08/24/22 Wednesday. $\mathbb{N} := \{1,2,3,\cdots\}$ $\mathbb{Z} := \{\cdots,-2,-1,0,1,2,\cdots\}$

*Definitions. $\mathbb{Q} := \{\frac{a}{b} \mid a,b \in \mathbb{Z}\ b \neq 0\}$. $\mathbb{R}$: real number. $\mathbb{C}$: complex number.

*Review presentations => Second lowest Hw.

$(\mathbb{Z}, +)$ -> Group.

$(\mathbb{Z}, +, \times)$ -> Ring.

$(\mathbb{Q}, +, \times)$ -> field.

Set.

Def: A **set** is a collection of elements.

Set = {Notation for elements in the set | condition that needs to be satisfied to be in the set}.

e.g. Even Number $\{x \in \mathbb{Z} \mid 2 \mid x\}$.

If S and T are two sets, $S \subset T$ if every object in S is contained in T.

$S \subset T$, $T \subset S \Rightarrow T = S$.

S is not contained in T. ↳ #elements in S; size; cardinality.

$S \not\subset T$. $s \in S$, $s \notin S$. finite set, $|S|$

The set of objects contained in both S and T $S \cap T$.

The set of objects that is either in T or in S $S \cup T$. (if disjoint, $S \cap T = \emptyset$, $S \amalg T$.)

$S \times T = \{(a,b) \mid a \in S \text{ and } b \in T\}$ the **cartesian product**.

the set containing no objects is the empty set $\emptyset$.

08/26/2022 Friday.

Function.

$f: A \to B$ $A \xrightarrow{f} B$ is a map / function the value of f at $a \in A$ is $f(a)$.

A specifying a function on element $f: a \mapsto b$ or $a \mapsto b$,

A is called the **domain**, B is called the **codomain**.

f is **well-defined** if $a_1 = a_2 \Rightarrow f(a_1) = f(a_2)$ $\forall a_1, a_2 \in A$.

The set $f(A) = \{b \in B \mid b = f(a) \text{ for some } a \in A\}$ is a subset of B called the **range / image**.

The set $f^{-1}(C) = \{a \in A \mid f(a) \in C\}$. $C \subseteq B$.

↑ **preimage** of C under f.

f is **injective** if $f(x) = f(y) \Rightarrow x = y$.

f is **surjective** if given $b \in B$, $\exists a \in A$ s.t. $f(a) = b$.

f is **bijective** if injective AND surjective.

f is the **identity map** if $A = B$ and $f(a) = a$ $\forall a \in A$. $f = id_A$.

if $f: A \to B$, $g: B \to C$, the composite map $g \circ f: A \to C$ $(g \circ f)(a) = g(f(a))$.

Equivalence Relations

let A be a nonempty set, a **binary relation** on a set A is a subset R of $A \times A$

$a \sim b$ if $(a, b) \in R$.

$\sim$ is an **equivalent relation** if $\sim$ is 1) **reflexive** $x \sim x$ $\forall x \in A$

2) **symmetric** $x \sim y \Rightarrow y \sim x$ $\forall x, y \in A$.

3) **transitive** $x \sim y$, $y \sim z \Rightarrow x \sim z$ $\forall x, y, z \in A$.

eg. $x \sim y$ iff $2 \mid x - y$. ① $2 \mid x - x$. $2 \mid 0$. $x \sim x$ ✓.

② $2 \mid x - y$. $\Rightarrow 2 \mid y - x$. $(= -(x - y))$ ✓.

③ $2 \mid x - y$, $2 \mid y - z \Rightarrow 2 \mid x - z$ $(= x - y + y - z)$. ✓.

if $\sim$ defines an equivalence relation on A, then the **equivalence class** of $a \in A$

$[a] = \{x \in A \mid x \sim a\}$. ↘ $x, y \in A$.

eg. equivalent class of $x \sim y$ iff $2 \mid x - y$?

if x is even, $x = 2n$ $n \in \mathbb{Z}$. $2 \mid 2n - y \Rightarrow y$ is even.

if x is odd, $x = 2n + 1$ $n \in \mathbb{Z}$ $[x] = \{y \mid y \sim x\}$. $y \mid x - 2n - 1 \Rightarrow y$ is odd.

the symmetric and transitive properties imply $y \in [x]$ iff $[y] = [x]$.

the reflexive property implies $x \in [x]$, so equivalence class is nonempty and its union is A.

08/29/22 Monday.

Properties of $\mathbb{Z}$.

if $a,b \in \mathbb{Z}$, $a \neq 0$ we say **a divides b** if $\exists c \in \mathbb{Z}$, s.t. $b = ac$ "$a \mid b$"

if $a,b \in \mathbb{Z} \setminus \{0\}$, $\exists!$ positive integer d, called **$\gcd(a,b)$** s.t. $d \mid a$ and $d \mid b$.

if $e \mid a$ and $e \mid b$ then $e \mid d$.

if $a,b \in \mathbb{Z} \setminus \{0\}$, $\exists!$ positive integer ℓ, called **$\text{lcm}(a,b)$** s.t. $a \mid \ell$ and $b \mid \ell$.

if $a \mid m$ and $b \mid m$, $\ell \mid m$.

The division algorithm: if $a,b \in \mathbb{Z}$ and $b \neq 0$, $\exists! q, r \in \mathbb{Z}$ with $0 \leq r < |b|$ s.t. $a = qb + r$. (q: quotient, r: remainder.)

The Eudidean Algorithm: (find gcd).

if $a,b \in \mathbb{Z} \setminus \{0\}$,

$a = q_0 b + r_0$

$b = q_1 r_0 + r_1$

$r_0 = q_2 r_1 + r_2$

$\vdots$

$r_{n-2} = q_n r_{n-1} + r_n$ → last nonzero remainder. $\gcd(a,b) = r_n$.

$r_{n-1} = q_{n+1} r_n$.

$|b| > |r_0| > \cdots > |r_n|$ strictly decreasing seq. of nonnegative integers $\Rightarrow r_n$ exists.

Claim $\gcd(a,b) = \gcd(b, r_0)$.

pf: $r_0 = a - q_0 b$. if $d \mid a, d \mid b \Rightarrow d \mid a - q_0 b \Rightarrow d \mid r_0$.

$r_0 + q_0 b = a$. if $d \mid r_0, d \mid b \Rightarrow d \mid r_0 + q_0 b \Rightarrow d \mid a$. same set of divisors $\Rightarrow$ same greatest.

Thm: Given $a,b \in \mathbb{Z}$, $\exists u, v \in \mathbb{Z}$ s.t. $au + bv = \gcd(a,b)$

Primes.

Def: an integer $p > 1$ is **prime** if its only divisors are 1 and itself.

Euclid's Lemma: p is a prime if $p \mid ab$, $p \mid a$ or $p \mid b$.

pf: $p \mid ab$, if $p \nmid a$, p and a are coprime ($\gcd(a,p) = 1$).

$\exists u, v \in \mathbb{Z}$ s.t. $au + pv = 1$

$b = bau + bpv = abu + pvb$.

$p \mid ab \Rightarrow p \mid abu$, $p \mid pvb \Rightarrow p \mid b$.

Fundamental theorem of Arithmetic.

If $n \in \mathbb{Z}$, $n > 1$ then n can be factored uniquely into a product of primes.

$n = p_1^{d_1} \cdots p_m^{d_m}$ unique up to ordering.

Thm: there are infinitely many primes.

proof: Suppose there are only finitely many primes $p_1, \cdots, p_r$

Let $N = p_1 p_2 \cdots p_r + 1$, if N is a prime, contradicts.

if N is not a prime, say $p_k | N$. Since $p_k | p_1 p_2 \cdots p_n$, $p_k | 1$ contradicts.

08/31/2022 Wednesday.

Congruences

fix $m \in \mathbb{N}$ by division algorithm. if $a \in \mathbb{Z}$ $\exists$ unique q, r s.t. $a = mq + r$ $0 \le r < m$.

Def: a and b are congruent mod m or congruent modulo m if $m | a-b$.

"$a \sim b$ iff $m | a-b$" on $\mathbb{Z}$. a and b have the same remainder when divided by m.

$\Downarrow$

residue class

integers mod m.

$\mathbb{Z}/m\mathbb{Z} = \{[0], [1], \cdots, [m-1]\}$ OR $\{\bar{0}, \bar{1}, \cdots, \overline{m-1}\}$.

$\bar{a} = \{a, a+m, a+2m, \cdots, a-m, a-2m, \cdots\}$.

natural map $[\,]: \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$.

$a \to [a]$.

$[a] \times [b] = [a \times b]$ $\forall a, b \in \mathbb{Z}$.

$[a] + [b] = [a+b]$.

a is an arbitrary element in $[a]$.

x.+ doesn't depend on choice of representation.

proof: suppose $a_1 \equiv b_1 \bmod m$ $m | a_1 - b_1$.

$a_1 = b_1 + sm$ $s \in \mathbb{Z}$.

suppose $a_2 \equiv b_2 \bmod m$

$a_2 = b_2 + tm$ $t \in \mathbb{Z}$.

$a_1 + a_2 = b_1 + b_2 + (s+t)m$. $\Rightarrow (a_1 + a_2) \equiv (b_1 + b_2) \bmod m$.

