda_i \begin{bmatrix} 1 & -1 & i & -i \\ i & -i & -1 & 1 \end{bmatrix} = (1\ i\ \ -1\ \ -i) \\ -i \to \lambda_{-i} = \begin{bmatrix} 1 & -1 & i & -i \\ -i & i & 1 & -1 \end{bmatrix} = (1\ \ -i\ \ -1\ i) \end{gathered}$$

Example 21.7

$$Q_8 \cong \overline{Q_8} \subset S_8$$

Example 21.8

$$\mathbb{Z}_6 \hookrightarrow S_{\mathbb{Z}_6} = S_{\{0,1,2,3,4,5\}}$$
$$2 \to_\phi \lambda_2 \qquad \lambda_2 : \mathbb{Z}_6 \to \mathbb{Z}_6 \qquad \lambda_2(x) = 2 + x$$
$$\lambda_2 = (0\ 2\ 4)(1\ 3\ 5)$$
$$\lambda_3 = (0\ 3)(1\ 4)(2\ 5)$$
$$\lambda_5 = (0\ 5\ 4\ 3\ 2\ 1)$$

§22 Direct Products

Let $(G, \cdot), (H, \cdot)$ be groups. The external direct product of $G \times H$.

$$G \times H = \{gh : g \in G, h \in H\}$$

with binary opteration $(g_1, h_1)(g_2, h_2) = (g_1 \cdot g_2, h_1 \cdot h_2$.

Note 22.1. Associative. Proof.

Note 22.2. Identity $= (1_G, 1_H)$.

We define the external direct product of $G_1 \times G_2 \times \cdots \times G_k$

Note 22.3.

$$|G| = \prod_{i=1}^{k} |G_i|$$

Definition 22.4. $G^n = G \times \cdots \times G$.

Example 22.5

$\mathbb{R}^n$ and $\mathbb{Z}_2^3$.

We have 5 groups of order 8. $Q_8, D_4, \mathbb{Z}_8, \mathbb{Z}_4 \times \mathbb{Z}_2, \mathbb{Z}_2^3$.

1. cyclic with 3 subgroups of order 4. nonabelian
2. cyclic with 1 subgroup of order 4. nonabelian
3. cyclic. abelian
4. not cyclic with cosets of order 4 abelian
5. each element has order 2 abelian

Theorem 22.6

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

Example 22.7

Theorem 22.8
$\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn} \Leftrightarrow \gcd(m, n) = 1$

Proof. □

§23 Normal Subgroups and Factor Groups

Definition 23.1. A subgroup $H \subset G$ is normal if $gH = Hg$ for all $g \in G$.

Example 23.2

1. Every subgroup of H is normal if G is abelian.
2. If $[G : H] = 2$, then H is normal. This is because $gH \cup H = G = H \cup Hg$.
3. Let $H \subset D_h$ be a subgroup of rotations. Then H is normal (because $[D_h : H] = 2$). However, let $R = \langle r \rangle$ where r is reflection, then R is not normal in D_n.
4. $\{e\} \subset G$ and $G \subset G$ are normal.

Theorem 23.3
Let $N \subset G$ be a subgroup. TFAE

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

Note 23.4. For $S \subset G$ and $x, y \in G$, $xSy = \{xsy : s \in S\}$

Proof.

(1 ⇒ 2) We must show that $gng^{-1} \in N$ for all $n \in N$.

$$gN = Ng \Rightarrow \exists n' \in N \text{ such that } gn = n'g$$
$$\text{Hence:} \quad (gn)g^{-1} = (n'g)g^{-1} = n' \in N$$

(2 ⇒ 3) Suffices to show that $N \subset gNg^{-1}$.

$$g^{-1}ng \in g^{-1}N(g^{-1})^{-1} \subset N \Rightarrow g^{-1}ng = n' \text{ for some } n' \in N$$
$$\text{So } n = gn'g^{-1}$$

(3 ⇒ 1) Right multiply by g. $gNg^{-1} = N$ gives $gN = Ng$.

□

§23.1 Factor Group or Quotient Group

Definition 23.5. Let $N \subset G$ be a normal subgroup of G. The left cosets of N in G form a group whose operation is $(aN)(bN) = (abN)$. This is the quotient group of G and N, denoted by G/N.

Theorem 23.6

G/N is really a group!

Proof.

1. To show: Operation is well defined. If $aN = a'N$ and $bN = b'N$, then $abN = a'b'N$.

   We know that $a' = an_1$ and $b' = bn_2$ where $n_1, n_2 \in N$. Hence $a'b' = (an_1)(bn_2)$. Because $Nb = bN$, we hvae that $n_1 b = bn_3$ for some $n_3 \in N$. Therefore $a'b' = a(n_1 b)n_2 = a(bn_3)n_2 = abn_3n_2$.

   Thus $a'b'N = abN$ since $(ab)^{-1}(a'b') = b^{-1}a^{-1}abn_3n_2 = n_3n_2 \in N$.

2. To show: Associativity.

$$\begin{aligned} aN(bNcN) &= aN(bcN) = a(bc)N = abcN \\ (aNbN)cN &= (abN)cN = (ab)cN = abcN \end{aligned}$$

To show: Identity. $eNxN = exN = xN = xeN = xNeN$

To show: Inverses. $(xN)(x^{-1}N) = xx^{-1}N = eN = x^{-1}xN = x^{-1}NxN$ $\square$

Recall 23.7. If G is finite, $|G/N| = [G : N] = |G|/|N|$

Example 23.8

$\mathbb{Z}_n$ is just notation for $\frac{\mathbb{Z}}{n\mathbb{Z}}$

Quotient Group $\mathbb{Z}/4\mathbb{Z}$:

$\circ$	$0+4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$
$0+4\mathbb{Z}$	$0+4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$
$1+4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$	$4+4\mathbb{Z}$
$2+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$	$4+4\mathbb{Z}$	$5+4\mathbb{Z}$
$3+4\mathbb{Z}$	$3+4\mathbb{Z}$	$4+4\mathbb{Z}$	$5+4\mathbb{Z}$	$6+4\mathbb{Z}$

Example 23.9

$H \subset D_n$ be subgroup of rotations. $D_n/H \cong \mathbb{Z}_2$ since $[D_n : H] = 2$.

Example 23.10

$S_n/A_n \cong \mathbb{Z}_2$

Example 23.11

$N = \{\pm 1\}$ is normal in Q. It's cosets are:

$$\begin{aligned} 1N &= \{\pm 1\} = N1 \\ jN &= \{\pm j\} = Nj \\ kN &= \{\pm k\} = Nk \\ iN &= \{\pm i\} = Ni \end{aligned}$$

What is Q/N? Note: $|Q/N| = [Q : N] = 4$.

$$Q/N : \quad \begin{array}{c|cccc} \circ & 1N & iN & jN & kN \\ \hline 1N & 1N & iN & jN & kN \\ iN & iN & 1N & kN & jN \\ jN & jN & kN & 1N & iN \\ kN & kN & jN & iN & 1N \end{array}$$

Example 23.12

$$(\mathbb{Z}_4, +) : \quad \begin{array}{c|cccc} \circ & (0,0) & (1,0) & (0,1) & (1,1) \\ \hline (0,0) & (0,0) & (1,0) & (0,1) & (1,1) \\ (1,0) & (1,0) & (0,0) & (1,1) & (0,1) \\ (0,1) & (0,1) & (1,1) & (0,0) & (1,0) \\ (1,1) & (1,1) & (0,1) & (1,0) & (0,0) \end{array}$$

§24 Isomorphisms

Definition 24.1. Let G, H be groups and $\phi : G \to H$ where ϕ is bijective and $\phi(ab) = \phi(a)\phi(b)$. Then ϕ is an isomorphism.

Example 24.2

$$(\mathbb{Z}_2, +) : \quad \begin{array}{c|cc} \circ & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array}$$

$$(U(4) = \{1, 3\}, \times) : \quad \begin{array}{c|cc} \circ & 1 & 3 \\ \hline 1 & 1 & 3 \\ 3 & 3 & 1 \end{array}$$

$$\mathbb{Z}_2 \cong U(4)$$

Example 24.3

Show that $\phi : \mathbb{C} \to \mathbb{C}$ is an isomorphism, where $\phi(a + ib) = a - ib$.

Surjective: Let $a + ib \in \mathbb{C}$, then $\phi(a - ib) = a + ib$. So for every element in $\mathbb{C}$, there exists an element in $\mathbb{C}$ that maps to it via ϕ.

Injective: Let $\phi(a+ib) = \phi(c+id)$. This implies that $a-bi = c-di \Rightarrow a = c$ and $b = d$.

Homomorphism: Let $x, y \in \mathbb{C}$. $x = a + bi$ and $y = c + id$ for some $a, b, c, d \in \mathbb{R}$.

$\phi(x+y) = \phi((a+c)+i(b+d)) = a+c-i(b+d) = (a-ib)+(c-id) = \phi(x)+\phi(y)$

Theorem 24.4

Let G be cyclic such that $G = \langle a \rangle$. Let H be a group isomorphic to G. Then H is cyclic.

Proof. Let $h \in H$. Because ϕ is surjective, $\exists g \in G$ such that $\phi(g) = h$.

$g \in G$, so $g = a^n$ for some n. Therefore $h = \phi(a^n) = (\phi(a)^n)$.

Because h is an arbitrary element in H, $\langle \phi(a) \rangle = H$. □

Remark 24.5. Let $G = \langle a \rangle$ be cyclic. Let $\phi : G \to H$ be an isomorphism. Then ϕ is completely determined by $\phi(a)$.

Example 24.6

$\phi : \mathbb{Z}_5 \to \mathbb{Z}_5$. In this case we chose $\phi(1) = 2$. The rest is determined by this because if $\phi(a) = b$, then $\phi(a^2) = (b^2)$. Note: Only for cyclic groups.

$$\begin{aligned} 0 &\to 0 \\ 1 &\to 2 \\ 2 &\to 4 \\ 3 &\to 1 \\ 4 &\to 3 \end{aligned}$$

Example 24.7

Prove or disprove that $\mathbb{Q}$ is isomorphic to $\mathbb{Z}$.

Answer 24.8. NO. We know that $\mathbb{Q}$ is not cyclic. Because $\mathbb{Z}$ is cyclic, $\mathbb{Z} \ncong \mathbb{Q}$.

Recall 24.9. If $G = \langle b \rangle$, then $|b^k| = \frac{n}{\gcd(k,n)}$.

Exercise 24.10. Find the order of the following.

(a) $(3, 4)$ in $\mathbb{Z}_4 \times \mathbb{Z}_6$.

$|3| = \frac{4}{\gcd(3,4)} = \frac{4}{1} = 4$ in $\mathbb{Z}_4$.

$|4| = \frac{6}{\gcd(4,6)} = \frac{6}{2} = 3$ in $\mathbb{Z}_6$.

$|(3,4)| = \text{lcm}(4,3) = 12$.

(b) $(5, 10, 15)$ in $\mathbb{Z}_{25} \times \mathbb{Z}_{25} \times \mathbb{Z}_{25}$.

$|5| = 5$

$|10| = 5$

$|15| = 5$

$|(5, 10, 15)| = \text{lcm}(5, 5, 5) = 5$

Exercise 24.11. Show that G is abelian if and only if $\phi : G \to G$ is an isomorphism where $\phi(x) = x^{-1}$.

($\Rightarrow$) Assume that G is abelian.

Surjectivity: Let $g \in G$. Then $\phi(g^{-1}) = (g^{-1})^{-1} = g$.

Injectivity: Let $x, y \in G$ be such that $\phi(x) = \phi(y) \Rightarrow x^{-1} = y^{-1} \Rightarrow x = y$

Homomorphism: Let $x, y \in G$. $\phi(xy) = (xy)^{-1} = y^{-1}x^{-1} \underbrace{=}_{G \text{ abelian}} x^{-1}y^{-1} = \phi(x)\phi(y)$

($\Leftarrow$) Assume that $\phi : G \to G$ is an isomorphism. Let $a, b, \in G$. We want to show that $ab = ba$.

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

Exercise 24.12. Show that isomorphism preserves the order of elements. i.e. that if $\phi : G \to H$ is an isomorphism and $a \in G$, then $|a| = |\phi(a)|$.

Proof. Assume that $|a| = n$ and $|\phi(a)| = m$.

We know that $\phi(a)^n = \phi(a^n) = \phi(id) = id$. Then $m|n$, in particular $m \leq n$. Now assuming that $m < n$:
$$id = \phi(a)^m = \phi(a^m) \Rightarrow a^m = id$$
This is a contradiction because $|a| = n > m$. Therefore $m = n$. $\square$

Exercise 24.13. Find an isomorphism between $U(12)$ and a subgroup of S_4.

$$U(12) = \{1, 5, 7, 11\}$$

Begin by learning about the elements in the set: $|5| = 2, \quad |7| = 2, \quad |11| = 2, \quad 5 \cdot 7 = 11.$

Remark 24.14. Isomorphisms are not necessarily unique.