$a_1a_2 = b_1b_2 + m(b_1t + b_2s + stm) \Rightarrow a_1a_2 \equiv b_1b_2 \bmod m$.

$[0] \in \mathbb{Z}/m\mathbb{Z}$ behaves like $0 \in \mathbb{Z}$. $[0]+[a]=[a]$.

$[1] \in \mathbb{Z}/m\mathbb{Z}$ behaves like $1 \in \mathbb{Z}$. $[1] \times [a] = [a]$.

$\underbrace{[1]+[1]+\cdots+[1]}_{m.} = [0]$ $\quad [m]=[0]$.

Prop: $\forall m \in \mathbb{N}, a \in \mathbb{Z}$, the congruence $ax \equiv 1 \bmod m$ has a solution in $\mathbb{Z}$ iff $\gcd(a,m)=1$.

pf: if $\gcd(a,m)=1$ $\exists u,v \in \mathbb{Z}$ s.t. $au+vm=1$. $au \equiv 1 \bmod m$.

Groups

Def: Let G be a set. A **binary operation** is a map of sets $*: G \times G \to G$

we write $a*b$ for $*(a,b)$ for $a,b \in G$.

Def: A **group** is a set G together with a binary operation $*$ s.t. the following hold:

1) **Associativity**: $(a*b)*c = a*(b*c)$

2) **Identity**: $\exists e \in G$ s.t. $a*e = e*a = a$ $\forall a \in G$. (e: identity element.)

3) **Inverses**: given $a \in G$, $\exists b \in G$ s.t. $a*b = b*a = e$. (Not reciprocal!)

Examples: $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$, $(\mathbb{Z}/m\mathbb{Z},+)$ ($[0]$), $(\mathbb{Q}\setminus\{0\}, \times)$ (1), $\{e\}$.

Counter Example: $(\mathbb{Z}\setminus\{0\}, \times)$ (no inverse.) $\quad (\mathbb{Z}/n\mathbb{Z}, \times)$ (Yes if n is a prime. $\Downarrow$ $\gcd(n,a)=1 \Rightarrow$ 3) ✓.) $\quad \phi$ (no identity.)

09/02/2022 Friday.

If $(A,*)$ and $(B,\diamond)$ are groups. we can form the group $(A \times B, (*,\diamond))$ where $A \times B = \{(a,b) \mid a \in A, b \in B\}$ whose operation is defined componentwise $(a_1,b_1)(a_2,b_2) = (a_1 * a_2, b_1 \diamond b_2)$.

the **trivial group** is a set with a single element e. $e*e=e$.

A set with a binary operation is called a **monoid** if the first two properties of being a group hold. e.g. $(\mathbb{Z},\times)$.

A group $(G,*)$ is called **Abelian** if it also satisfies $a*b=b*a$ $\forall a,b \in G$. (commutative.) e.g. $(\mathbb{Z},+)$.

Ex. $GL_n(\mathbb{R}) := \{M \in M_n(\mathbb{R}) \mid \det(M) \neq 0\}$.

Since square matrix $\det M \neq 0 \Leftrightarrow$ invertible, matrix multiplication is associative, identity matrix, we have $(GL_n(\mathbb{R}), \times)$ non-Abelian group for $n \geq 2$.

prop: if G is a group under $*$, then 1) the identity of G is unique.

2) $\forall a \in G$, a^{-1} is uniquely determined.

3) $\forall a \in G$. $(a^{-1})^{-1} = a$ $\quad (a^{-1}) * a = e$

4) $(a*b)^{-1} = (b^{-1}) * (a^{-1})$

proof: 1) suppose e_1 and e_2 are both identities, $e_1 * e_2 = e_1$, $e_1 * e_2 = e_2 \Rightarrow e_1 = e_2$.

2) suppose $a*b = e$. $a*c = e$. $\Rightarrow c = c*e = c*(a*b) = (c*a)*b = e*b = b$.

3) want to show a is the inverse of a^{-1}. since a^{-1} is the inverse of a, we have $a * a^{-1} = a^{-1} * a = e$. $\Rightarrow a^{-1} * a = a * a^{-1} = e$.

4) let $c = (a*b)^{-1}$, $(a*b) * c = e$. $\Rightarrow a * (b*c) = e \Rightarrow a^{-1} * a * (b*c) = a^{-1} * e$

$\Rightarrow (a^{-1} * a) * (b*c) = a^{-1} \Rightarrow e * (b*c) = a^{-1} \Rightarrow b*c = a^{-1} \Rightarrow b^{-1} * (b*c) = b^{-1} * a^{-1} \Rightarrow$

$(b^{-1} * b) * c = b^{-1} * a^{-1} \Rightarrow e * c = b^{-1} * a^{-1} \Rightarrow c = b^{-1} * a^{-1}$.

existence: multi. by inverses.
uniqueness: inverses are unique.

prop: let G be a group and $a, b \in G$ the equations $ax = b$ and $ya = b$ have unique solutions for $x, y \in G$. In particular, 1) if $au = av$, then $u = v$. 2) if $ub = vb$, then $u = v$.

Def: for G a group and $x \in G$, the order of x is the smallest positive integer n s.t. $x^n = 1$ (identity e). we denote this by $|x|$. ($x^n = x * x * \cdots * x$)

order of group/set = cardinality.

if no positive power of x is the identity, x is said to be of infinite order. $|x| = \infty$.

Example: under addition, all nonzero elements have order ∞ in $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$.

$(\mathbb{Z}/9\mathbb{Z}, +)$ $[6] + [6] + [6] = [18] = [0]$. $\Rightarrow [6]$ has order 3 in $\mathbb{Z}/9\mathbb{Z}$.

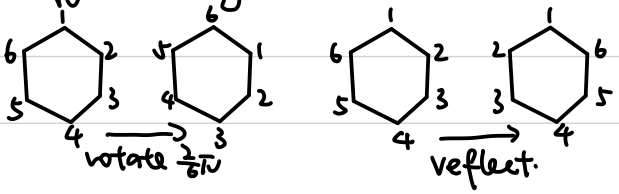
09/07/22 Wednesday.

Dihedral Group. ↑

elements are symmetries of geometric objects.

Example: regular polygons n-gons $n \geq 3$.

hexagon.



A symmetry of hexagon gives a map $\{1,2,\cdots,6\} \to \{1,2,\cdots,6\}$.

e.g. $\sigma(1)=3$. $\sigma(2)=6$.

$r(1)=2$ $\quad S(3)=5$. this function determines the symmetry. BUT not all do

if σ is a symmetry $\sigma(i)=j$ means σ sends i to where j used to be.

let D_{2n} be the set of symmetries of the n-gon.

composite fn.

Define $t_1 t_2$ to be the symmetry apply t_2 then apply t_1 for t_1, t_2 in D_{2n}.

1) Associative. Since composition of fns is associative.

2) Identity. the symmetry that does nothing. $\sigma(i)=i \ \forall i \in \{1,\cdots,n\}$.

3) Inverse. undo the symmetry.

$2\pi - x$ clockwise.

D_{2n} is called dihedral group of order $2n$. $|D_{2n}|=2n$.

vertex 1 have n choices to send.

vertex 2 have $(n-2)$ choices. (must next to 1).

vertex 3, 4, $\cdots$, 6 only have one choice left.

Hence there are $2n$ symmetries for the n-gon. e.g. hexagon. $|D_{12}|=12$.

n rotations about the center of the shape $\frac{2\pi}{n}$ radian clockwise. "r"

n reflections through n lines of symmetry. "s"

- n is odd. through vertex.
- n is even, half of them through vertex. half of them through oppo sides.

D_{12}.

1) $1, r, r^2, r^3, r^4, r^5$ $\quad |r|=6$.

r·r

$\frac{2\pi}{6}\ \frac{4\pi}{6}\ \pi\ \frac{8\pi}{6}\ \frac{10\pi}{6}$.

2) $|s|=2$.

3) $s \neq r^i \ \forall i$.

4) $sr^i \neq sr^j \ \forall i \neq j$.

5) $r^i \neq sr^j \ \forall i,j$. $\Rightarrow sr^i$ is a reflection in D_{2n}.

not a rotation.

$D_{12} = \{1, r, r^2, r^3, r^4, r^5, s, sr, sr^2, sr^3, sr^4, sr^5\}$. all distinct.

$D_{2n} = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \rangle$.

non-abelian. $srsr \cdots$ $\quad sr^{-1}$ $\quad |sr|=2$.

09/09/22 Friday:

Symmetric Groups.

Let Ω be a nonempty set, let S_Ω be the set of all bijections from Ω to itself. (Permutation).

Let σ, τ be permutations of Ω $\sigma: \Omega \to \Omega$, $\tau: \Omega \to \Omega$, $\sigma \circ \tau$ is also a bijection $\sigma \circ \tau: \Omega \to \Omega$.

1) Associative: function composition is associative.

2) identity. $\exists$. $1(a) = a$ $\forall a \in \Omega$.

3) inverse. $\forall \sigma \in \Omega$, $\exists \sigma^{-1}: \Omega \to \Omega$ s.t $\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = 1$.