Theorem 24.15
$\mathbb{Z}_{nm} \cong \mathbb{Z}_n \times \mathbb{Z}_m \Leftrightarrow \gcd(n, m) = 1$.

Corollary 24.16
You can do prime decomposition on $\mathbb{Z}_n$. This decomposes it into simple groups.

Example 24.17
Are the following isomorphic?

(a) $\mathbb{Z}_{14} \times \mathbb{Z}_4 \times \mathbb{Z}_5$ and $\mathbb{Z}_{10} \times \mathbb{Z}_{28}$

(b) $\mathbb{Z}_3 \times \mathbb{Z}_{16} \times \mathbb{Z}_9$ and $\mathbb{Z}_{27} \times \mathbb{Z}_2 \times ZZ_8$

§25 Simple Groups

Definition 25.1. A group G with no normal subgroups except G and $\{1_G\} = \{e\}$ is called simple.

Example 25.2

1. $\mathbb{Z}_p$ with p prime. The only subgroups are G and $\{1_G\}$.
2. $A_n \quad \forall n \geq 5$.

In some sense, simple groups are like the primes. Every group can be built from simple groups.

§26 Homomorphisms

Definition 26.1. A homomorphism from group $(G, \cdot)$ to $(H, \circ)$ is a map $\phi : G \to H$ such that is preserves multiplication. i.e. $\phi(g_1 \cdot g_2) = \phi(g_1) \circ \phi(g_2)$ for all $g_1, g_2 \in G$.

The range $\phi(G) \subset H$ is called the homomorphic image of G.

Remark 26.2. $\phi(G)$ is a subgroup of H.

Note 26.3. All isomorphisms are homomorphisms with the additional property that ϕ is a bijection.

Example 26.4
Let $g \in G$. There is a homomorphism $\phi : \mathbb{Z} \to G$ defined by $\phi(n) = g^n$.

Check: (review how binary operations apply below)

$$\phi(a + b) = g^{a+b} = g^a g^b = \phi(a)\phi(b)$$
$$\phi(\mathbb{Z}) = \langle g \rangle \subset G$$

Example 26.5

$$\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^*$$
$$\det(AB) = \det(A) \cdot \det(B)$$

Example 26.6

Let $G =$ the isometries of a tetrahedron.

$\phi : G \to \{\pm 1\}$. $\phi(g) = \pm 1$ if g preserves orientation. $\phi(g) = -1$ if g reverses orientation.

Theorem 26.7
Let $\phi : G_1 \to G_2$ be a homomorphism.

1. If e_1 is the identity element of G_1, the $\phi(e_1)$ is the identity element of G_2.
2. $\phi(g^{-1}) = [\phi(g)]^{-1}$
3. $H_1 \subset G_1$ is a subgroup $\Rightarrow \phi(H_1) \subset G_2$ is a subgroup
4. $H_2 \subset G_2$ is a subgroup $\Rightarrow \phi^{-1}(H_2) \subset G_1$ is a subgroup
5. $H_2 \subset G_2$ is a normal subgroup $\Rightarrow \phi^{-1}(H_2) \subset G_1$ is a normal subgroup

Note 26.8. Normal groups can be used to build factor and quotient groups.

Proof. Of the above statements.

1. $\phi(e_1) = \phi(e_1 e_1) = \phi(e_1)\phi(e_1)$. Therefore $e_2 = \phi(e_1)$.
2. $e_2 = \phi(e_1) = \phi(g \cdot g^{-1}) = \phi(g) \cdot \phi(g^{-1})$. Therefore $\phi(g)$ and $\phi(g^{-1})$ are inverse to one another.
3. Identity: $e_1 \in H_1 \Rightarrow e_2 = \phi(e_1) \in \phi(H_1)$, so image of ϕ contains identity element.

   Inverses: $g_2 \in \phi(H_1) \Rightarrow g_2 = \phi(g_1)$ for some $g_1 \in H_1 \Rightarrow g_1^{-1} \in H_1 \Rightarrow \phi(g^{-1}) = [\phi(g_1)]^{-1} = g_2^{-1} \in \phi(H_1)$. Therefore image contains inverses.

   Closure: Let $g_2, g_2' \in \phi(H_1)$. Therefore $\exists g_1, g_1' \in H_1$ such that $g_2 = \phi(g_1)$ and $g_2' = \phi(g_1')$. Therefore:

   $$g_1 g_1' \in H_1 \Rightarrow \phi(g_1 g_1') \in \phi(H_1) \Rightarrow g_2 g_2' = \phi(g_1)\phi(g_1') \in \phi(H_1)$$

4. Identity: $e_1 \in \phi^{-1}(H_2)$ because $\phi(e_1) = e_2 \in H_2$.

   Inverses: $g_1 \in \phi^{-1}(H_2) \Rightarrow g_1^{-1} \in \phi^{-1}(H_2)$ because $\phi(g_1^{-1}) = [\phi(g_1)]^{-1} \in H_2$.

   Closure: $g_1, g_1' \in \phi^{-1}(H_2) \Rightarrow g_1 g_1^{-1} \in \phi^{-1}(H_2)$ because $\phi(g_1 g_1') = \phi(g_1)\phi(g_1') \in H_2$

5. Show that for all $g_1 \in G_1$, $g_1 \phi^{-1}(H_2) g_1^{-1} \subset \phi^{-1}(H_2)$

   Let $k \in \phi^{-1}(H_2)$. Then $\phi(g_1 k g_1^{-1}) = \phi(g_1)\phi(k)\phi(g_1^{-1}) = \phi(g_1)\phi(k)[\phi(g_1)]^{-1} \in H_2$. Since we construct with $H_2 \subset G_2$ is normal. Remember that $\phi(k) \in H_2$.

□

§27 Kernal

Definition 27.1. The <u>kernel</u> of the homomorphism $\phi : G \to K$ is the pre image of the identity element. i.e. $\phi^{-1}(\{e\})$.

Theorem 27.2

The kernel of $\phi : G \to H$ is a normal subgroup of G.

Proof. Special case of Thm 11.4 □

Example 27.3

$\ker(\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^*) = \mathrm{SL}_n(\mathbb{R})$

Example 27.4

Let $g \in G$ be an element of order n. Let $\phi : \mathbb{Z} \to G$ be $\phi(p) = g^p$.

Which integers are going to map to the identity? Any integers that are multiplies of n. So $\ker(\phi) = n\mathbb{Z}$.

Example 27.5

Let N be a normal subgroup of G. The map $\phi : G \to G/N$ given by $\phi(g) = gN$ is a homomorphism. Indeed, $\phi(ab) = (ab)N = aNbN = \phi(a)\phi(b)$.

Note 27.6. This is the natural or canonial homomorphism.

Theorem 27.7 (First isomorphism theorem.)

Let $\psi G \to H$ be a homomorphism. Let N be the kernel of ϕ. Let $\phi : G \to G/N$ be canonical homomorphism. Then there exists an isomorphism $f : G/N \to \psi(G)$ such hat $\psi = f \circ \phi$.

$f(xN) = \psi(x)$. (f is well defined).

Example 27.8

Let $g \in G$, and $\psi(p) = g^p$. We know that if $|g| = n$, then $\ker(\psi) = n\mathbb{Z}$.

$\langle g \rangle = \psi(\mathbb{Z}) \subset G$.

$Z/n\mathbb{Z}$ is a cyclic group of order n and is therefore isomorphic to $\langle g \rangle = \psi(\mathbb{Z})$ which is also a cyclic group of order n.

Lemma 27.9

If $f : A \to B$ and $g : B \to C$ are homomorphisms, then $g \circ f : A \to C$ is a homomorphism.

Proof.

$$g \circ f(a_1 a_2) = g(f(a_1 a_2)) = g(f(a_1)f(a_2)) = g(f(a_1))g(f(a_2))$$

□

Example 27.10
$\phi : A \times B \to A$. $\phi((a,b)) = a$ is a homomorphism.

Check: $\phi((a_1, b_1)(a_2, b_2)) = \phi((a_1 a_2, b_1 b_2)) = a_1 a_2 = \phi(a_1, b_1)\phi(a_2, b_2)$

$\ker(\phi) = \{(e, b) : b \in B\} = \{e\} \times B \subset A \times B$.

Example 27.11

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_2$$

$\phi(a, b, c) = (a + b + c) \mod 2$. Kernel of ϕ is $\{(0,0,0), (1,0,1), (0,1,1), (1,1,0)\} = N$.

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 / N \cong \mathbb{Z}_2$$

Example 27.12
ϕ :Isometries of a cube$\to S_3 =$ permutations (x, y, z)

$\phi(g) =$ permutations of axes determined by ϕ.

Kernel of $\phi \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

§28 10-30

§28.1 Classification of finitely generated abelian groups

Definition 28.1. A group G is generated by a subset of its elements $\{g_1, g_2, \dots\}$ if $\{g_1, g_2, \dots\}$ is not contained in any proper subgroup.

Equivalently, every element $h \in G$ can be expressed as $h = x_1 x_2 x_3 \dots x_n$ where each $x_i \in \{g_1^{\pm 1}, g_2^{\pm 2}, \dots\}$.

Note 28.2. We then write $G = \langle g_1, g_2, \dots \rangle$

Example 28.3

1. $\mathbb{Z} = \langle 1 \rangle = \langle 2, 3 \rangle$
2. $S_n = \langle (ij) : i \neq j \rangle$

Definition 28.4. G is finitely generated if $G = \langle g_1, \dots, g_n \rangle$ for some finite set $\{g_1, \dots, g_n\}$.

Example 28.5

1. Every finite group is finitely generated because it is generated by the group itself.
2. $\mathbb{R}$ is not finitely generated because it is uncountable.
   Finitely generated $\Rightarrow$ countable.
3. Any finitely generated subgroup of $\mathbb{R}$ is isomorphic to $\mathbb{Z}^m$ for some $m \geq 0$.
$$\langle \sqrt{2}, \pi, e \rangle \cong \mathbb{Z}^3$$
4. $\mathbb{Q}$ is not finitely generated. Every subgroup of $\mathbb{Q}$ is infinite cyclic.
5. $\underbrace{\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots}_{\infty}$ is not finitely generated.

Theorem 28.6 (Fundamental theorem of finitely generated abelian groups.)
Let G be a finitely generated abelian group. Then G is isomorphic to a product of infinitely many cyclic groups (finite or infinite).

Example 28.7

$$G \cong \underbrace{\mathbb{Z} \times \mathbb{Z} \times \cdots}_{m \geq 0} \times \underbrace{\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}}_{k \geq 0}$$

Moreover,
$$G \cong \mathbb{Z}_0^m \times \underbrace{\mathbb{Z}_{p_1^{m_1}} \times \mathbb{Z}_{p_2^{m_2}} \times \cdots \times \mathbb{Z}_{p_k^{m_k}}}_{k \geq 0}$$

where each p_i is prime. Moreover, decomposition is unique up to permuting factors.

Example 28.8
What are all possible abelian groups of order $1000 = 2^3 \cdot 5^3$.

$$\mathbb{Z}_{5^3} \times \mathbb{Z}_{2^3}$$
$$\mathbb{Z}_{5^3} \times \mathbb{Z}_{2^2} \times \mathbb{Z}_{2^1}$$
$$\mathbb{Z}_{5^3} \times \mathbb{Z}_{2^1} \times \mathbb{Z}_{2^1} \times \mathbb{Z}_{2^1}$$
$$\mathbb{Z}_{5^2} \times \mathbb{Z}_{5^1} \times \mathbb{Z}_{2^3}$$
$$\mathbb{Z}_{5^2} \times \mathbb{Z}_{5^1} \times \mathbb{Z}_{2^2} \times \mathbb{Z}^{2^1}$$
$$\mathbb{Z}_{5^2} \times \mathbb{Z}_{5^1} \times \mathbb{Z}_{2^1} \times \mathbb{Z}_{2^1} \times \mathbb{Z}^{2^1}$$
$$\mathbb{Z}_{5^1} \times \mathbb{Z}_{5^1} \times \mathbb{Z}_{5^1} \times \mathbb{Z}_{2^3}$$
$$\mathbb{Z}_{5^1} \times \mathbb{Z}_{5^1} \times \mathbb{Z}_{5^1} \times \mathbb{Z}_{2^2} \times \mathbb{Z}_{2^1}$$
$$\mathbb{Z}_{5^1} \times \mathbb{Z}_{5^1} \times \mathbb{Z}_{5^1} \times \mathbb{Z}_{2^1} \times \mathbb{Z}_{2^1} \times \mathbb{Z}_{2^1}$$

§29 Tutorial 2019-11-01. Normal Subgroups and Quotient Groups

§29.1 Normal Subgroups

$N \subseteq G$ is normal if $gN = Ng, \quad \forall g \in G$. Equivalently $gNg^{-1} \subseteq N$ and $gNg^{-1} = N$.

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

Prooving that gNg^{-1} is a subgroup.

Identity: $e \in N \Rightarrow$

$$geg^{-1} = gg^{-1} = e \in gNg^{-1}$$

Inverses: $gng^{-1} \in gNg^{-1}$. $(gng^{-1})^{-1} = gn^{-1}g^{-1}$. $n \in N$ so $gn^{-1}g^{-1} \in gNg^{-1}$

Closure: $gn_1g^{-1}, gn_2g^{-1} \in gNg^{-1}$

$$gn_1g^{-1}gn_2g^{-1} = gn_1n_2g^{-1}$$

$n_1n_2 \in N$ so $gn_1n_2g^{-1} \in gNg^{-1}$ ✓

§29.2 Quotient Groups

Let $N \subseteq G$ be a normal subgroup. Then G/N is a group with the operation $(aN)(bN) = (ab)N$

Example 29.1

Let $G = \mathbb{Z}$. Let $N = 24\mathbb{Z} = \{0, 24, 48, \ldots\}$. $\mathbb{Z}/24\mathbb{Z} \cong \mathbb{Z}_{24}$

Example 29.2

$D_8 = \{id, r, \ldots, r^7, s, sr, \ldots, sr^7\}$
$N = \langle r^4 \rangle = \{id, r^4\}$ is a normal subgroup.
$|D_8/N| = 16/2 = 8$. Finding all the cosets of N :

$$\begin{aligned} id \cdot N, &\quad sN \\ r \cdot N, &\quad srN \\ r^2 \cdot N, &\quad sr^2N \\ r^3 \cdot N, &\quad sr^3N \end{aligned}$$

Exercise 29.3. Let G be a cyclic group where $G = \langle a \rangle$. Show that G/N is cyclic.

Claim: $G/N = \langle aN \rangle$.

Let $bN \in G/N$. $b \in G$, so $b = a^k$ for some k. $bN = a^kN = (aN)^k \Rightarrow g/N = \langle aN \rangle$.

Remark 29.4. Let G be a group, and $H, K \subseteq G$ be subgroups of G such that $H \subseteq K \subseteq G$. Then H being normal in K and K being normal in G does NOT imply that H is normal in G.

Example 29.5

Consider the following:

$$D_4 = \{id, r, r^2, r^3, \mu_1, \mu_2, \mu_3, \mu_4\}$$
$$K = \{id, \mu_1, \mu_3, r^2\}$$
$$H = \{id, \mu_1\}$$

Show that K is normal in D_4, and that H is normal in K, but that H is not normal in D_4.

Note 29.6. Tips for determining wether or not H is normal in G:

1. If G abelian, then all of its subgroups must be normal.
2. If G is simple, then it has no normal non-trivial proper subgroups.
3. If $[G : H] = 2$, then H is normal (we proved this in a previous assignment).
4. If all else fails, compute

$[D_4 : K] = 2$ so K is normal in D_4. $[K : H] = 4/2 = 2$ so H is normal in K.

Now to show that H is not normal in D_4 with a counter example.

$$\mu_1 = (24)$$
$$H = \{(), (24)\}$$
$$r = (1234) \in D_4$$
$$rH = \{(1234, (12)(34)\}$$
$$Hr = \{(1234), (14)(23)\}$$

Therefore $rH \neq Hr \Rightarrow H$ is not normal in D_4.

Exercise. Let G be a group, and $N \subseteq G$ be a normal subgroup. Let $gN \in G/N$.

(a) Show that $|gN| = n$ in G/N where n is the smallest natural number such that $g^n \in N$.
Observe that $(gN)^n = g^nN = eN \Leftrightarrow g^n \in N$. Therefore the order of (gN) is the smallest of $n \in \mathbb{N}$ such that $g^n \in N$.

(b) Give an example where $|gN|$ in G/N is strictly smaller that $|g|$ in G.
Let $G = \mathbb{Z}_4 = \{0, 1, 2, 3\}$
Let $N = \langle 2 \rangle = \{0, 2\}$
Elements of G/N:

$$0 + N = \{0, 2\} = 2 + N$$
$$1 + N = \{1, 3\} = 3 + N$$

$$\mathbb{Z}/3\mathbb{Z} =$$
$$0 + 3\mathbb{Z} = \{0, 3\}$$
$$1 + 3\mathbb{Z} = \{1, 4\}$$
$$2 + 3\mathbb{Z} = \{2, 5\}$$

§30 2019-11-01 Rings

Definition 30.1. A ring is a set R with two binary operations.

1. (+ is associative): $(a+b)+c = a+(b+c)$
2. There is an additive identity element $0 \in R$ such that $a+0 = a = 0+a$ for all $a \in R$.
3. Each $a \in R$ has an additive inverse $-a$ such that $a + -a = 0 = -a + a$
4. $+$ is commutative: $a+b = b+a$ for all $a, b \in R$.
5. Multiplication is associative: $a \cdot (bc) = (ab) \cdot c$
6. Left / right distributive: $a \cdot (b+c) = a \cdot b + a \cdot c$ and $(a+b) \cdot c = a \cdot c + b \cdot c$

Definition 30.2. If R has a multiplicative identity element $1 \neq 0$ such that $1a = a = a1\ \forall a$ then R is a ring with unity / identity

If multiplication is commutative, R is a commutative ring.

If R is commutative with 1 and $(ab = 0) \Rightarrow (a = 0 \text{ or } b = 0)$, then R is an integral domain

If R has the identity element and every $x \neq 0$ has a multiplicative inverse in R then R is a division ring. i.e. $(R - \{0\}, \cdot) = (\mathbb{R}^*, \cdot)$ is a group.

If $(R^*, \cdot)$ is a commutative group then R is a field.

Example 30.3

$$\text{Integral domain: } (\mathbb{Z}, +, \cdot)$$
$$\text{Fields: } (\mathbb{R}, +, \cdot), (\mathbb{Q}, +, \cdot), (\mathbb{C}, +, \cdot)$$
$$\text{Commutative Ring: } (\mathbb{Z}_n, +, \cdot)$$
$$(\mathbb{Z}_p, +, \cdot) \text{ is a field because } a^{p-1} \equiv_p 1 \text{ for } a \neq 0 \text{ so } (a)(a^{p-2}) \text{ are inverses.}$$

$\mathbb{Z}_n$ is not a field when $n > 1$ is not prime. One example is $3 \in \mathbb{Z}_6$ which doesn't have a multiplicative inverse. $\mathbb{Z}_n$ is also not an integral domain when n is not prime. e.g. $3 \cdot 2 \equiv_6 = 0$ even though neither 3 nor 2 are equal to 0.

$\mathbb{Z}_1$ is commutative and $ab = 0 \Rightarrow a = 0$ or $b = 0$ but not a ring with unity because unity must be satisfied by an element other than the additive identity element. There is only one element so this is not possible.

Definition 30.4. A non zero element $a \in R$ such that $ab = 0$ but $b \neq 0$ is a zero divisor. A unit $u \in R$ is an element with a multiplicative inverse.

Definition 30.5. $\mathbb{Z}[x]$ is a ring of all polynomials with integer coefficients.
A polynomial $a_n x^n + a_{n-1}^{n-1} + \cdots = a_1 x^1 + a_0$ has degree n if $a_n \neq 0$ has degree n if $a_n \neq 0$. Add polynomials by corresponding coefficients. Multiply by multiplying and

then combining like terms.

$\mathbb{Z}[x]$ is an integral domain! It's commutative, it has unity, and there is no way to multiply two non zero polynomials and get 0.

§31 11-04

Definition 31.1. An element $a \in \mathbb{R}$ is a zero-divisor if $\exists b \neq 0$ such that $ab = 0$ or $ba = 0$. You can get more specific and declare a left zero-divisor or a right zero-divisor.

Definition 31.2. $u \in \mathbb{R}$ is a unit if u has a multiplicative inverse.

Lemma 31.3

Let R be a ring with unity. The set $U(R) = \mathbb{R}^*$ of units of R forms a group using multiplication.

Note 31.4. Some people assume that when you say a ring, it means a ring with unity.

Recall 31.5. $\mathbb{Z}[x]$ is a ring of polynomials. Variable is x with coefficients in $\mathbb{Z}$.

Lemma 31.6

$\mathbb{Z}[x]$ is an integral domain. Because it is commutative, includes the identity element, and when $ab = 0$, either $a = 0$ or $b = 0$.

Lemma 31.7

$\mathbb{Z}_p[x]$ is integral domain when p is prime.

Example 31.8

$$\mathbb{Z}_6[x] = \{2x^5 + 3x^4 + 5x^3 + 1x^2 + 0x^1 + 4x^0, \cdots\}$$
$$(2x + 2)(3x + 3) = 0$$

So $\mathbb{Z}_6[x]$ is not an integral domain. In general, $\mathbb{Z}_n[x]$ is not an integral domain when n is composite.

Definition 31.9. $M_{n\times n}(\mathbb{R})$ is the set of $n \times n$ matrices with real coefficients. Addition and multiplication of matrices as defined in linear algebra.

$$1 = I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Note that this ring is not an integral domain because it contains zero divisors.

$$\underbrace{\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}}_{\text{Zero divisors}} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Note 31.10. $U(M_{n\times n}(\mathbb{R})) = \mathrm{GL}_n(\mathbb{R})$

Note 31.11. $M_{n\times n}(\mathbb{Z}_m)$ has m^{n^2} elements and works very nicely when n is prime.

Example 31.12

$$M_{2\times 2}(\mathbb{Z}_2) =$$
$$\{\begin{pmatrix}1&1\\0&1\end{pmatrix},\begin{pmatrix}1&1\\1&1\end{pmatrix},\begin{pmatrix}1&0\\1&0\end{pmatrix},\begin{pmatrix}1&1\\0&0\end{pmatrix},\begin{pmatrix}1&0\\1&1\end{pmatrix},\begin{pmatrix}0&1\\1&0\end{pmatrix},\begin{pmatrix}1&0\\0&0\end{pmatrix},\begin{pmatrix}0&0\\0&1\end{pmatrix},$$
$$\begin{pmatrix}0&0\\0&0\end{pmatrix},\begin{pmatrix}1&0\\0&1\end{pmatrix},\begin{pmatrix}0&0\\1&1\end{pmatrix},\begin{pmatrix}0&1\\0&1\end{pmatrix},\begin{pmatrix}1&1\\1&0\end{pmatrix},\begin{pmatrix}0&1\\1&1\end{pmatrix},\begin{pmatrix}0&1\\0&0\end{pmatrix},\begin{pmatrix}0&0\\1&0\end{pmatrix}\}$$
$$\text{Example of multiplication: }\begin{pmatrix}1&1\\0&1\end{pmatrix}\begin{pmatrix}1&0\\1&0\end{pmatrix}=\begin{pmatrix}0&0\\1&0\end{pmatrix}$$

Note 31.13. Each element is its own additive inverse.

$$(M_{2\times 2}(\mathbb{Z}_2),+) \cong \mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$$

Definition 31.14. The "real-quaternions" $\mathbb{R}Q$ forms a division ring that isn't a field (because it isn't commutative).

$$\mathbb{R}Q = \{a_1 + bi + cj + dk : a,b,c,d \in \mathbb{R}\}$$

Addition and multiplication works like in $\mathbb{C}$. Let scalars commute with i, j, k.

$$\begin{aligned} i^2 = j^2 = k^2 &= -1 \\ ij = k \quad & ji = -k \\ jk = i \quad & kj = -i \\ ki = j \quad & ik = -j \end{aligned}$$

There is crazy algebra to show that:

$$(a+bi+cj+dk)(a-bi-cj-dk) = a^2+b^2+c^2+d^2$$

Hence when $a^2+b^2+c^2+d^2 \neq 0$, we get the following:

$$(a+bi+cj+dk)^{-1} = \frac{a-bi-cj-dk}{a^2+b^2+c^2+d^2}$$

Proposition 31.15 (16.8)
Let R be a ring and let $a, b \in R$.

1. $a0 = 0 = 0a$
2. $a(-b) = (-a)(b) = -(ab)$
3. $(-a)(-b) = ab$

Proof.

1. $a0 = a(0+0) = a0 + a0 \Rightarrow 0 = a0$
   $0a = (0+0)a = 0a + 0a \Rightarrow 0 = 0a$
2. $0 = a0 = a(b + -b) = ab + a(-b)$ so $-(ab)$ is the additive inverse of $a(-b)$ i.e. $-(ab) = a(-b)$.
   Similarly, $(-a)(b) = -(ab)$ because $0 = 0b = (a + -a)b = ab + (-a)b \Rightarrow -(ab) = (-a)(b)$
3. $(-a)(-b) = -(-(a)b) = -(-(ab))$. But $-(-ab) = ab$ because inverse of inverse is itself. Note, use notation $a - b = a + -b$.