Hence $(S_\Omega, \circ)$ is a group. "symmetric group on the set Ω".

usually we take $\Omega = \{1, 2, \cdots, n\}$. we write S_n.

Ex. Let $\Omega = \{1,2,3\}$. Let σ be in S_3 $\sigma(1)=2$, $\sigma(2)=3$, $\sigma(3)=1$. $(1,2,3)$.

Let τ be in S_3 $\tau(1)=2$, $\tau(2)=1$, $\tau(3)=3$. $(1,2)(3)$. or $(1,2)$

A cycle is a string of integers representing an element of S_n which cyclically permutes the integers.

The length of a cycle is the number of integers that appear in it.

Two cycles are called disjoint if they have no numbers in common.

the group S_3

$\sigma_1(1)=1$, $\sigma_1(2)=2$, $\sigma_1(3)=3$. $1, e, (1)(2)(3)$

$\sigma_2(1)=1$, $\sigma_2(2)=3$, $\sigma_2(3)=2$. $(2\,3)$.

$\sigma_3(1)=3$, $\sigma_3(2)=2$, $\sigma_3(3)=1$. $(1\,3)$.

$\sigma_4(1)=2$, $\sigma_4(2)=1$, $\sigma_4(3)=3$. $(1\,2)$

$\sigma_5(1)=2$, $\sigma_5(2)=3$, $\sigma_5(3)=1$. $(1\,2\,3)$.

$\sigma_6(1)=3$, $\sigma_6(2)=1$, $\sigma_6(3)=2$ $(1\,3\,2)$.

for any $\sigma \in S_n$, the cycle decomposition of σ^{-1} is obtained by writing the numbers in each cycle of the cycle decomposition of σ in reverse order.

e.g. $\sigma = (1\ 12\ 8\ 10\ 4)(2\ 13)(5\ 11\ 7)(6\ 9)$

$\sigma^{-1} = (4\ 10\ 8\ 12\ 1)(13\ 2)(7\ 11\ 5)(9\ 6)$.

$(2\,13) = (13\ 2)$ by convention, write the smallest number first.

Composing $\sigma \circ \tau$ in S_n read from right to left.

e.g. $(1\ 2\ 3) \circ (1\ 2)(3\ 4)$ (σ: $(1\ 2\ 3)$, τ: $(1\ 2)(3\ 4)$)

$\tau: 1 \to 2$. $\sigma: 2 \to 3$. $\sigma\circ\tau: 1 \to 3$.

$\tau: 2 \to 1$ $\sigma: 1 \to 2$ $\sigma\circ\tau: 2 \to 2$.

$\tau: 3 \to 4$. $\sigma: 4 \to 4$. $\sigma\circ\tau: 3 \to 4$.

$\tau: 4 \to 3$. $\sigma: 3 \to 1$. $\sigma\circ\tau: 4 \to 1$.

So $\sigma\circ\tau = (1\ 3\ 4)$

Non-abelian e.g. $(12)(13) = (132)$ $(13)(12) = (123)$ But disjoint cycles commute.

the **order** of a permutation is the lcm of the lengths of the cycles in decomposition.

$|S_n| = n!$

A **transposition** is a cycle of length 2.

Homomorphisms and Isomorphisms.

Def: let $(G,*)$ and $(H,\diamond)$ be groups. A map $\varphi: G \to H$ s.t. $\varphi(x*y) = \varphi(x) \diamond \varphi(y)$. $\forall x,y \in G$ is called a **homomorphism**.

Def: The map $\varphi: G \to H$ is an **isomorphism** and G and H are said to be **isomorphic** written $G \cong H$ if (1) φ is a homomorphism $\varphi(xy) = \varphi(x)\varphi(y)$ AND ($\varphi(x^n) = \varphi(x)^n$.)

(2) φ is a bijection.

Def: A homomorphism from a group to itself is called an **endomorphism**.

Def: **Automorphism** = endomorphism + isomorphism.

Ex. 1) $(\mathbb{Z},+) \to (\mathbb{Q},+)$ $\mathbb{Z} \subseteq \mathbb{Q}$. inclusion map. $x \mapsto x$.

$\varphi(x+y) = x+y$. $\varphi(x) + \varphi(y) = x+y$ $\Rightarrow$ Homomorphism.

injective but Not surjective $\Rightarrow$ Not isomorphism.

2) $(\mathbb{Z},+) \to (\mathbb{Z}/m\mathbb{Z},+)$ $x \mapsto [x]$. $\varphi(x+y) = [x+y]$ $\varphi(x)+\varphi(y) = [x]+[y] = [x+y]$ $\Rightarrow$ Homomorphism.

surjective but Not injective $\Rightarrow$ Not isomorphism.

3) $\forall G$, the identity map $G \to G$, $x \mapsto x$ is an isomorphism. (Automorphism).

4) $\forall G, H$, $\varphi: G \to H$ $g \mapsto e_H$ ($\Rightarrow$ identity element in H.) is called trivial homomorphism. Not isomorphism.

$\varphi(g_1 g_2) = e_H$, $\varphi(g_1)\varphi(g_2) = e_H e_H = e_H$.

Prop: let $(G,*)$, $(H,\circ)$, $(M,\square)$ be three groups. let $f:G\to H$, $g:H\to M$ be homomorphisms, then $g\circ f: G\to M$ is a homomorphism.

pf: $g(f(x*y)) = g(f(x)\circ f(y)) = g(f(x))\square g(f(y))$

9/12/2022 Monday.

Prop: if $\varphi: G\to H$ is isomorphism ("iff") then ① $|G|=|H|$.

② G abelian $\Leftrightarrow H$ abelian.

③ $\forall x\in G$, $|x|=|\varphi(x)|$.

proof ③: suppose $|\varphi(x)|=\infty$ and $|x|=n<\infty$, then $\varphi(x)^n=\varphi(x^n)=\varphi(e_G)=e_H$. $\Rightarrow |\varphi(x)|=n$. contradicts.

suppose $|x|=\infty$ and $|\varphi(x)|=n<\infty$, then $\varphi(x^n)=\varphi(x)^n=e_H=\varphi(e_G)$

since φ is injective, $x^n=e_G$. contradicts.

So $|x|$ and $|\varphi(x)|$ either both finite or both infinite. $\Rightarrow |x|=|\varphi(x)|$.

suppose $|x|=n$, $|\varphi(x)|=m$, $\varphi(x)^n=\varphi(x^n)=\varphi(e_G)=e_H$. $\Rightarrow m\le n$.

Similarly, $\varphi(e_G)=\varphi_H=\varphi(x)^m=\varphi(x^m)$ φ injective $\Rightarrow e_G=x^m$ $n\le m$.

Hence $n=m$.

Ex. S_3 and $\mathbb{Z}16\mathbb{Z}$ S_3 nonabelian $\mathbb{Z}16\mathbb{Z}$ abelian. $\Rightarrow$ Not isomorphic.

$D_6\cong S_3$ $D_6=\{r,s\mid r^3=s^2=1, sr=r^{-1}s\}$. map $a=(1\,2\,3)\mapsto r$. $b=(1\,2)\mapsto s$.

any non-abelian group of order 6. check $a^3=b^2=1$ and $ba=a^{-1}b$. check S_3 is generated by a and b.

lemma: let $\varphi: G\to H$ be a homomorphism, then $\varphi(x^n)=\varphi(x)^n$ $\forall n\in\mathbb{R}$.

prop: if $\varphi: G\to H$ is homomorphism, then $\varphi(e_G)=e_H$.

proof: $e_G\cdot e_G=e_G$.

$\varphi(e_G\cdot e_G)=\varphi(e_G) \Rightarrow \varphi(e_G)\varphi(e_G)=\varphi(e_G) \Rightarrow \underbrace{\varphi(e_G)^{-1}}_{(e_H)^{-1}=e_H\cdot e_H=e_H}\varphi(e_G)\varphi(e_G)=\varphi^{-1}(e_G)\varphi(e_G)$. $\Rightarrow \varphi(e_G)=e_H$.

Subgroups.

Def: let $(G,*)$ be a group, a subgroup H of G is a subset $H\subseteq G$ s.t.

① $e\in H$ ② $x,y\in H\Rightarrow x*y\in H$. ③ $x\in H\Rightarrow x^{-1}\in H$. write $H\le G$.

(A subgroup H of $(G,*)$ is a subset H of G that is a group under the same operation as G.)

Ex. $(\mathbb{Z},+)$ is a subgroup of $(\mathbb{Q},+)$.

$(\mathbb{Q},+)$ is a subgroup of $(\mathbb{R},+)$.

$(\mathbb{Q}\setminus\{0\},\times)$ is a subgroup of $(\mathbb{R}\setminus\{0\},\times)$.

If G is a group, H s.t. $H=G$ is a subgroup; $H=\{e\}$ is a subgroup. ↪ trivial subgroup.

Suppose $m\in\mathbb{Z}$, $m\mathbb{Z}:=\{ma \mid a\in\mathbb{Z}\}$ is a subgroup of $(\mathbb{Z},+)$.

CounterEx. $(\mathbb{Z}^+,+)$ is Not a subgroup of $(\mathbb{Z},+)$. No identity. No inverse.