□

§32 11-06

Definition 32.1. A subring of a ring is a subset $S \subseteq R$ such that $(S, +, \cdot)$ is itself a ring (some operations are restricted).

Example 32.2
$5\mathbb{Z} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$

Proposition 32.3
A subset $S \subseteq R$ is a ring if and only if:

1. $S \neq \varnothing$
2. Let $x, y \in S$, then $x - y \in S$. (If this is true, then the set contains the identity element, whenever an element is inside its inverse is inside, whenever two elements are in S its product is in S. This is just a faster way of showing these).
3. Let $x, y \in S$, then $x \cdot y \in S$.

What about associativity and distributive, etc? Those properties are inherited from the ring.

Example 32.4

$$2\mathbb{Z}_{10} \subseteq \mathbb{Z}_{10}$$
$$\{0, 2, 4, 6, 8\} \subset \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

Yes, this is a subring but it does not have unity because it does not include "1".

$$S \neq \varnothing, \qquad x - y \in S, \qquad x \cdot y \in S$$

Example 32.5

$$\mathbb{Z}[x^2] \subseteq \mathbb{Z}[x]$$
$$\mathbb{Z}[x^2] = \{a_{2n}x^{2n} + a_{2(n-1)}x^{2(n-1)} + \cdots + a_0x^0\}$$

i.e. $\mathbb{Z}[x^2]$ represents polynomials where the odd polynomial coefficients are 0.

Yes, this is a subring and it has unity because it contains "1", the identity element.

$$S \neq \varnothing, \qquad x - y \in S, \qquad x \cdot y \in S$$

Example 32.6

$$T_{n\times n}(\mathbb{R}) \subset M_{n\times n}(\mathbb{R})$$

$T_{n\times n}(\mathbb{R})$ which represents upper triangular matrices. i.e. zeros bellow diagonal.

$$\begin{bmatrix} * & * & * & * \\ 0 & * & * & * \\ 0 & 0 & * & * \\ 0 & 0 & 0 & * \end{bmatrix}$$

Yes a subring.

§32.1 Integral domains and fields

Definition 32.7. The subring $\mathbb{Z}[i] \subset \mathbb{C}$ consisting of $\{m + ni : m, n \in \mathbb{Z}\}$ is the Gaussian Integers.

Remark 32.8. Not every Gaussian Integer is a unit in the Gaussian Integers. Indeed, ± 1 and $\pm i$ are the only units. Proof:

Suppose $\alpha, \beta \in \mathbb{Z}[i]$, and $\alpha\beta = 1$ where $\alpha = a_1 + a_2 i$ and $\beta = b_1 + b_2 i$. Remember that for $z_1 = a_1 + b_1 i$ and $z_2 = a_2 + b_2 i$:

$$\overline{z_1 z_2} = \overline{z_1} \cdot \overline{z_2}$$

Then if follows that

$$1 = 1 \cdot 1 = (\alpha\beta)(\overline{\alpha\beta}) = (\alpha\beta)(\overline{\alpha}\overline{\beta}) = (\alpha\overline{\alpha})(\beta\overline{\beta}) = (a_1^2 + a_2^2)(b_1^2 + b_2^2)$$

Hence $(a_1^2 + a_2^2) = \pm 1$ and $(b_1^2 + b_2^2) = \pm 1$.

$\mathbb{Z}[i]$ is an integral domain since it is the subring of a field with unity which implies that the subring is an integral domain.

$$xy = 0 \Rightarrow x = 0 \vee y = 0$$

because $x^{-1}xy = x^{-1}0 \Rightarrow y = 0$.

Example 32.9

$\mathbb{Z}_p$ is a field with p elements.

Theorem 32.10

There exista a field with p^n elements for each $n \geq 1$ when p is prime.

Example 32.11

$$M_{2\times 2}(\mathbb{Z}_2) \supset \mathbb{F}_4 = \{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\}$$

is a field with 2^2 elements.

Proposition 32.12

Let D be a commutative ring with "1" i.e. unity.

Then D is an integral domain if and only if for all non zero $a \in D$, $(ab = ac) \Rightarrow (b = c)$

Proof.

$(\Rightarrow)$

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

$(\Leftarrow)$

$$ab = 0 \Rightarrow ab = a0 \Rightarrow b = 0 \text{ because } a \neq 0$$

□

§33 Tutorial 11-08

§33.1 Homomorphisms

$\varphi : G \to H$. Then $\varphi(xy) = \varphi(x) \cdot \varphi(y)$. Intuitively thing of a homomorphism as recovering some of the structure of one group in another group.

Theorem 33.1 (1st Isomorphism Theorem)

Let $\varphi : G \to H$ be a homomorphism. Then

$$N = \ker(\varphi) = \{x \in G | \varphi(x) = e_H\}$$

Note that N is normal in G, that $\varphi(G)$ is a subgroup of H and that $G/N \cong \varphi(G)$.

Example 33.2

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

where $\varphi(a) = (a, 0)$. Therefore $\ker(\varphi) = \{0\}$, the trivial subgroup.

Example 33.3

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

where $\varphi(a, b) = a$. $\ker(\varphi) = \{(0, b) : b \in \mathbb{Z}\}$. This is a non trivial kernel.

Thus $\mathbb{Z} \cong \mathbb{Z}^2 / \ker(\varphi)$ by the 1st Isomorphism Theorem.

Exercise 33.4. Let A be an $n \times m$ matrix. Then the map $\varphi(x) = Ax$ defines a homomorphism from $\mathbb{R}^n \to \mathbb{R}^m$.

Let $x, y \in \mathbb{R}^n$. Then $\varphi(x + y) = A(x + y) = Ax + Ay = \varphi(x) + \varphi(y)$

<u>Intution</u>: Multiplying by a matrix corresponds to applying a linear map (we could be scaling, rotating, projecting, etc).

Example 33.5

$$A = \begin{pmatrix} 4/5 & 2/5 \\ 2/5 & 1/5 \end{pmatrix}$$

Exercise 33.6.

$$\epsilon : S_n \to \{\pm 1\}$$

$$\epsilon(\sigma) = \begin{cases} 1, & \sigma \text{ composed of an even number of transpositions} \\ -1, & \sigma \text{ composed of an even number of transpositions} \end{cases}$$

<u>Homomorphism</u>: $\sigma, \tau \in S_n$,

$$\epsilon(\sigma\tau) = \begin{cases} 1, & \sigma\tau \text{ composed of an even number of transpositions} \\ -1, & \sigma\tau \text{ composed of an even number of transpositions} \end{cases}$$

$$\epsilon(\sigma\tau) = \begin{cases} 1, & \sigma \text{ \& } \tau \text{ both even or odd} \\ -1, & \text{Either } \sigma \text{ even and } \tau \text{ odd or } \sigma \text{ odd and } \tau \text{ even} \end{cases}$$

Therefore it works out that $\epsilon(\sigma\tau) = \epsilon(\sigma)\epsilon(\tau)$.

Example computation:

$$\sigma = (1\,2)$$
$$\tau = (1\,4)(3\,5)(1\,6)$$
$$\sigma\tau = (1\,2)(1\,4)(3\,5)(1\,6)$$
$$\epsilon(\sigma) \cdot \epsilon(\tau) = -1 \cdot -1 = 1 = \epsilon(\sigma\tau)$$

What is the kernel of ϵ? $\ker(\epsilon) = A_n$ (all the even permutations)

Therefore, by the 1st Isomorphism Theorem, $S_n/A_n \cong \{\pm 1\}$.

Exercise 33.7. Let $\varphi : G \to H$. Prove that φ is injective if and only if $\ker(\varphi) = \{e\}$.

Proof.

($\Rightarrow$) Let $g \in \ker(\varphi)$.

$$\varphi(g) = e = \varphi(e)$$

So therefore $g = e$ because φ is injective. Therefore the only element that maps to $\{e\}$ is e itself.

($\Leftarrow$) Assume that $\ker(\varphi) = \{e\}$ and let $g_1, g_2 \in G$ such that $\varphi(g_1) = \varphi(g_2)$. We want to show that $g_1 = g_2$.

$$\begin{aligned} \varphi(g_1) = \varphi(g_2) &\Rightarrow \varphi(g_1)(\varphi(g_2))^{-1} = e_H \\ &\Rightarrow \varphi(g_1)\varphi(g_2^{-1}) = e_H \\ &\Rightarrow \varphi(g_1 g_2^{-1}) = e_H \\ &\Rightarrow g_1 g_2^{-1} = e_G \\ &\Rightarrow g_1 = g_2 \end{aligned}$$

□

Intuitively this makes sense. If and only if φ is injective than we can recover everything from G. If and only if $\ker(\varphi) = \{e\}$ then we can recover everything from G. Therefore φ is injective if and only if $\ker(\varphi) = \{e\}$.

Exercise 33.8. Let $\phi : G \to H$, $N = \ker(\phi)$, $K \subseteq G$ is a subgroup. Show that $\phi^{-1}(\phi(K)) = KN$ where $KN = \{kn : k \in K, n \in N\}$.

Proof.

$$\begin{gathered} \text{Let } g \in \phi^{-1}(\phi(K)) \\ \Leftrightarrow \phi(g) = \phi(k) \text{ for some } k \in K \\ \Leftrightarrow \phi(g) \cdot \phi(k)^{-1} = \phi(gk^{-1}) = e \\ \Leftrightarrow gk^{-1} \in N \Rightarrow g \in kN \\ \Leftrightarrow g \in KN \end{gathered}$$

□

Exercise 33.9. Let $\varphi : G \to H$ where $G = \langle g \rangle$ i.e. G is cyclic. Show that φ is determined by $\varphi(g)$.

Proof. Let $g' \in G$. Then $g' = g^k$ for some k (we know this because of the properties of a generator).

$$\begin{gathered} \text{Fix } \varphi(g) = h. \text{ Then} \\ \varphi(g') = \varphi(g^k) = \varphi(g)^k = h^k. \end{gathered}$$

□

Remark 33.10. We can generalize this statement to groups that have finitely many generators.

Example 33.11
Try to find an Isomorphism between $U(20)$ and $U(16)$.

$$U(20) = \{1, 3, 7, 9, 11, 13, 17, 19\}$$
$$\langle 3 \rangle = \{3, 9, 7, 1\}$$
$$\langle 19 \rangle = \{19, 1\}$$
$$\langle 3 \rangle \times \langle 19 \rangle = U(20)$$

$$U(16) = \{1, 3, 5, 7, 9, 11, 13, 15\}$$
$$\langle 3 \rangle = \{3, 9, 11, 1\}$$
$$\langle 15 \rangle = \{15, 1\}$$
$$\langle 3 \rangle \times \langle 15 \rangle = U(16)$$

So fixing $\varphi(3) = 3, \varphi(19) = 15$ is a valid isomorphism.

§34 11-08

Proposition 34.1 (16.15)
For commutative ring with unity:

D is an integral domain $\Leftrightarrow$ for all nonzero $a \in D$, $ab = ac \Leftrightarrow b = c$

Theorem 34.2 (16.16)
Finite integral domain $\Rightarrow$ field.

Let $a \in D^* = D \setminus \{0\}$

Then $\varphi : D^* \to D^*$ where $\varphi(x) = ax$ for all $x \in D^*$.

φ is injective because $\varphi(x_1) = \varphi(x_2) \Rightarrow ax_1 = ax_2 \Rightarrow x_1 = x_2$

φ is surjective because $|D^*| < \infty$

Thus, $1 = \varphi(x)$ for some $x \in D^*$. Hence $ax = 1$ for some x, so a^{-1} exists.

Definition 34.3. The [Characteristic] of R is the smallest n such that $nr = 0$ for all $r \in R$. If there isn't such a smalest n, we say that R has characteristic 0.

Example 34.4

$\mathbb{Z}_n$ has characteristic n.

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ all have characteristic 0.

$\mathbb{F}_4$ has characteristic 2.

$$\mathbb{F}_4 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}$$

Lemma 34.5

If R is a ring with unity, then $\operatorname{char}(R)$ equals the smallest n such that $n_1 = 0$. i.e. the order of 1 is $(R, +)$.

"It is enough to find the additive order of the multiplicative identity element".

Proof.

$$nr = \underbrace{r + r + \cdots + r}_{n}$$

Let n denote n_1 for a ring with unity.

$$nr = (n1)r = 0r = 0$$

holds for all r! n is minimal with this property because $n = |1|$ in $(\mathbb{R}, +)$. □

Theorem 34.6

The characteristic of an integral domain is either 0 or p prime.

Proof. Suppose $\operatorname{char}(R)$ is $m = ab$ with $1 < a, b < m$.

Then $a1, b1 \neq 0$. But $(a1)(b1) = ab1 = m1 = 0$. Contradiction because this contradicts integral domain.

$$(n_1 r_1)(n_2 r_2) = n_1 n_2 (r_1 r_2)$$

□

§34.1 Ring Homomorphisms & Ideals

A ring homomorphism $\varphi : R \to S$ satisfies:

$$\varphi(a + b) = \varphi(a) + \varphi(b)$$
$$\varphi(ab) = \varphi(a)\varphi(b)$$

A bijective ring homomorphism is an <u>isomorphism</u>.

Example 34.7

$\varphi : \mathbb{Z} \to \mathbb{Z}_n$. $\varphi(a) = a \mod (n)$ is a homomorphism.

Proposition 34.8

Let $\varphi : R \to S$ be a homomorphism.

1. $\varphi(R)$ is a subring of S.
2. If R is commutative, then $\varphi(R)$ is commutative.
3. $\varphi(0) = 0$
4. If R and S are rings with unity 1_R and 1_S and φ is surjective, then $\phi(1_R) = 1_S$
5. If R is a field, then either $\varphi(R) = 0$ or $\varphi(R)$ is a field.

Proof.

3. $\varphi(0_R) = \varphi(0_R + 0_R) = \varphi(0_R) + \varphi(0_R)$ so $\varphi(0_R) = 0_S$
1. $0_S \in \varphi(R)$.

   $a, b \in \varphi(R) \Rightarrow a - b \in \varphi(R)$ because $a = \varphi(a')$ and $b = \varphi(b')$ for some $a', b' \in R$ so $a - b = \varphi(a') - \varphi(b') = \varphi(a' - b') \in \varphi(R)$

   Likewise, $ab = \varphi(a')\varphi(b') = \varphi(a'b') \in \varphi(R)$.
2. If $a'b' = b'a'$, then:

$$ab = \varphi(a')\varphi(b') = \varphi(a'b') = \varphi(b'a') = \varphi(b')\varphi(a') = ba$$

4. Let $x \in R$ such that $\varphi(x) = 1_S$. Then $1_S = \varphi(x) = \varphi(1_R x) = \varphi(1_R)\varphi(x) = \varphi(1_R)(1_S) = \varphi(1_R)$

$\square$

§35 11-11

Proposition 35.1

Let $\varphi : R \to S$ be a ring homomorphism.

1. R is commutative implies that $\varphi(R)$ is a commutative ring
2. If R and S have unity 1_R and 1_S and φ is surjective, then $\varphi(1_R) = 1_S$
3. If R is a field, then $\varphi(R) = \{0\}$ or $\varphi(R)$ is a field.

   Proof of 3. We know that $\varphi(R)$ is a commutative subring by (1). Let $a \in \varphi(R)$.

   $\varphi(1_R)$ is the multiplicative identity for $\varphi(R)$ so $a = \varphi(\hat{a})$ for some $\hat{a} \in R$.

   $$a \cdot \varphi(1_R) = \varphi(\hat{a})\varphi(1_R) = \varphi(\hat{a}1_R) = \varphi(\hat{a}) = a$$

   Similarly, $\varphi(1_R)a = a$.

   If $\varphi(x) \neq 0_S$, then $x \neq 0_R$. So $\exists x^{-1} \in R$ such that $xx^{-1} = 1_R$.

   $$\varphi(x) \cdot \varphi(x^{-1}) = \varphi(xx^{-1}) = \varphi(1_R)$$

   So $\varphi(x^{-1})$ equals $(\varphi(x))^{-1}$.

   Either $\varphi(R) = \{0\}$, or it doesn't.

   If $\varphi(1_R) \neq 0_S$, we are done.

   If $\varphi(1_R) = 0_S$, then $\varphi(R) = \{0\}$ because for each $a \in \varphi(R)$, $a = \varphi(\hat{a})$ for some $\hat{a} \in R$. Therefore:

   $$a = \varphi(\hat{a}) = \varphi(\hat{a}1_R) = \varphi(\hat{a})\varphi(1_R) = a \cdot 0_S = 0$$

   Recall 35.2. Being a field is a stronger property than being an integral domain. When every element has a multiplicative inverse, it must be an integral domain.

   □

§35.1 Ideals

Definition 35.3. An ideal I in ring R is a subring $I \subset R$ such that if $x \in I$ and $r \in R$, then $xr \in I$ and $rx \in I$.

Example 35.4

$\{0\} \subseteq R$ and $R \subseteq R$ are ideals.

Example 35.5

If $a \in R$ is a commutative ring, then $\langle a \rangle = \{ar : r \in R\}$ is an ideal.

$\langle a \rangle$ is a principal ideal.

Proof.
Prooving that $\langle a \rangle$ is a subring:

$\langle a \rangle$ is non empty because $0 = 0a \in \langle a \rangle$.

$r_1 a, r_2 a \in \langle a \rangle \Rightarrow r_1 a \cdot r_2 a = (r_1 \cdot r_2)a \in \langle a \rangle$.

$(ar_1)(ar_2) = a(r_1 a r_2) = ar_3 \in \langle a \rangle$.

Prooving that $\langle a \rangle$ is an ideal:

$$x \in \langle a \rangle \Rightarrow rx \in \langle a \rangle$$

because $x = as$ for some $s \in R$. Therefore $rx = r(as) = a(rs) \in \langle a \rangle$. □

Theorem 35.6

Every ideal in $\mathbb{Z}$ is $\langle n \rangle$ for some n.

Proposition 35.7

The kernel of a ring homomorphism $\varphi : R \to S$ is an ideal of R.

Proof. $K = \ker(\varphi)$ is an additive subgroup.

We must check that $k \in K \Rightarrow rk \in K$ and $kr \in K$ for all $r \in R$.

$rk \in K$ because $\varphi(rk) = \varphi(r)\varphi(k) = \varphi(r)0 = 0$

$kr \in K$ because $\varphi(kr) = \varphi(k)\varphi(r) = 0\varphi(r) = 0$

□

Theorem 35.8
Let I be an ideal of R. The factor group R/I is a ring with multiplication!

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

Proof. Check that it is well defined. i.e. that if $a+I = a'+I$ and $b+I = b'+I$, then we need $(a+I)(b+I) = (a'+I)(b'+I)$.

Let $a' = a+\alpha$ where $\alpha \in I$, and let $b' = b+\beta$ where $\beta \in I$. Then:

$$a'b' = (a+\alpha)(b+\beta) = ab + a\beta + \alpha b + \alpha\beta$$

$ab + a\beta + \alpha b + \alpha\beta \in ab + I$ because $a\beta + \alpha b + \alpha\beta \in I$. Therefore $a'b' + I = ab + I$ $\square$

Theorem 35.9 (1st Isomorphism Theorem for Rings)
Let $\varphi : R \to S$ be a homomorphism.

Let $I = \ker(\varphi)$.

Let $\phi : R \to R/I$.

Then there exists $\nu : R/I \to \varphi(R)$ such that $\varphi = \nu \circ \phi$.

§36 Lecture 11-13

Definition 36.1. Let I be an ideal of R. Then $\phi : R \to R/I$ is a canonical homomorphism associated to I.

$$\begin{aligned} \phi(r) &= r + I \\ \phi(xy) &= xh + I \\ \phi(x)\phi(y) &= (x+I)(y+I) \end{aligned}$$

§36.1 Maximal and Prime Ideals

Definition 36.2. An ideal $M \subseteq R$ is maximal if the only ideal larger than M is R itself.

i.e. There does not exist ideal I with $M \subsetneq I \subsetneq R$.

Definition 36.3. An ideal $P \subsetneq R$ where R is commutative is prime if for all $a, b \in R$, $ab \in P \Rightarrow [a \in P \text{ or } b \in P]$.

Example 36.4

A proper ideal $n\mathbb{Z} \subset \mathbb{Z}$ is maximal $\Leftrightarrow$ $n\mathbb{Z} \subset \mathbb{Z}$ is prime $\Leftrightarrow$ n is a prime number. Reasoning:

$n\mathbb{Z} \subsetneq m\mathbb{Z} \subsetneq \mathbb{Z}$ if and only if $m|n$ but $m \neq 1$ and $m \neq n$ i.e. n is not prime.

$(ab \in n\mathbb{Z}) \Leftrightarrow n|(ab)$ but if n is prime then $n|(ab) \Leftrightarrow n|a$ or $n|b$. Hence $a \in n\mathbb{Z}$ or $b \in n\mathbb{Z}$.

If n is not prime, then $n = xy$ where $1 < x, y < n$ and $xy \in n\mathbb{Z}$ but $x \notin n\mathbb{Z}$ and $y \notin n\mathbb{N}$. This would mean that $n\mathbb{Z}$ is not prime.

Example 36.5

In $\mathbb{Z}[x]$, the ideal $\langle x \rangle$ is prime but not maximal.

Maximal Proof:

$\langle x \rangle$ is not maximal because $\langle x \rangle \subsetneq \langle x, 2 \rangle \subsetneq \mathbb{Z}[x]$

$\langle x, 2 \rangle$ consists of all polynomials of the form $f \cdot x + g \cdot 2$ (where $f, g \in \mathbb{Z}[x]$). i.e. all polynomials whose consant term is even.

$\langle x \rangle$ consists of all polynomials of the form $f \cdot x$. i.e. all polynomials whose constant term is zero.

Prime Proof:

$\langle x \rangle$ is prime because $f \cdot g \in \langle x \rangle \Rightarrow (f \in \langle x \rangle$ or $g \in \langle x \rangle$ because if both f and g have non zero constant term than $f \cdot g$ has a non zero constant term.

Theorem 36.6

Let R be a commutative ring with 1. Let $I \subsetneq R$ be a proper ideal. Then:

I is maximal $\Leftrightarrow$ R/I is a field.

I is prime $\Leftrightarrow$ R/I is an integral domain.

Example 36.7

Let $R = \mathbb{R}[x]$, and $I = \langle x^2 + 1 \rangle$. Then $R/I \cong \mathbb{C}$. Note the following for gaining an intuition:

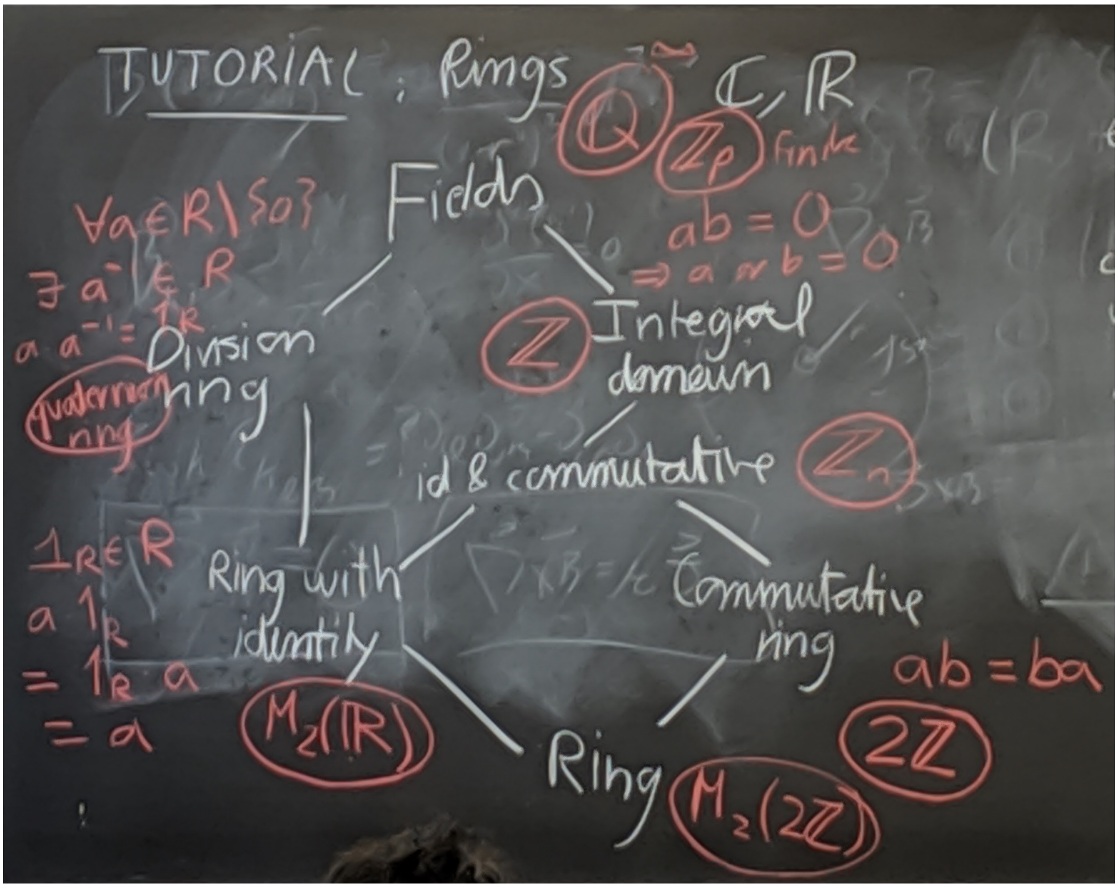
$$(x + I)(x + I) = (x^2 + I)$$
$$(x^2 + I) + (1 + I) = (x^2 + 1 + I) = 0 + I \Rightarrow (x^2 + I) = (-1 + I)$$

$$i \leftrightarrow x + I$$
$$1 \leftrightarrow 1 + I$$

Going through an a demonstration:

$$7x^3 - 3x^2 + x + 9 + I \leftrightarrow ? \in \mathbb{C}$$
$$(7x^3 + I) + (-3x^2 + I) + (x + I) + (9 + I)$$
$$(7x + I)(x^2 + I) + (-3 + I)(x^2 + I) + (x + I) + (9 + I)$$
$$(7x + I)(-1 + I) + (-3 + I)(-1 + I) + (x + I) + (9 + I)$$
$$(-7x + I) + (3 + I) + (x + I) + (9 + I)$$
$$(-6x + I) + (12 + I)$$

§37 Tutorial 11-15



Definition 37.1. $(R, +, \cdot)$ is a ring if

1. $(R, +)$ is an abelian group.
2. $(ab)c = a(bc)$.
3. $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$.