$(\mathbb{Z}\setminus\{0\},\times)$ is Not a subgroup of $(\mathbb{Q}\setminus\{0\},\times)$ No inverse.

prop: $K\leq H, H\leq G \Rightarrow K\leq G$.

prop: $H,K\leq G \Rightarrow H\cap K\leq G$.

proof: ① $e\in H, e\in K \Rightarrow e\in H\cap K$.

$x,y\in K \Rightarrow x*y\in K$.

② $x,y\in H\cap K \Rightarrow x,y\in H \Rightarrow x*y\in H \Rightarrow x*y\in H\cap K$.

③ $x\in H\cap K \Rightarrow \cdots \Rightarrow x^{-1}\in H\cap K$.

the subgroup criterion: A subset H of G is a subgroup iff ① $H\neq\phi$ ② $\forall x,y\in H, xy^{-1}\in H$.

09/14/2022 Wednesday.

proof: $\Rightarrow$: $H\leq G \Rightarrow e\in H \Rightarrow H\neq\phi$.

$H\leq G \Rightarrow x\in H \Rightarrow x^{-1}\in H$. $x,y\in H \Rightarrow xy\in H \Rightarrow xy^{-1}\in H$.

$\Leftarrow$: $H\neq\phi \Rightarrow$ let $x\in H$, $y=x$. by ②, $xx^{-1}=e\in H$.

$e,x\in H \Rightarrow ex^{-1}=x^{-1}\in H$.

$x,y^{-1}\in H$ by ②, $x(y^{-1})^{-1}=xy\in H$.

Centralizers and Normalizers.

Let A be any nonempty subset of G. Def $C_G(A)=\{g\in G \mid gag^{-1}=a\ \forall a\in A\}$ be the centralizer of A in G. ↪ subset of G. * normal subgroup.

($gag^{-1}=a$ iff $ga=ag$, $C_G(A)$ is the set of elements of G that commute with every element of A.)

prop: $C_G(A)\leq G$.

proof: $\forall a\in A$, $eae^{-1}=a \Rightarrow e\in C_G(A)$.

If $y\in C_G(A)$, $\forall a\in A$, $yay^{-1}=a \Rightarrow y^{-1}yay^{-1}y=y^{-1}ay \Rightarrow a=y^{-1}ay \Rightarrow y^{-1}\in C_G(A)$.

if $x, y \in C_G(A)$, $xya(xy)^{-1} = xyay^{-1}x^{-1} = x(yay^{-1})x^{-1} = xax^{-1} = a \Rightarrow xy \in C_G(A)$.

Def: Let $Z(G) = \{g \in G \mid gx = xg \ \forall x \in G\}$ be the center of G. (↳ subset of G.) * normal subgroup.

$Z(G) = C_G(G) \Rightarrow Z(G) \leq G$. $\quad Z(G) \leq C_G(A)$.

Let $gAg^{-1} = \{gag^{-1} \mid a \in A\}$. define the normalizer of A in G to be $N_G(A) = \{g \in G \mid gAg^{-1} = A\}$. (↳ subset of G.)

if $g \in C_G(A)$, $\forall a \in A$, $gag^{-1} = a \Rightarrow g \in N_G(A) \Rightarrow C_G(A) \leq N_G(A)$. * Not normal subgroup.

$C_G(A) \leq N_G(A) \leq G$.

Ex. if G is abelian, then $Z(G) = G$. $\forall A \leq G$. $C_G(A) = N_G(A) = G$. $(gag^{-1} = gg^{-1}a = a)$.

Ex. $G = D_8$. let $A = \{1, r, r^2, r^3\}$.

claim: $C_{D_8}(A) = A$.

proof: $rs = sr^{-1} \neq sr \Rightarrow s \notin C_{D_8}(A)$.

$r^i \cdot r^j = r^j \cdot r^i = r^{i+j} \Rightarrow \{1, r, r^2, r^3\} \in C_{D_8}(A)$.

check sr^i for $i \in \{0,1,2,3\}$. if $sr^i \in C_{D_8}(A)$, $sr^i \cdot r^{-i} = s \in C_{D_8}(A)$. contradicts. (subgroup is closed under multiplication.)

claim: $N_{D_8}(A) = D_8$.

proof: $A \leq N_{D_8}(A)$.

$sAs^{-1} = \{sIs^{-1}, srs^{-1}, sr^2s^{-1}, sr^3s^{-1}\} = \{1, r^3, r^2, r\} = A$. ⇒ generalize to sr^i.

$rs = sr^{-1} \Rightarrow (rs)^{-1} = (sr^{-1})^{-1} \Rightarrow s^{-1}r^{-1} = rs^{-1} \Rightarrow ss^{-1}r^{-1} = srs^{-1} \Rightarrow r^{-1} = srs^{-1}$. ⇒ generalize to $r^is = sr^{-i}$

$r^{-1} = r^3$.

$D_8 \leq N_{D_8}(A)$. $\quad N_{D_8}(A) \leq D_8$. $\Rightarrow N_{D_8}(A) = D_8$.

claim: $Z(D_8) = \{1, r^2\}$.

proof: $Z(D_8) \leq C_{D_8}(A) = A$.

check $\{1, r, r^2, r^3\}$: $1s = s1$. $rs = sr^{-1} \neq sr$. $r^2s = sr^{-2} = sr^2$. $r^3s = sr^{-3} = sr \neq sr^3$.

in general: $Z(D_{2n}) = \begin{cases} \{1, r^{n/2}\}. & \text{if } n \text{ is even.} \\ \{1\}. & \text{if } n \text{ is odd.} \end{cases}$

09/16/2022 Friday.

Cyclic Group.

Def: A group H is called a **cyclic group** if it is generated by one element.

$H = \langle x \rangle = \{x^n \mid n \in \mathbb{Z}\}$. x is the **generator** for H.

Ex. $(\mathbb{Z}, +) = \langle 1 \rangle = \{1^n \mid n \in \mathbb{Z}\}$. inverse $\Rightarrow$ subtraction. $1^{-n} = -n$.

$= \langle -1 \rangle$. $\underbrace{1+1+\cdots+1}_{n} = n$

Ex. $(\mathbb{Z}/n\mathbb{Z}, +) = \langle [1] \rangle = \{[1], [1+1], \cdots, \underbrace{[1+(n-1)]}_{[0]}\}$.

Prop: generators may not be unique.

Prop: **cyclic groups are abelian**.

proof: $a, b \in H = \langle x \rangle$. let $a = x^\alpha$, $b = x^\beta$. $ab = x^\alpha \cdot x^\beta = x^{\alpha+\beta} = x^\beta \cdot x^\alpha = ba$.

Prop: let $H = \langle x \rangle$. $|H| = |x|$. order of the group = order of the element.

proof: if $|x| = n$, $1, x, \cdots, x^{n-1}$ are distinct. $\Rightarrow H$ has n distinct elements.

check there are only n distinct elements:

$t = nq + k$. $0 \le k < n$. $x^t = x^{nq+k} = x^{nq} x^k = (x^n)^q x^k = 1^q x^k = x^k \in \{1, x, \cdots, x^{n-1}\}$.

if $|x| = \infty$, no power of x is the identity. if $x^a = x^b$, suppose $a < b$. $x^{a-b} = 1$ contradicts.

Prop: if $|x| = n$, $x^a = 1 \Leftrightarrow n \mid a$.

proof: $\Rightarrow$: if $n \nmid a$, $\gcd(a, n) = d$ for $d < n$. $\Rightarrow \exists u, v \in \mathbb{Z}$ s.t. $nu + av = d$.

$x^d = x^{nu+av} = x^{nu} x^{av} = (x^n)^u (x^a)^v = 1^u 1^v = 1$. $x^n = 1$ contradicts.

$\Leftarrow$: $a = nb$. $x^a = x^{nb} = (x^n)^b = 1^b = 1$.

Thm: let G be a cyclic group, then 1) if G is infinite, $G \cong (\mathbb{Z}, +)$.

2) if G is finite, $|G| = m$. $G \cong (\mathbb{Z}/m\mathbb{Z}, +)$.

proof: (1) $G = \langle x \rangle$. define $\varphi: G \to \mathbb{Z}$: $x^n \to n$.

$\forall a, b \in \mathbb{Z}$. $\varphi(x^a x^b) = \varphi(x^{a+b}) = a + b$. $\varphi(x^a) + \varphi(x^b) = a + b$.

if $a = b$, know $x^a = x^b \Rightarrow$ injective.

$\forall n \in \mathbb{Z}$, take x^n to be its preimage $\Rightarrow$ surjective.

(2) define $\varphi: G \to \mathbb{Z}/m\mathbb{Z}$: $x^j \to [j]$ for $j = 1, 2, \cdots, m$ $|G| = m$.

well-defined: $x^j = x^k$ Recall if $|x| = m$ and $x^a = 1$, $m \mid a$.

$x^k = x^j x^a = x^j (x^{tm})$ for $t \in \mathbb{Z}$. $k = j + mt$. $[j] = [k]$.

homomorphism: $\varphi(x^j * x^k) = \varphi(x^{j+k}) = [j+k] = [j] + [k] = \varphi(x^j) + \varphi(x^k)$.

bijective: if $[j] = [k]$, $j = k + mb$. $x^j = x^k x^{mb} = x^k \Rightarrow$ injective.