Caution: $(R, \cdot)$ is not a group.

Example 37.2

$(\mathbb{Z}, +, \cdot)$ is a ring.

1. $(\mathbb{Z}, +)$ is an abelian group.
2. 2 is satisfied.
3. 3 is satisfied.

Example 37.3

$(\mathbb{Z}, \cdot)$ is not a group because $\forall n \in \mathbb{Z}$, $n \neq 1, -1$, then $\nexists n^{-1} \in \mathbb{Z}$.

Exercise 37.4. Find an example for each type of ring.

1. Ring: $M_2(2\mathbb{Z})$ doesn't have the identity and isn't commutative.
2. Ring with Identity: $M_2(\mathbb{R})$. Matrix multiplication is not commutative but $M_2(\mathbb{R})$ contains the identity element.
3. Commutative Ring: $2\mathbb{Z}$. Commutative, but doesn't contain the multiplicative identity element.
4. Division Ring: Quaternion Ring
5. Identity and Commutative: $\mathbb{Z}_n$ where n is not prime. It has the identity and multiplication is commutative, but it is not an integral domain.
$$a, b \in \mathbb{Z}_n \text{ where } n = ab$$
$$\Rightarrow a \cdot b = 0 \mod (n)$$
but $a, b \neq 0$.
6. Integral Domain: $\mathbb{Z}$ because there is identity, multiplication is commutative, there aren't any zero divisors, but there aren't inverses for all elements.
7. Field: Examples include $\mathbb{Q}$ and $\mathbb{Z}_p$ where p is prime.

Example 37.5

Let R be a ring. $x \in R$ is idempotent if $x^2 = x$. Show that the only idempotent elements in an integral domain are 0 and 1.

Let $x \in \mathbb{R}$, where R is an integral domain, such that $x^2 = x$.

$$x^2 = x$$
$$\Rightarrow x^2 - x = 0$$
$$\Rightarrow x(x - 1) = 0$$
$$\text{Because } R \text{ is an integral domain, this implies that } x = 0 \text{ or } x = 1$$

Note that the following argument would be incorrect because R is not a division ring:

$$x \neq 0$$
$$\Rightarrow x^{-1}x^2 = x^{-1}x$$
$$\Rightarrow x = 1$$

Theorem 37.6

Let R be an integral domain. Then $ab = ac \Rightarrow b = c$.

Example 37.7

In $\mathbb{Z}$ (an integral domain):

$$\begin{aligned} n \cdot m &= n \cdot m' \\ \Rightarrow m &= m' \end{aligned}$$

In $\mathbb{Z}_6$ (not an integral domain):

$$3 \cdot 2 = 3 \cdot 4 = 0$$

but 2 is not equal to 4.

Example 37.8

Prove or disprove: R is a ring with identity 1_R. $S \subset R$ is a subring that has identity 1_S. Then does $1_R = 1_S$?

FALSE. Counter example:

$R = \mathbb{Z}_6$ ring with identity $1_R = 1$ and $S = \{0, 3\}$.

Subring conditions:

1. $S \neq \varnothing$
2. $r - s \in S \ \forall r, s \in S$

$$\begin{aligned} 0 - 0 = 0 \in \mathbb{Z}_6 \\ 0 - 3 = 3 \in \mathbb{Z}_6 \\ 3 = 3 = 0 \in \mathbb{Z}_6 \end{aligned}$$

3. $r \cdot s \in \S \ \forall r, s \in S$

$$\begin{aligned} 0 \cdot 0 = 0 \in \mathbb{Z}_6 \\ 0 \cdot 3 = 0 \in \mathbb{Z}_6 \\ 3 \cdot 3 = 3 \in \mathbb{Z}_6 \end{aligned}$$

But $1_R = 1 \neq 3 = 1_S$.

Example 37.9

Is $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ an integral domain?

1. Ring ✓
2. Identity 1 ✓
3. Commutative ✓

$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i = (c + di)(a + bi)$$

   Follows because addition and multiplication in $\mathbb{Z}$ are commutative .

4. No zero divisors:

$$\begin{gathered}
\text{Assume } a + bi \neq 0 \\
(a + bi)(c + di) = 0 \\
\Rightarrow (a - bi)(a + bi)(c + di) \\
\Rightarrow \underbrace{(a^2 + b^2)}_{\in \mathbb{Z}}(c + di) \\
\text{Let } n = a^2 + b^2 \in \mathbb{Z} \\
\Rightarrow n(c + di) = 0 \\
\Rightarrow nc + ndi = 0 \\
\Rightarrow \begin{cases} nc = 0 \\ nd = 0 \end{cases} \quad \Rightarrow c = d = 0 \text{ because } \mathbb{Z} \text{ is an integral domain} \\
\Rightarrow c + di = 0
\end{gathered}$$

   Therefore there are no zero divisors because the only way to satisfy the equality is if $(c + di) = 0$.

Definition 37.10 (Ring homomorphism)**.** Ring homomorphism: Let $\varphi : R \to S$ where R, S are rings. Then:

$$\begin{aligned}
\varphi(a + b) &= \varphi(a) + \varphi(b) \\
\varphi(ab) &= \varphi(a)\varphi(b)
\end{aligned}$$

Definition 37.11 (Ideal)**.** Let $I \subset R$. I is an ideal if it is a subring such that $\forall r \in R$, $rI \subset I$ and $Ir \subset I$.

i.e. $\forall a \in I$, $\forall r \in R$, $ar \in I$ and $ra \in I$.

Example 37.12

Find all possible ring homomorphisms $\varphi : \mathbb{Z}_6 \to \mathbb{Z}_{15}$.

First we will answer the following: what are all the possible group homomorphisms?

$\mathbb{Z}_6 = \langle 1 \rangle$ is cyclic so φ is defined by $\varphi(1)$. i.e.

$$\begin{gathered} 1 \to x \\ \Rightarrow n \to nx \end{gathered}$$

Also,

$$\begin{gathered} 0 = \varphi(0) = \varphi(6) = 6x \in \mathbb{Z}_{15} \\ \Rightarrow [6x]_{15} = 0 \\ \Rightarrow [2x]_5 = 0 \\ \Rightarrow [x]_5 = 0 \end{gathered}$$

So the possible values of x are $x = \{0, 5, 10\}$. Group homomorphisms:

$$\begin{gathered} \varphi_0 : 1 \to 0 \\ \varphi_5 : 1 \to 5 \\ \varphi_{10} : 1 \to 10 \end{gathered}$$

Are these also ring homomorphisms?

1. φ_0. ✓

$$\begin{gathered} 1 \to 0 \\ n \to 0 \\ \varphi(nm) = nm \cdot 0 = 0\varphi(n)\varphi(m) \end{gathered}$$

2. φ_5

$$\begin{gathered} 1 \to 5 \\ n \to 5n \\ \varphi(nm) = 5nm \\ \varphi(n)\varphi(m) = 5n \cdot 5m = 25nm = 10nm \\ 5nm \neq 10nm \text{ so not a ring homomorphism} \end{gathered}$$

3. φ_{10}. ✓

$$\begin{gathered} 1 \to 10 \\ n \to 10n \\ \varphi(nm) = 10nm \\ \varphi(n)\varphi(m) = 10n \cdot 10m = 100nm = 10nm \end{gathered}$$

So the ring homomorphisms from $\mathbb{Z}_6 \to \mathbb{Z}_{15}$ can be described by $\varphi(1) = 0$ and $\varphi(1) = 10$.

§38 Lecture 11-15

Example 38.1

$$\mathbb{Z}_3[x]/I \text{ where } I = \langle x^2+2\rangle$$
$$(x^2+I)+(2+I) = (x^2+2+I) = (0+I)$$
$$(2+I)+(1+I) = (0+I)$$
$$\text{so } (x^2+I) = -(2+I) = (1+I)$$
$$\underbrace{((2x+1)+I)}_{\text{Non zero}}\underbrace{((x+1)+I)}_{\text{Non zero}} = (2x^2+2x+x+1+I) = (2x^2+1+I)$$
$$= (x^2+I)+(x^2+I)+(1+I) = (1+I)+(1+I)+(1+I) = (0+I)$$

Hence $\mathbb{Z}_3[x]/I$ is not an integral domain.

Theorem 38.2 (The Chinese Remainder Theorem)
Let $n_1, n_2, n_3, \ldots, n_k$ be positive integers with $\gcd(n_i, n_j) = 1$ for $i \neq j$.

Then for any $a_1, a_2, a_3, \ldots, a_k$, the following has a solution:

$$\begin{aligned} x &\equiv_{n_1} a_1 \\ x &\equiv_{n_2} a_2 \\ &\vdots \\ x &\equiv_{n_k} a_k \end{aligned}$$

Moreover, for any two solutions x and x', $x \equiv x' \mod (n_1 n_2 \cdots n_k)$.

Example 38.3
Generally, $\mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$ if $\gcd(p, q) = 1$.

For example, $\mathbb{Z}_7 \times \mathbb{Z}_8 \cong \mathbb{Z}_{56}$.

Proof. Consider the homomorphism $\varphi : \mathbb{Z} \to \mathbb{Z}_7 \times \mathbb{Z}_8$ defined by

$$\varphi(a) = ([a]_7, [a]_8)$$

$$\begin{aligned} \varphi(a+b) &= ([a+b]_7, [a+b]_8) = ([a]_7 + [b]_7, [a]_8 + [b]_8) \\ &= ([a]_7, [a]_8) + ([b]_7, [b]_8) = \varphi(a) + \varphi(b) \end{aligned}$$

$$\varphi : \mathbb{Z} \to G \qquad \varphi(n) = g^n \text{ where } g = (1, 1)$$

φ is surjective by the chinese remainder theorem. Indeed fo any a_1, a_2, there exists x such that $x \equiv_7 a_1$ and $x \equiv_8 a_2$ so $\varphi(x) = (a_1, a_2)$.

Note 38.4. $[a]_7$ means $a \mod (7)$.

What is $\ker(\varphi)$?

$\ker(\varphi) = 7\mathbb{Z} \cap 8\mathbb{Z} = 56\mathbb{Z}$ by the first isomorphism theorem. Because we know that $\varphi(\mathbb{Z}) = \mathbb{Z}_7 \times \mathbb{Z}_8$, and that by the first isomorphism theorem, $\varphi(\mathbb{Z}) \cong \mathbb{Z}/\ker(\varphi)$. And $\varphi(\mathbb{Z}) = \mathbb{Z}_7 \times \mathbb{Z}_8 \cong \mathbb{Z}_{56} = \mathbb{Z}/\mathbb{Z}_{56}$. $\square$

Lemma 38.5 (16.41)
Let m and n be positive integers with $\gcd(m,n) = 1$. Then for all $a, b \in \mathbb{Z}$,

$$x \equiv_m a$$
$$x \equiv_n b$$

has a solution.

Moreover, the solution is unique mod (mn). i.e. if x_1 and x_2 are solutions, then $x_1 \equiv_{mn} x_2$.

Example 38.6

$$x \equiv_7 6$$
$$x \equiv_8 4$$

has solution 20. The full set of solutions is $20 + 56\mathbb{Z}$.

Proof. We know that $x \equiv_m a$ has solutions of the form $\{a + mp : p \in \mathbb{Z}\}$. We must find solutions such that

$$a + mp \equiv_n b \Rightarrow mp \equiv_n b - a$$

But $\gcd(m,n) = 1$ implies that there exists s, t such that $1 = sm + tn$. i.e. s is the multiplicative inverse of m in $\mathbb{Z}_n$. Hence

$$smp \equiv_n s(b-a)$$
$$\Rightarrow p \equiv_n s(b-a)$$

Therefore we have found x which satisfies $x \equiv_m a$ and $x \equiv_n b$. □

Suppose x_1 and x_2 are both solutions. Then:

$$x_1 - x_2 \equiv_m 0$$
$$x_1 - x_2 \equiv_n 0$$

Hence $m \mid (x_1 - x_2)$ and $n \mid (x_1 - x_2)$ so $mn \mid (x_1 - x_2)$.