$|G| = |\mathbb{Z}/n\mathbb{Z}|$, injective $\Rightarrow$ surjective.

09/19/2022 Monday.

Cor: Any two cyclic groups of the same order are isomorphic.

Prop: Let G be a group $x \in G$ and $a \in \mathbb{Z} \setminus \{0\}$. if $|x| = n < \infty$, then $|x^a| = \frac{n}{\gcd(n,a)}$

pf: Let $y = x^a$. Let $d = \gcd(n,a)$ then $n = db$ $a = dc$ for some $b, c \in \mathbb{Z}$.

$y^b = x^{ab} = x^{dcb} = x^{dbc} = (x^{db})^c = (x^n)^c = 1^c = 1$. so $|y| \mid b$.

Let $k = |y|$, $y^k = x^{ak} = 1 \Rightarrow n \mid ak \Rightarrow db \mid ak \Rightarrow db \mid dck \Rightarrow b \mid ck$. $\Rightarrow b \mid k \Rightarrow b \mid |y|$ ($\gcd(b,c) = 1$)

Hence $|y| = b$.

Example: $\mathbb{Z}/6\mathbb{Z} = \langle [1] \rangle$. $|[1]| = 6$ skip1 $|[2]| = \frac{6}{\gcd(6,2)} = 3$. skip2 $|[3]| = \frac{6}{\gcd(6,3)} = 2$. skip3 $|[4]| = 3$. skip4. $|[5]| = 6$.

#people touch it.

if a is relatively prime to the order of the element, it generates the group.

Example: D_{16}. $|r| = 8$. $R = \langle r \rangle = \{1, r, r^2, \cdots, r^7\}$ r generates R.

$\langle r^2 \rangle = \{r^2, r^4, r^6, r^8 = 1\}$. r^2 doesn't.

$\langle r^3 \rangle = \{r^3, r^6, r, r^4, r^7, r^2, r^5, 1\}$. r^3 generates R. Also r^5, r^7. ($\gcd(1,3,5,7,8) = 1$.)

Example: $[1], [5], [7], [11]$ generates $\mathbb{Z}/12\mathbb{Z}$. * find generators quickly.

Thm: if $H = \langle x \rangle$ is a cyclic group.

① every subgroup of H is cyclic.

② if $|H| = n < \infty$, then $\forall a \in \mathbb{Z}^+$ s.t. $a \mid n$, $\exists$ unique subgroup of H of order a. $\langle x^d \rangle$ $d = \frac{n}{a}$.

Proof: (1) Let $k \leq H = \langle x \rangle$ if $k = \{1\}$, done. Otherwise, let $a = \min\{a > 0 \mid x^a \in k\}$.

Claim $k = \langle x^a \rangle$. Prove by contradiction.

Suppose $\exists x^b \in k$ with $a \nmid b$. $b = aq + r$. $0 < r < a$.

$x^b \in k$, $x^{aq} \in k \Rightarrow x^{b-aq} \in k \Rightarrow x^r \in k$. Since $r < a$, contradicts.

Hence $a \mid b$, $x^b \in \langle x^a \rangle$ $k \leq \langle x^a \rangle$.

Since $x^a \in k$. $\langle x^a \rangle \leq k$.

09/21/2022 Wednesday.

(2) if $a|n$, take $\langle x^{\frac{n}{a}} \rangle$ with order $\frac{n}{\gcd(\frac{n}{a}, n)} = \frac{n}{\frac{n}{a}} = a$.

uniqueness:

Example: Subgroups of $\mathbb{Z}/12\mathbb{Z}$ 1, 2, 3, 4, 6, 12

Subgroup of order 12: $\langle [1] \rangle = \langle [5] \rangle = \langle [7] \rangle = \langle [11] \rangle = \mathbb{Z}/12\mathbb{Z}$. $\frac{12}{\gcd(1,5,7,11,12)} = 12$

Subgroup of order 6: $\langle [2] \rangle = \langle [10] \rangle$.

Subgroup of order 4: $\langle [3] \rangle = \langle [9] \rangle$.

Subgroup of order 3: $\langle [4] \rangle = \langle [8] \rangle$.

Subgroup of order 2: $\langle [6] \rangle$

Subgroup of order 1: $\langle [0] \rangle$

Inclusions between different subgroups of $\mathbb{Z}/n\mathbb{Z}$:

$\langle [a] \rangle \subseteq \langle [b] \rangle$ iff $\gcd(b,n) | \gcd(a,n)$ $1 \le a, b \le n$.

Subgroups are generated by subsets of a group.

cyclic subgroup $\langle x \rangle$ generated by a single element $\{x\}$ is the smallest subgroup of G containing x.

Prop: for any nonempty collection of subgroups of G, their intersection is a subgroup.

Def: if $A \subseteq G$, define $\langle A \rangle = \bigcap_{A \subseteq H \le G} H$. $\langle A \rangle$ is the minimal subgroup of G containing A.

Def: $\bar{A} = \{a_1^{\varepsilon_1} \cdots a_n^{\varepsilon_n} \mid n \in \mathbb{Z}, n \ge 0, \varepsilon_i = \pm 1, a_i \in A\}$. (doesn't need to be distinct)

(identity)

if $A = \phi$, define $\bar{A} = \{1\}$

$\bar{A}$ is the set of all finite products of elts in A AND inverses of elements of A.

Prop: $\langle A \rangle = \bar{A}$.

Proof: let $a, b \in \bar{A}$. $a = a_1^{\varepsilon_1} \cdots a_n^{\varepsilon_n}$ $b = b_1^{\delta_1} \cdots b_m^{\delta_m}$ $ab^{-1} = a_1^{\varepsilon_1} \cdots a_n^{\varepsilon_n} b_1^{-\delta_1} \cdots b_m^{-\delta_m} \in \bar{A}$. So $\bar{A} \le G$.

$a \in A$ can be written as $A \subseteq \bar{A}$. $\bar{A} \le G$ and $A \subseteq \bar{A} \Rightarrow \langle A \rangle \subseteq \bar{A}$.

$\langle A \rangle$ is a group containing A and it is closed under multiplication and inverses.

So $\bar{A} \subseteq \langle A \rangle$

Example: $\langle (12), (13)(24) \rangle$ is a subgroup of S_4 (isomorphic to D_8).

Def: If $\varphi: G_1 \to H$ is a homomorphism, the kernel of φ is $\ker(\varphi) = \{g \in G_1 \mid \varphi(g) = e\}$. ($e$: identity in H.)

Def: If $\varphi: G_1 \to H$ is a homomorphism, the image of φ is $\mathrm{Im}(\varphi) = \{\varphi(x) \mid x \in G_1\}$.

09/23/22 Friday.

Prop: Let H, G_1 be groups, $\varphi: G_1 \to H$ a homomorphism, then $\ker\varphi$ is a subgroup of G_1, and $\mathrm{Im}\varphi$ is a subgroup of H.

Proof: ($\ker\varphi \leq G_1$).

$\varphi(e_{G_1}) = e_H \Rightarrow \ker\varphi \neq 0$.

Let $x, y \in \ker\varphi$, we have $\varphi(x) = \varphi(y) = e_H$.

$\varphi(xy^{-1}) = \varphi(x)\varphi(y^{-1}) = \varphi(x)\varphi(y)^{-1} = e_H e_H^{-1} = e_H e_H = e_H \Rightarrow xy^{-1} \in \ker\varphi$.

($\mathrm{Im}\varphi \leq H$).

$\varphi(e_{G_1}) = e_H \in \mathrm{Im}\varphi \Rightarrow \mathrm{Im}\varphi \neq 0$.

Let $x, y \in \mathrm{Im}\varphi$, we have $\varphi(a) = x$ $\varphi(b) = y$ for $a, b \in G_1$.

$xy^{-1} = \varphi(a)\varphi(b)^{-1} = \varphi(ab^{-1}) \Rightarrow xy^{-1} \in \mathrm{Im}\varphi$.

Quotient Group.

Another way of getting a smaller group from group G_1 apart from taking a subgroup.

- Subgroup group: $H \to G_1$. injective homomorphism.
- quotient group: $G_1 \twoheadrightarrow H$. surjective homomorphism.

$\varphi: G_1 \to H$ homomorphism. A fiber of φ is the set of elements of G_1 that are mapped to a single element of H. fibers form a group.

Example: $G_1 = \mathbb{Z}$. $H = \langle x \rangle$ $|x| = n$. $\varphi: \mathbb{Z} \to \langle x \rangle : a \to x^a$.

$\varphi(a+b) = x^{a+b} = x^a x^b = \varphi(a)\varphi(b) \Rightarrow$ homomorphism. $|H| = n \Rightarrow$ surjective. (finite?)

$\varphi^{-1}(x^a) = \{m \in \mathbb{Z} \mid x^m = x^a\} = \{m \in \mathbb{Z} \mid x^{m-a} = 1\} = \{m \in \mathbb{Z} \mid n \mid m-a\} = \{m \in \mathbb{Z} \mid m \equiv a \bmod n\} = \bar{a}$ OR $[a]$ in $\mathbb{Z}/n\mathbb{Z}$.

in H, $x^a x^b = x^{a+b}$ inherent: $[a] * [b] = [a+b] \Rightarrow$ the group $(\mathbb{Z}/n\mathbb{Z}, +)$.

Def: Let $\varphi: G \to H$ be a homomorphism with kernel k. The quotient group G/k "G mod k" is the group whose elts are the fibers of φ with group operation inherented from H.

multiplication of fibers is defined by first project to H, multiply in H.

remark: this definition requires knowing φ explicitly.

It is possible to define the group operation on fibers directly.

09/26/2022 Monday.

prop: let $\varphi: G \to H$ be a homomorphism with kernel k. let $X \in G/k$ be the fiber above a, $X = \varphi^{-1}(a)$, then $\forall u \in X$, $X = \{uk \mid k \in k\}$ $(\{ku \mid k \in k\})$.

proof: let $u \in X$, $\varphi(u) = a$. let $uk = \{uk \mid k \in k\}$. we want to show $X = uk$.

$uk \subseteq X$: for $k \in k$, $\varphi(uk) = \varphi(u)\varphi(k) = a \cdot e = a$. $uk \in X$.

$X \subseteq uk$: let $g \in X$, let $k = u^{-1}g$. $\varphi(k) = \varphi(u^{-1})\varphi(g) = \varphi(u)^{-1}\varphi(g) = a^{-1}a = e$. $k \in k$. $g = uk \in uk$

Def: $\forall N \leq G$ and $g \in G$, $gN = \{gn \mid n \in N\}$ is a (left) coset of N in G. ($Ng = \{ng \mid n \in N\}$ is a right coset.)

fibers of a homomorphism are cosets of the kernel.

Thm: $\varphi: G \to H$ a homomorphism with kernel k. Then the set of cosets of k in G (gk) with operation $uk \cdot vk = (uv)k$ forms the quotient group G/k and multiplication doesn't depend on choice of coset representation.

↓ Not true for any subgroups.

proof: let $X, Y \in G/k$, $Z = XY \in G/k$. $\varphi: G \to H$. $X = \varphi^{-1}(a)$ $Y = \varphi^{-1}(b)$ for some $a, b \in H$.

then $Z = \varphi^{-1}(ab)$ → this is how we define the operation on G/k.

let u, v be representations of X, Y, so $\varphi(u) = a$. $\varphi(v) = b$. $X = uk$. $Y = vk$.

WTS $uv \in Z$. $\iff uv \in \varphi^{-1}(ab) \iff \varphi(u)\varphi(v) = ab$. Hence $Z = uvk$.

the product of X and Y is the coset uvk for any choice of representations $u, v \in X, Y$.

claim: if $\varphi: G \to H$ is a homomorphism with kernel k, then $\forall g \in G$. $gkg^{-1} \in k$

proof: WTS $\varphi(gkg^{-1}) = e$. $\forall g \in G, k \in k$.

$\varphi(gkg^{-1}) = \varphi(g)\varphi(k)\varphi(g^{-1}) = \varphi(g)\varphi(k)\varphi(g)^{-1} = \varphi(g)e\varphi(g)^{-1} = e$.

09/28/2022 Wednesday.

prop: if we have a subgroup N of G s.t. $gNg^{-1} \in N$ $\forall g \in G$, we can show that the multiplication in G/N is well defined (doesn't depend on choice of representative).

$G/N \times G/N \to G/N$: $(xN, yN) \mapsto xyN$. where if $x_1N = x_2N$, $y_1N = y_2N$, then $x_1y_1N = x_2y_2N$.

Proof: $x_1^{-1}x_2, y_1^{-1}y_2 \in N$. let $u = (x_1y_1)^{-1}(x_2y_2) = y_1^{-1}x_1^{-1}x_2y_2$

$uy_2^{-1} = y_1^{-1}x_1^{-1}x_2 \Rightarrow uy_2^{-1}y_1 = y_1^{-1}\underbrace{x_1^{-1}x_2}_{\in N}y_1$ and $y_1^{-1} \in G$. $\Rightarrow uy_2^{-1}y_1 \in N \Rightarrow u \in N$.

Def: A subgroup $N \leq G$ is called normal if $\forall g \in G$. $gNg^{-1} = \{gng^{-1} \mid n \in N\} = N$. $N \trianglelefteq G$.

remark: N is normal $\Leftrightarrow N_G(N) = G$.

$\forall n \in N$, $gng^{-1} \in N$.

if G is abelian, every subgroup of G is normal. $\forall n \in N, g \in G, gng^{-1} = n$.

prop: The map $\varphi: G \to G/H$ $x \mapsto xH$ is a homomorphism with $\ker(\varphi) = H$ iff $H \trianglelefteq G$.

pf: $\forall x, y \in G$. $\varphi(xy) = xyH = xHyH = \varphi(x)\varphi(y) \Rightarrow$ homomorphism.
($uk \cdot vk = (uv)k$; $1H$; $xe^{-1} \in H$.)

Consider $x \in \ker\varphi$, $\varphi(x) = xH = H \Leftrightarrow x \in H$. So $\ker(\varphi) = H$.

3 perspectives of quotient group: fibers of homomorphisms; ($xh_1 = eh_2$.)

sets of cosets;

images of homomorphisms.

Lagrange's Theorem: If G is a finite group and $H \leq G$. $|H| \mid |G|$ (整除) and the number of (left) cosets of H in G equals $\frac{|G|}{|H|}$.

if G is a finite group and $n \mid |G|$, G need not have a subgroup of order n.

Sylow's Theorem:

for prime p, $p \mid |G| \Rightarrow$ G has an element of order p. thus a cyclic subgroup

for prime p, if $|G| = p^d m$, then G has a subgroup of order p^d.

09/30/2022 Friday.

Proof: let $|H| = n$ and the number of cosets of H in G be k.

the set of cosets of H partition G.

the map $H \to gH$: $h \mapsto gh$ is bijective. So $|H| = |gH| = n$.

Since G is partitioned into k disjoint subsets, each of which has cardinality n, $|G| = k \cdot n$ $k = \frac{|G|}{n} = \frac{|G|}{|H|}$.

Def: The number of cosets of H in G is called the index of H in G, denoted $[G:H]$.

Cor: If G is a finite group and $x \in G$ then $|x| \mid |G|$. In particular, $x^{|G|} = 1 \ \forall x \in G$.

pf: $|x| = |\langle x \rangle|$, take the subgroup H generated by x.

by Lagrange, $|H| \mid |G| \Rightarrow |x| \mid |G|$. then $x^{|G|} = 1$ b/c $|x| \mid |G|$.

Cor: Every group of prime order is cyclic.

pf: let $x \in G$, $x \neq 1$, $|\langle x \rangle| = |x| > 1$ and $|\langle x \rangle| \mid |G| \Rightarrow |\langle x \rangle| = |G| \Rightarrow G = \langle x \rangle$

prop: Every subgroup of index 2 is normal. (Not every normal subgroup has index 2).

$H \leq G$ and $[G:H] = 2$ then $H \trianglelefteq G$.

pf: let $g \in G \setminus H$, the two left cosets of H in G are eH and gH. $eH = H$, so $gH = G \setminus H$.

the two right cosets of H in G are Hg and $He = H$ so $Hg = G \setminus H$. $\Rightarrow gH = Hg$.

let $g \in H$, $gH = H = Hg$

$gHg^{-1} = H$. $\forall g \in G$.

the isomorphism theorem

let $\varphi: G \to H$ be a homomorphism. Recall $\ker(\varphi) \subset G$ is a normal subgroup, so quotient group $G/\ker\varphi$.

let $x, y \in G$ be in the same coset of $\ker\varphi$. i.e. $x\ker(\varphi) = y\ker(\varphi) \iff x^{-1}y \in \ker(\varphi) \iff \varphi(x^{-1}y) = e_H$.

$\iff \varphi(x)^{-1}\varphi(y) = e_H \iff \varphi(x)\varphi(x)^{-1}\varphi(y) = \varphi(x) \iff \varphi(y) = \varphi(x)$ φ is constant on each coset of $\ker(\varphi)$.

$\psi: G/\ker(\varphi) \to \mathrm{Im}(\varphi) : x\ker(\varphi) \mapsto \varphi(x)$. well-defined.

First Isomorphism Theorem:

let G, H be groups. $\varphi: G \to H$ a homomorphism, then $G/\ker(\varphi) \cong \mathrm{Im}(\varphi)$.

10/03/2022 Monday.

proof: preimage$(\varphi(x)) = x\ker(\varphi)$ surjective. ($\psi: x\ker(\varphi) \mapsto \varphi(x)$)

given $x, y \in G$. $\psi(x\ker(\varphi)) = \psi(y\ker(\varphi)) \iff \varphi(x) = \varphi(y) \iff x\ker(\varphi) = y\ker(\varphi)$. injective.

$\psi(x\ker(\varphi)\, y\ker(\varphi)) = \psi(xy\ker(\varphi)) = \varphi(xy) = \varphi(x)\varphi(y)$

$\psi(x\ker(\varphi))\psi(y\ker(\varphi)) = \varphi(x)\varphi(y)$

Example: $\varphi: (\mathbb{Z}, +) \to (\mathbb{Q}, +)$ is a homomorphism kernel is $\{0\} = e_{(\mathbb{Z},+)}$ image is $(\mathbb{Z}, +)$.