§39 Lecture 11-18

§39.1 Polynomial Rings

Definition 39.1. Let R be a commutative ring with 1.

Polyomial over R with indeterminate x.

$$f(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x^1 + \cdots + a_n x^n$$

Usually assume that $a_n \neq 0$ so that a_n is a leading coefficient.

f is monic if $a_n = 1$. $a_0, \cdots, a_n$ are coefficients of f.

n is the degree of f. The degree of 0 polynomial is $-\infty$.

$R[x]$ is the set of all polynomials over R. It is a ring. Add component wise and multiply by combining like terms.

$$\sum_{i=0} a_i x^i + \sum_{i=0} b_i x^i = \sum (a_i + b_i) x_i$$

$$(\sum a_i x^i)(\sum b_j x^j) = \sum c_k x^k \qquad \text{where } c_k = \sum_{i+j=k} a_i b_j$$

Multiplication and addition are associative, distributive, etc.

Example 39.2

$\mathbb{Z}_2[x]$:

$$(1 + x^2 + x^4)(1 + x^2 + x^4) = 1 + x^4 + x^8$$
$$(1 + x + x^2 + x^3)(1 + x + x^2 + x^3) = (1 + x^2 + x^4 + x^6)$$

$\mathbb{Z}_4[x]$:

$$(1 + x + x^2 + x^3)(1 + x + x^2 + x^3) = (1 + 2x + 3x^2 + 3x^4 + 2x^5 + x^8)$$

$\mathbb{Z}_6[x]$:

$$(2x^2 + 4 + 2)(3x^2 + 3x) = 0$$

Proposition 39.3

If R is an integral domain, then $R[x]$ is an integral domain.

Moreover, degree$(p \cdot q)$ = degree(p) + degree(q) for $p, q \in R[x]$.

$$\underbrace{(a_n x^n + \cdots + a_0)}_{p} \underbrace{(b_m x^m + \cdots + b_0)}_{q} = (a_n b_m x^{n+m} + \cdots + a_0 b_0)$$

Definition 39.4 (The evaluation homomorphism)**.** Let F be the set of functions $\{f : \mathbb{R} \to \mathbb{R}\}$. Define the following:

$$(f + g)(x) = f(x) + g(x)$$
$$(f \cdot g)(x) = f(x) \cdot g(x)$$

Associative, distributive, etc. F is a commutative ring with unity.

The evaluation homomorphism is defined as follows:

$$\varphi_a : F \to \mathbb{R}$$

Let $a \in \mathbb{R}$. Define $\varphi_a(f) = f(a)$. This is a homomorphism because:

$$\varphi_a(fg) = \varphi_a(f)\varphi_a(g)$$
$$\varphi_a(f+g) = \varphi_a(f) + \varphi_a(g)$$

Likewise: $\varphi_a : R[x] \to R$ defined by $\varphi_a(f) = f(a)$ is homomorphic (where $a \in R$). Let

$$f = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x^1 + b_0$$

Then

$$f(a) = b_n a^n + b_{n-1}a^{n-1} + \cdots + b_1 a^1 + b_0$$

You can check that φ_a is a homomorphism for each $a \in R$.

Example 39.5

1. $\varphi_0 : R[x] \to R$

$$\varphi_0(f) = \text{ the constant term of } f$$

2. $\varphi_1 : R[x] \to R$

$$\varphi_1(f) = \sum(\text{ coefficients of } f)$$

3. $\varphi_1 : \mathbb{Z}_2[x] \to \mathbb{Z}_2$

   The kernel of φ_1 is ideal of all polynomials with an even number of terms.

Theorem 39.6 (Division Algorithm)
Let $f, g \in \mathbb{F}[x]$ where $\mathbb{F}$ is a field. Suppose $g \neq 0$. Then there exists unique $q, r \in \mathbb{F}[x]$ such that $f = gq + r$ where $r = 0$ or $\deg(r) < \deg(g)$.

Proof by induction on $\deg(f) - \deg(g)$.

If $\deg(f) < \deg(g)$ we stop $f = g \cdot 0 + f$. Otherwise, let $f = a_n x^n + \cdots$ and let $g = b_m x^m + \cdots$ where $m < n$.

Now let $f' = f - \frac{a_n}{b_m}x^{n-m}g$. Then $\deg(f') < \deg(f)$.

So by induction, $f' = gq' + r$ where $\deg(r) < \deg(g)$. So

$$f = f' + \frac{a_n}{b_m}x^{n-m}g = g(\frac{a_n}{b_m}x^{n-m} + q') + r$$

□

Example 39.7

Apply the division algorithm to $x^2 + 0x + 1$ in $\mathbb{Z}_3[x]$. Let $f = 2x^5 + x^4 + 1$ and $g = x^2 + 1$.

$$
\begin{array}{r|l}
 & 2x^3 + x^2 - 2x - 1 \\
\hline
x^2 + 1 & 2x^5 + x^4 + 1 \\
 & -2x^5 - 2x^3 \\
\hline
 & x^4 - 2x^3 \\
 & -x^4 - x^2 \\
\hline
 & -2x^3 - x^2 \\
 & 2x^3 + 2x \\
\hline
 & -x^2 + 2x + 1 \\
 & x^2 + 1 \\
\hline
 & 2x + 2
\end{array}
$$

§40 Lecture 11-20

Corollary 40.1 (If α is a zero of a polynomial, then $(x - \alpha)$ is a factor)
$\alpha \in \mathbb{F}$ is a zero of $p(x) \in \mathbb{F}[x] \Leftrightarrow (x - \alpha)$ is a factor of $p(x)$.

Proof. Apply division algorithm.

$p(x) = (x - \alpha)q(g) + r(x)$ where $\deg(r) < \deg(x - \alpha) = 1$

Hence, $p(\alpha) = 0 \Leftrightarrow r = 0 \Leftrightarrow (x - \alpha) \mid p(x)$ □

Theorem 40.2 (An n degree polynomial has at most n distinct zeros)
Let $p(x) \in \mathbb{F}[x]$ be a nonzero degree n polynomial.

Then $p(x)$ has at most n distinct zeros (roots).

Proof. By induction on $\deg(p)$.

Base case: has $\deg(p) = 0$ so $p(x) = c \neq 0$. (Not equal to 0 because then the degree would be minus infinity)

Hence $p(a) \neq 0$ for all $a \in \mathbb{F}$. Hence at most $\deg(p)$ roots in this case.

Suppose that the statement holds for $n = k$. Now we prove it for $n = k + 1$.

Suppose $p(x)$ ha sa root r, so $p(r) = 0$.

So $p(x) = (x - r)q(x)$ for some $q \in \mathbb{F}[x]$ with $\deg(q) = \deg(p) - 1 = k$

Any root r' is either r or is a root of $q(x)$ because $0 = p(r') = (r' - r)q(r')$.

By induction, $q(x)$ has at most k distinct roots. Thus $p(x)$ has at most $k + 1$ distinct roots. i.e. the roots of q and r. □

Definition 40.3 (Greatest Common Divisor Definition)**.** Let $p, q \in \mathbb{F}[x]$ where $\mathbb{F}$ is a field. A monic polynomial $d \in \mathbb{F}[x]$ is a gcd of p, q if $d|p$ and $d|q$ and $d'|d$ wherever $d'|p$ and $d'|q$.

Notation: $d = \gcd(p, q)$. p, q are relatively prime if $1 = \gcd(p, q)$.

Example 40.4

If $\mathbb{Z}_5[x]$, consider how $(x+1) = \gcd(x^2+4, x^3+4x^2+2)$.

Proposition 40.5

Let $\mathbb{F}$ be a field and $p, q \in \mathbb{F}[x]$. Also let $d = \gcd(p, q)$.

Then there exists $r, s \in \mathbb{F}[x]$ such that $d = rp + sq$.

Proof. Let d be the smallest degree monic polynomial in the ideal

$$J = \{fp + gq : f, g \in \mathbb{F}[x]\}$$

Then J contains non zero polynomial because $p = 1p + 0q \in J$.

Claim: $d \mid s$ for each $s \in J$ because otherwise $s = hd + r$ with $\deg(r) < \deg(d)$ and $r \neq 0$.

$$r = s - hd = fp + gq - h(f'p + g'q) \in J$$

hence $d \mid p$ and $d \mid q$ so $J = \langle d \rangle$.

Finally, if $d' \mid p$ and $d' \mid q$ then $d' \mid d$ because $p = p'd'$ and $q = q'd'$ so $d = r(p'd') + s(q'd') = d = (rp' + sq')d'$ ☐

Theorem 40.6

$\mathbb{F}[x]$ is a P.I.D. (principle ideal domain) i.e. every ideal in $\mathbb{F}[x]$ is principal i.e. is $\langle d \rangle$.

Example 40.7

$\mathbb{Z}[x]$ is not a principle ideal domain because $\langle x, y \rangle$ is not principal.

$\mathbb{F}[x, y]$ is not a principle ideal domain because $\langle x, y \rangle$ is not principal.

§40.1 Irreducible Polynomials

Definition 40.8. A monic polynomial $f \in \mathbb{F}[x]$ is irreducible over $\mathbb{F}$ if $f \neq gh$ with $\deg(g) \geq 1$ and $\deg(h) \geq 1$.

Example 40.9

$x^2 - 3$ is irreducible over $\mathbb{Q}$ but not over $\mathbb{R}$.

$x^2 + 1$ is irreducible over $\mathbb{R}$, but it is not over $\mathbb{C}$.

$x^2 + 2$ is not irreducible over $\mathbb{Z}_3$. $(x^2 + 2) = (x - 1)(x - 2)$.

$x^2 + 2$ is irreducible over $\mathbb{Z}_5$ because it has no roots. Hence no degree factors.

§41 Lecture 11-22

Non constant $f \in \mathbb{F}[x]$ is irreducible over F if f cannot be expressed as $f = gh$ where $\deg(g), deg(h) \geq 1$

Theorem 41.1 (Fundamental Theorem of Algebra)

Every $f \in \mathbb{C}[x]$ can be expressed as $f = l(x - r_1)(x - r_2)(\cdots)(x - r_n)$ where l is the leading coefficient of f and n is the degree of f.

Corollary 41.2

Only degree 1 polynomials can be irreducible in $\mathbb{C}$.

Example 41.3

Let $f \in \mathbb{R}[x]$ with $\deg(f)$ is odd and $\deg(f) > 1$.

Theorem 41.4

An ideal $\langle p \rangle \subset \mathbb{F}[x]$ is maximal $\Leftrightarrow p$ is irreducible over $\mathbb{F}$.

Recall 41.5. Ideal $p = gh$. $\langle p \rangle \subsetneq \langle g \rangle \subseteq \mathbb{F}[x]$

Theorem 41.6

$\mathbb{F}[x]/\langle p \rangle$ is a field $\Leftrightarrow$ $\langle p \rangle$ is a maximal ideal $\Leftrightarrow p$ is irreducible.

So $\mathbb{F}[x]/\langle p \rangle$ is a field $\Leftrightarrow p$ is irreducible.

Example 41.7

$\mathbb{C} \cong \mathbb{R}[x]/\langle x^2 + 1 \rangle$ motivating amazing case.

Lemma 41.8

A degree 2 or 3 polynomial $p \in \mathbb{F}[x]$ is irreducible $\Leftrightarrow p$ has no zero.

Proof. If $p = gh$ with $\deg(g), \deg(h) \geq 1$, then one of these, say g, has $\deg(g) = 1$. Therefore $p = (x - r)g$ for $r \in \mathbb{F} \Leftrightarrow p(r) = 0$. $\square$

Example 41.9

$x^3 + x + 1$ is irreducible in $\mathbb{Z}_2[x]$ because it has no roots. $p(0) = 1$ and $p(1) = 1$.

$x^3 + x + 1$ is reducible in $\mathbb{Z}_3[x]$ because it has a root. $p(0) = 1$. $p(1) = 0$. $p(2) = 2$

$x^3 + x + 1$ is irreducible in $\mathbb{Z}_5[x]$ has no roots.

Therefore

$$\mathbb{Z}_2[x]/\langle x^3 + x + 1\rangle \text{ is a field}$$
$$\mathbb{Z}_5[x]/\langle x^3 + x + 1\rangle \text{ is a field}$$
$$\mathbb{Z}_3[x]/\langle x^3 + x + 1\rangle \text{ is not a field}$$
$$(x + 2 + \langle x^3 + x + 1\rangle)((x^2 + ax + b) + \langle x^3 + x + 1\rangle) = 0 + \langle x^3 + x + 1\rangle$$

Lemma 41.10

Each element of $\mathbb{Z}_n[x]/\langle p\rangle$ (where n is prime) is of the form $a_{d-1}x^{d-1} + a_{d-2}x^{d-2} + \cdots + a_0 + \langle p\rangle$. Assume p is monic and that p is irreducible of degree d.