$\varphi: \mathbb{Z} \to \mathbb{Q}$ kernel$(\varphi) = 0 = e_{\mathbb{Z}}$. $\mathbb{Z}/e_{\mathbb{Z}} \cong \mathbb{Z}$. $|\mathbb{Z}/e_{\mathbb{Z}}| = |\mathbb{Z}|$.

↓ #Cosets

2) $(\mathbb{Z},+) \to (\mathbb{Z}/m\mathbb{Z},+)$: $a \mapsto [a]$. Kernel is multiples of m.

$\varphi: \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ $\ker\varphi = m\mathbb{Z}$. $\mathrm{Im}\varphi = \mathbb{Z}/m\mathbb{Z}$ since φ is surjective. $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z}$

3) $\varphi: G \to H: g \mapsto e_H$. $\ker\varphi = G$. $\mathrm{Im}\varphi = \{e_H\}$. $G/G \cong \{e\}$. $|G/G| = 1$. $G/G = G$.

Third Isomorphism Theorem:

Let G be a group and H and K are normal subgroups of G with $H \leq K$.

then $K/H \trianglelefteq G/H$ and $G/H \,/\, K/H \cong G/K$.

proof: WTS $K/H \in G/H$.

$e_H = H \in K/H \Rightarrow$ identity $\in K/H$.

$xH, yH \in K/H \Rightarrow xHyH = xyH \in K/H$ ($x, y \in K \Rightarrow xy \in K$)

$xH \in K/H \Rightarrow (xH)^{-1} = x^{-1}H \in K/H$. ($xHx^{-1}H = xx^{-1}H = H$. $x^{-1} \in K$)

WTS $K/H \trianglelefteq G/H$. $\Rightarrow$ WTS $gHkH(gH)^{-1} \in K/H$. $\forall gH \in G/H$.

$gHkHg^{-1}H = gkg^{-1}H$ $K \trianglelefteq G \Rightarrow gkg^{-1} \in K \Rightarrow gkg^{-1}H \in K/H$.

WTS $G/H \,/\, K/H \cong G/K$ by applying 1st iso theorem to $\varphi: G/H \to G/K: gH \mapsto gK$. ($H \leq K$.)

φ is well-defined: $g_1H = g_2H \Rightarrow g_2^{-1}g_1 \in H \Rightarrow g_2^{-1}g_1 \in K \Rightarrow g_1K = g_2K$ i.e. $\varphi(g_1H) = \varphi(g_2H)$

for gK, take gH mapping to gK. $\Rightarrow \mathrm{Im}\varphi = G/K$

$\ker\varphi = \{gH \in G/H \mid \varphi(gH) = K\} = \{gH \in G/H \mid gK = K\} = \{gH \in G/H \mid g \in K\} = K/H$.

Fourth Isomorphism Theorem:

Let G be a group, $N \trianglelefteq G$, then there is a natural bijection between the subgroups of G containing N and the subgroups of G/N.

10/05/2022 Wednesday.

Question 1. Is the function $f: \mathbb{N} \to \mathbb{N}$ defined by $f(x) = x + 1$ surjective? Justify your answer.

No $\nexists x \in \mathbb{N}$ s.t. $f(x)=1$. 0 in $\mathbb{N}$: $f(x)=0 \Rightarrow x=-1$.

0 Not in $\mathbb{N}$: $f(x)=1 \Rightarrow x=0$.

Question 2. Let G be a finite group with order $|G| = n > 2$. Prove that G cannot have a subgroup H of order $|H| = n - 1$.

Lagrange's $|H| \mid |G| \Rightarrow n-1 \mid n$.

Let $k = n-1 > 1$ $k \mid k+1 \Rightarrow k \mid 1$.

$n-1 \mid n$.

$k \mid k+1$

$k+1 = nk$ $1 = (n-1)k$. $k \mid 1$.

Question 3. Let $n \geq 3$, and consider the dihedral group D_{2n}. Prove that the subgroup $\langle r \rangle$ is a normal subgroup of D_{2n}.

Let $N = \langle r \rangle$. $N \trianglelefteq D_{2n}$ iff $\forall d \in D_{2n}$ $dNd^{-1} = \{dnd^{-1} \mid n \in N\} = N$.

$D_{2n} = \{1, r, \cdots, r^{n-1}, s, sr, \cdots sr^{n-1}\}$. ① index $= 2 \Rightarrow$ Normal.

$sr^i r^j r^{-i} s = r^j$.

$\in D_{2n} \Rightarrow$ Associativity.

Question 4. Prove that the subset of odd integers in $\mathbb{Z}$ is *not* a subgroup of $\mathbb{Z}$.

$1, 3 \in \mathbb{Z}_{odd}$ $1+3 = 4 \notin \mathbb{Z}_{odd}$. $\neq$ identity.

Question 5. Find the order of the element [42] in $\mathbb{Z}/180\mathbb{Z}$.

$$|\langle 42 \rangle| = \frac{180}{\gcd(180, 42)} = 30.$$

6 7 30.

Question 6. List the generators of the cyclic group $\mathbb{Z}/16\mathbb{Z}$.

$[1], [3], [5], [7], [9], [11], [13], [15]$.

Question 7. List the subgroups of the cyclic group $\mathbb{Z}/10\mathbb{Z}$

Subgroups of $\mathbb{Z}/10\mathbb{Z}$ have orders corresponding to divisors of 10 i.e. 1, 2, 5, 10.

Subgroup of order 1: $\langle [10] \rangle = \langle [0] \rangle$. Subgroup of order 2: $\langle [5] \rangle$.

Subgroup of order 5: $\langle [2] \rangle = \langle [4] \rangle = \langle [6] \rangle = \langle [8] \rangle$

Subgroup of order 10: $\langle [1] \rangle = \langle [3] \rangle = \langle [7] \rangle = \langle [9] \rangle$.

Question 8. Prove that the relation on $\mathbb{R}$ defined by $x \sim y$ iff $x - y \in \mathbb{Z}$ is an equivalence relation.

① Reflexive: $x-x=0\in\mathbb{Z} \Rightarrow x\sim x$.

② Symmetric: $x\sim y \Rightarrow x-y\in\mathbb{Z} \Rightarrow x-y\in\mathbb{Z} \Rightarrow y\sim x$.

③ transitive: $x\sim y, y\sim z \Rightarrow x-y+y-z=x-z\in\mathbb{Z} \Rightarrow x\sim z$.

Question 9. Find the order of each element in D_8.

$D_8=\{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$.

$|1|=1$. $|r|=4$. $|r^2|=2$ $|r^3|=4$ $|s|=2$ $|sr|=2$ $|sr^2|=2$ $|sr^3|=2$.

Question 10. Let $GL_n(\mathbb{R})$ be the set of $n \times n$ matrices with nonzero determinant be the general linear group under matrix multiplication. Prove that the set of matrices $SL_n(\mathbb{R})$, defined as $n \times n$ matrices with determinant 1 is a subgroup of $GL_n(\mathbb{R})$.

① identity: $\det(I_n)=1$.

② multiplication: let $A, B\in SL_n(\mathbb{R})$, $\det(AB)=\det(A)\cdot\det(B)=1\cdot 1=1$.

③ inverse: let $C\in SL_n(\mathbb{R})$, $\det(C^{-1})=\det(C)^{-1}=1^{-1}=1$

Question 11. Given $\sigma = (1523)(47)$ and $\tau = (183462)(57)$ in S_8, compute $\sigma\tau$ and compute the orders of σ and τ.

$1\to 8$ $2\to 5$ $3\to 7$ $4\to 6$ $5\to 4$ $6\to 3$ $7\to 2$ $8\to 1$ $9\to 9$.

$\sigma\tau=(18)(25463 7)$

$|\sigma|=4$. $|\tau|=6$.

Question 12. Let G be a group, show that for all $a, b, c \in G$, the equation $axb = c$ has a unique solution in G.

existence: $a^{-1}, b^{-1}, c^{-1}\in G$. let $x=a^{-1}cb^{-1}$. $axb=aa^{-1}cb^{-1}b=ece=c$.

uniqueness: suppose x, y both are solutions. $axb=ayb \iff a^{-1}axbb^{-1}=a^{-1}aybb^{-1} \iff x=y$.

Question 13. Let A be an abelian group and B a subgroup of A. Prove that A/B is abelian.

claim: $B\trianglelefteq A$. pf: let $a\in A$, $aBa^{-1}=\{aba^{-1} \mid b\in B\}=\{aa^{-1}b \mid b\in B\}=B$.

$A/B=\{aB \mid a\in A\}$. let $x, y\in A/B$ $x=cB$ $y=dB$ $c, d\in A$.

$xy=cBdB=cdB=dcB=dBcB=yx$.

Question 14. Let $\phi : G \to H$ be a homomorphism, prove that $\ker(\phi)$ is a normal subgroup of G.