Note that each element can be written in the form $f = \langle p\rangle$ to hvae $\deg(f) < d = \deg(p)$.

Idea:

$$p = x^d + q$$
$$(x^d + \langle p\rangle) + (q + \langle p\rangle) = (x^d + q + \langle p\rangle) = 0 + \langle p\rangle.$$

So we can replace any occurence of x^d by $-q$ and have the same element.

§41.1 Eisention's Criterion

Let p be prime.

Let $f = a_nx^n + \cdots + a_0 \in \mathbb{Z}[x]$

Suppose

1. p divides each a_i except a_n
2. p^2 does not divide a_0

Then f is irreducible over $\mathbb{Q}$.

Example 41.11

$2x^3 + 25x + 5$ is irreducible use $p = 5$.

$2x^5 + 6x^4 + 5x^3 + 9x^2 + 0x^1 + 30$

§42 Lecture 11-25

Lemma 42.1 (Gauss's Lemma)
Let $p \in \mathbb{Z}[x]$ be monic. Suppose p is reducible over $\mathbb{Q}$. So $p = \alpha\beta$ where $\alpha, \beta \in \mathbb{Q}[x]$ and $\deg(\beta), \deg(\alpha) \geq 1$.

Then $p = a \cdot b$ where $a, b \in \mathbb{Z}[x]$ and $\deg(a) = \deg(\alpha)$, $\deg(b) = \deg(\beta)$.

Corollary 42.2
Let $p \in \mathbb{Z}[x]$ where $p = x^n + a_{n-1}x^{n-1} + \cdots + a_0$. Suppose p has a zero in $\mathbb{Q}$. Then p has a zero $z \in \mathbb{Z}$. Moreover $z \mid a_0$.

Proof. If $p(z) = 0$, then $p(x) = q(x)(x - z)$. Hence $p(x) = a(x) \cdot b(x)$ where $\deg(b) = 1$ and $b \in \mathbb{Z}[[x]$. Hence $b = (x - z)$ for some $z \in \mathbb{Z}$ and $p(z) = q(z)b(z) = 0$. □

Often recognize irreducible deg 3 polynomials in $\mathbb{Q}[x]$. $x^2 + x + 1$ must be irreducible in $\mathbb{Q}[x]$. Since it has no $\mathbb{Q}$ zero, since no $\mathbb{Z}$ zero.

§42.1 Eisenstein's Criterion

Let p be prime. Let $f = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$.

Suppose p divides each a_i for $i < n$, p does not divide a_n, and p^2 does not divide a_0.

Example 42.3

$$7x^4 + 5x^3 + 10x^2 + 25x^1 + 5x^0$$

Show it is irreducible over $\mathbb{Q}$.

Under assumption f monic by Gauss's Lemma, it suffices to show that f is irreducible over $\mathbb{Z}$.

Suppose $f = (b_r x^r + \cdots + b_0)(c_s x^s + \cdots + c_0)$. Note either $p \nmid b_0$ or $p \nmid c_0$ because $p^2 \nmid a_0 = b_0 c_0$.

Suppose $p \nmid b_0$, hence $p \mid c_0$.

Let m be the smallest such that $p \nmid c_m$.

Note $p \nmid c_s$ because $p \nmid a_n = b_r c_s$ so $m < s$.

Then $a_m = b_1 c_{m-1} + \cdots + b_m c_0$.

$p \mid a_m$ by hypothesis. $p \nmid b_0$, $b \nmid c_m$ and $p | c_{m-1} \cdots c_0$. So $P|$left but $p \nmid$ right. Contradiction! □

For each $n \geq 1$, there is a homomorphism $\phi_n : \mathbb{Z}[x] \to \mathbb{Z}_n[x]$ induced by $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$.

$$\phi_n(f) = f \quad \text{with coefficients mod } n$$

Example 42.4

$$\underbrace{\phi_3(5x^3 + 4x + 7)}_{\in\mathbb{Z}[x]} = \underbrace{2x^3 + x + 1}_{\in\mathbb{Z}_3[x]}$$

Lemma 42.5
If $\phi_n(f)$ is irreducible in $\mathbb{Z}_n[x]$ (and $f \neq mf'$ for some $m \in \mathbb{Z}$), then f is irreducible in $\mathbb{Z}[x]$.

Proof. Indeed, if $f = g \cdot h$ in $\mathbb{Z}[x]$, then $\phi_n(f) = \phi_n(gh) = \phi_n(g)\phi_n(h)$. $\square$

Example 42.6
$\mathbb{Q}[x]/\langle 5x^3 + 4x + 7\rangle$ is a field.

To compute $\gcd(f, g)$, $f, g \in \mathbb{F}[x]$, just apply Euclid's algorithm.

Example 42.7
$\gcd(x^3 + x + 1, x^2 + 2)$ in $\mathbb{Z}_3[x]$.

$$\begin{array}{r|l} & x \\ \hline x^2+2 & x^3 \quad + x + 1 \\ & -x^3 - 2x \\ \hline & \qquad -x + 1 \end{array}$$

$\gcd(x^2 + 2, 2x + 1) = 2x + 1$

$$\begin{array}{r|l} & \frac{1}{2}x - \frac{1}{4} \\ \hline 2x+1 & x^2 \qquad + 2 \\ & -x^2 - \frac{1}{2}x \\ \hline & \quad -\frac{1}{2}x + 2 \\ & \quad \frac{1}{2}x + \frac{1}{4} \\ \hline & \qquad \frac{9}{4} \end{array}$$

§43 Lecture 11-27

Example 43.1

$$\mathbb{Z}_3[x]/\langle x^3 + 2x + 1\rangle$$

$x^3 + 2x + 1$ is irreducible because deg ≤ 3 and no zeros. Hence we obtain a field.

Elements s: $\{ax^2 + bx + c + I : a, b, c \in \mathbb{Z}_3\}$ where $I = \langle x^3 + 2x + 1\rangle$. There are 3^3 elements because $\mathbb{Z}_3$ has 3 elements and there are three coefficients in each polynomial.

Then:

$$0 + I = (x^3 + 2x + 1 + I) = (x^3 + I) + (2x + 1 + I)$$

So $x^3 + I = (x + 2 + I)$.

Example 43.2
Example of addition

$$\begin{aligned} &(x^2 + 2x + I) + (2x + 1 + I) \\ &= x^2 + 4x + 1 + I \\ &= x^2 + x + 1 + I \end{aligned}$$

Example 43.3
Example of multiplication

$$\begin{aligned} &(2x + 1 + I)(x^2 + 2x + I) \\ &= 2x^3 + x^2 + x^2 + 2x + I \\ &= 2x^3 + 2x^2 + 2x + I \\ &= 2(x + 2) + 2x^2 + 2x + I \\ &= 2x^2 + x + 1 \end{aligned}$$

Fact 43.4. The group of units of a finite field is cyclic!

Exercise 43.5. Find the inverse of $(x^2 + 1 + I)$.

It's inverse is $(x^2 + 1 + I)^2 5$.

Another way to do it would be to take $(ax^2 + bx + c + I)(x^2 + 1 + I) = 1 + I$ and solve the system of linear equations over $\mathbb{Z}_3$ just like you would in linear algebra.

§43.1 Classification of symmetries over E^2 plane

1. e identity
2. θ_p θ notation. Counterclockwise rotation about point $p \in E^2$.

3. translation $\vec{u} \to \vec{u} + \vec{v}$
4. reflection over some line l
5. glide reflection a reflection and translation over the same line

Definition 43.6. A Freeze Group G is an infinite subgroup G of isometries(E^2) that is actually a subgroup of Isom(Strip) which is discrete in the sense that finitely many elements $g \in G$ have distance $(p, g(p)) < 1$.

Classification: 7 types of freeze groups.

§44 Tutorial 12-02

Example 44.1

$$\begin{cases} x \equiv [3]_7 \\ x \equiv [0]_8 \\ x \equiv [5]_{15} \end{cases}$$

§45 Lecture 12-02

Theorem 45.1 (Finding a field from an integral domain)
Let D be an integral domain. $\exists$ a field $\mathbb{F}_D$ and an injective homomorphism $\phi : D \to \mathbb{F}_D$ such that every $f \in F_D$ is equal to $\phi(d_1) \cdot \phi(d_2)^{-1}$ for some $d_1, d_2 \in D$.

$\mathbb{F}_D$ is called the field of fractions equal associated to D.

Example 45.2
$\mathbb{Q}[x]$ is not a field, but $\mathbb{Q}(x) = \{p/q : p, q \in \mathbb{Q}[x],\ q \neq 0\}$ is a field.

Example 45.3
If D is a field, then $D = \mathbb{F}_D$.

§45.1 Construction of $\mathbb{F}_D$

We represent a/b as (a, b).

$$S = \{(a, b) \in D : b \neq 0\}$$

Define $\sim$ on S such that $(a_1, b_1) \sim (a_2, b_2)$ if and only if $a_1 b_2 = a_2 b_1$. i.e.

$$\frac{a_1}{b_1} = \frac{a_2}{b_2} \quad \text{if and only if} \quad a_1 b_2 = a_2 b_1$$

Proof that $\sim$ is an equiv relation.

1. Reflexive

   $a_1b_1 = a_1b_1$

   $(a_1, b_1) \sim (a_1, b_1)$

2. Symmetric

   If $(a_1, b_1) \sim (a_2, b_2)$, then $(a_2, b_2) \sim (a_1, b_1)$

3. Transitive

   If $(a_1, b_1) \sim (a_2, b_2)$ and $(a_2, b_2) \sim (a_3, b_3)$, then $(a_1, b_1) \sim (a_3, b_3)$.

□

Claim: $+, \cdot$ are well-defined on $S/\sim$. Proof as an exercise.

Notation:

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1a_2, b_1b_2)$$
$$\frac{a_1}{b_1} \cdot \frac{a_2}{b_2} = \frac{a_1b_2}{a_2b_2}$$

$$(a_1, b_1) + (a_2, b_2) = (a_1b_2 + a_2b_1, b_1b_2)$$
$$\frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{a_1b_2 + a_2b_1}{b_1b_2}$$

Claim: $(S/\sim, \cdot, +, 0/1, 1/1) \equiv \mathbb{F}_D$ is a field.

with inverses

$$(\frac{a}{b})^{-1} = \frac{b}{a} \quad \text{if} \quad a \neq 0$$
$$-(\frac{a}{b}) = (-\frac{a}{b})$$

Proof. Check associativity, distributivity, commutativity. (Exercise)

$$\frac{0}{1} + \frac{a}{b} = \frac{0b + a1}{b1} = \frac{a}{b} \checkmark$$

$$\frac{1}{1} \cdot \frac{a}{b} = \frac{1a}{1b} = \frac{a}{b} \checkmark$$

$$\frac{a}{b} \neq 0 \quad (a \neq 0)$$
$$\frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ab} \sim \frac{1}{1}$$
$$\Rightarrow \frac{b}{a} = (\frac{a}{b})^{-1}$$

$$\frac{a}{b} + \frac{-a}{b} = \frac{ab + (-a)b}{b^2} = \frac{0}{b^2} \sim \frac{0}{1}$$
$$\Rightarrow -(\frac{a}{b}) = \frac{-a}{b}$$

□

§45.2 Factorization

Let R be a commutative ring with unity.

Definition 45.4 (Definition of divides, unit, and associate). a divides b if $\exists c \in R$ such that $a \cdot c = b$.

A unit u is an element with an inverse.

a and b are associates if $a = b \cdot u$ for a unit u.

Example 45.5

$$4 = 2 \cdot 2 = (-2) \cdot (-2)$$
$$2 = \underbrace{(-1)}_{\text{unit}} \cdot (-2)$$

Note 45.6. Being associates is an equivalence relation.

$$a = b \cdot u$$
$$\Rightarrow b = a \cdot u^{-1}$$

Example 45.7

In $\mathbb{Z}$, associates are $\pm n$

Definition 45.8 (Irreducible. Prime).

Suppose D is an integral domain.

$p \in D$ non-zero, non-unit is irreducible if $p = ab \Rightarrow a$ is a unit or b is a unit.

p is prime if $p \mid a \cdot b \Rightarrow p \mid a$ or $p \mid b$.

§45.3 Summary

Key take away: Really just trying to do what the rationals did to the integers, but to a general integral domain. This is useful because fields are very easy to work with, while integral domains are not very easy to work with.

What's special about the prime numbers? You can uniquely factor everything into a product of prime numbers. Everything you do with $\mathbb{Z}$ crucially lies on this fact. The question is whether or not you could do this with all general rings. The answer is not always, but many times you can.