Normal:

let $g\in G, k\in\ker(\varphi)$ $\varphi(gkg^{-1})=\varphi(g)\varphi(k)\varphi(g^{-1})=\varphi(g)e_H\varphi(g)^{-1}=e_H$. $\Rightarrow gkg^{-1}\in\ker(\varphi)$

Subgroup:

$\phi(e_G)=e_H$. for $x, y\in\ker(\varphi)$. $\varphi(x)=\varphi(y)=e$. $\varphi(xy)=e\cdot e=e$. $\varphi(x^{-1})=\varphi(x)^{-1}=e^{-1}=e$.

Question 15. Prove that the identity element of a group is unique.

Suppose e_1, e_2 both are identity elements.

$e_1 * e_2 = e_2 * e_1 = e_1 \quad e_2 * e_1 = e_1 * e_2 = e_2 \Rightarrow e_1 = e_2$.

Question 16. Let G be a group, prove that $C_G(Z(G))$ is G (and $N_G(Z(G)) = G$).

$Z(G) = \{g \in G \mid gx = xg \ \forall x \in G\}$. $C_G(A) = \{g \in G \mid gag^{-1} = a \ \forall a \in A\} = \{g \in G \mid ga = ag \ \forall a \in A\}$

$C_G(Z(G)) = \{g \in G \mid ga = ag \ \forall a \text{ s.t. } ax = xa \ \forall x \in G\} = G$.

Question 17. Find an element of order 30 in S_{10}.

$\text{lcm} = 30$. $2 3 5$. $(1\,2)(3\,4\,5)(6\,7\,8\,9\,10)$.

Question 18. Let G be a group with identity element e. Suppose that $|G| = n$. Prove that $x^n = e$ for all $x \in G$. You may use results we proved in class.

$|G| = n \Rightarrow G$ is finite $\forall x \in G$. $|x| \mid |G| \quad x^{|G|} = e$.

Subgroup $\langle x \rangle$. $|\langle x \rangle| = |x| \mid |G|$.

10/10/2022 Monday.

Corollary: $\varphi: G \to H$ homomorphism, then ① φ injective $\iff \ker(\varphi) = \{e\}$.

② $|G|\ker(\varphi)| = |\mathrm{Im}(\varphi)|$. $G/\ker(\varphi) \cong \mathrm{Im}(\varphi)$.

pf: ① $\Rightarrow$: $\varphi(e_G) = e_H$.

If $g \in \ker(\varphi)$, $\varphi(g) = e_H$. Injective $\Rightarrow g = e_G \Rightarrow \ker(\varphi) = \{e_G\}$.

$\Leftarrow$: Suppose $\ker(\varphi) = \{e_G\}$. Suppose $\varphi(g_1) = \varphi(g_2)$ for $g_1, g_2 \in G$, WTS $g_1 = g_2$.

$\varphi(g_1)\varphi(g_2)^{-1} = e_H \iff \varphi(g_1 \cdot g_2^{-1}) = e_H \Rightarrow g_1 g_2^{-1} \in \ker(\varphi) = \{e_G\} \Rightarrow g_1 = g_2$.

proof by ▶ : $\ker(\varphi) = \{e_G\} \iff G/\{e_G\} \cong \mathrm{Im}(\varphi) \iff G \cong \mathrm{Im}(\varphi) \iff G$ injective.

Group Actions.

Cayley's Theorem: Every group of order n is isomorphic to a subgroup of S_n. ($|S_n| = n!$)

Def: A group action of Group G* on set A is a map $G \times A \to A$ satisfying $(g, a) \to g \cdot a$.

① $g_1 \cdot (g_2 \cdot a) = (g_1 * g_2) \cdot a \quad \forall g_1, g_2 \in G, a \in A$.

② $1 \cdot a = a \quad \forall a \in A$

lemma: for each fixed $g \in G$, define $\sigma_g: A \to A : a \mapsto g \cdot a$.

σ_g is a permutation of A i.e. σ_g is a bijection.

↳ symmetric group.

$\varphi: G \to S_A : g \mapsto \sigma_g$ is homomorphism.

proof: $(\sigma_{g^{-1}} \circ \sigma_g)(a) = \sigma_{g^{-1}}(g \cdot a) = g^{-1} \cdot (g \cdot a) = (g^{-1} * g) \cdot a = 1 \cdot a = a$. $\Rightarrow \sigma_{g^{-1}}$ is the inverse of σ_g. $\Rightarrow$ bijection

$\varphi(g_1 * g_2)(a) = \sigma_{g_1 * g_2}(a) = (g_1 * g_2) \cdot a = g_1 \cdot (g_2 \cdot a) = \sigma_{g_1}(\sigma_{g_2}(a)) = (\varphi(g_1) \cdot \varphi(g_2))(a)$. $\Rightarrow$ homo.

def: φ is the permutation representation associated to the action of G on A.

prop: bijection between {Actions of G on A} and {homomorphisms $G \to S_A$}.

proof: given an action $G \times A \to A : (g, a) \mapsto g \cdot a$ we can define $\varphi: G \to S_A$ via φ.

given $\varphi: G \to S_A : g \mapsto \varphi(g)$, we can define a group action $G \times A \to A : (g, a) \mapsto \varphi(g)(a)$.

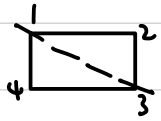
Def: The stabilizer of a in G is $G_a = \{g \in G \mid g \cdot a = a\}$. ($= g \cdot a$ by definition)

$G_a \leq G$. * Not Normal subgroup

Def: The kernel of the action is $\{g \in G \mid g \cdot a = a \ \forall a \in A\}$.

= kernel of the permutation representation.

10/12/2022 Wednesday.

Example: $G=D_8$. $A=\{1,2,3,4\}$. 

transitive define $\varphi: D_8 \to S_4$: $r \mapsto (1234)$ $s \mapsto (24)$

$\sigma_{sr} = (24)(1234) = (14)(23)$

prop: G acting on A, the relation on A defined by $a \sim b \iff a = g\cdot b$ for some $g\in G$ is an equivalence relation. for each $a\in A$. # elements in the equivalence class of $a = [G:G_a]$.

proof: ① reflexive $a = 1\cdot a \Rightarrow \forall a\in A, a\sim a$.

② Symmetric. $g^{-1}\cdot a = g^{-1}\cdot(g\cdot b) = (g^{-1}g)\cdot b = b \Rightarrow b\sim a$. $g^{-1}\in G$.

③ transitive. $\exists g\in G$ s.t. $a = g\cdot b$, $\exists h\in G$ s.t. $b = hc \Rightarrow a = g\cdot b = g\cdot(h\cdot c) = (gh)\cdot c \Rightarrow a\sim c$. $gh\in G$.

let $C_a = \{g\cdot a \in | g\in G\}$ equivalence class of a. let $b = g\cdot a \in C_a$, then gG_a is the coset of G_a.

$C_a \to \{\text{cosets of } G_a\}: b = ga \mapsto gG_a$.

$\forall g\in G, g\cdot a\in C_a \Rightarrow$ surjective.

$gG_a = hG_a \iff h^{-1}g\in G_a \iff (h^{-1}g)a = a \iff ga = ha$. $\Rightarrow$ injective.

Def: the equivalence class of a, i.e. $\{g\cdot a | g\in G\}$, is the orbit of G containing a.

the action of G on A is transitive if there is one orbit [i.e. given $a, b\in A$, $\exists g\in G, g\cdot a = b$].

Thm: let G be a group, $H\leq G$. $A = \{gH | g\in G\}$ ⇝ set of cosets. G acting on the cosets. define action $G\times A\to A: (g_1, g_2H)\mapsto (g_1g_2)H$.

left multiplication. $g\cdot aH = gaH$.

① G acts transitively on A.

② The stabilizer in G of $1H$ is H.

③ The kernel of the action is $\bigcap_{x\in G} xHx^{-1}$ = largest normal subgroup contained in H.

$1H\in A$.

generalize (take $H = \{1\}$).

10/14/2022 Friday.

Group Actions acting on themselves. $A = G$. $G\times A\to A: (g,a)\mapsto g\cdot a = ga$ left multiplication.

check if it is a group action: for $g_1, g_2\in G$, $g_1\cdot(g_2\cdot a) = g_1\cdot(g_2a) = (g_1g_2)a = (g_1g_2)\cdot a$.

$1\cdot a = 1a = a$.

proof: (1) let $aH, bH\in A$, let $g = ba^{-1}$. $g\cdot(aH) = (ba^{-1}a)H = bH$.

(2) $G_{1H} = \{g\in G | g\cdot 1H = 1H\} = \{g\in G | gH = H\} = \{g\in G | g\in H\} = H$.

(3) $\ker(\varphi_H) = \{g \in G \mid g(xH) = xH \ \forall x \in G\} = \{g \in G \mid (x^{-1}gx)H = H \ \forall x \in G\}$.

$= \{g \in G \mid x^{-1}gx \in H \ \forall x \in G\} = \{g \in G \mid g \in xHx^{-1} \ \forall x \in G\} = \bigcap_{x \in G} xHx^{-1}$.

$\ker(\varphi_H) \trianglelefteq G$. $\ker(\varphi_H) \leq H$.

if N is any normal subgroup of G contained in H, $N = xNx^{-1} \leq xHx^{-1} \ \forall x \in G$.

$N \leq \bigcap_{x \in G} xHx^{-1} = \ker(\varphi_H)$. $\Rightarrow$ the largest normal subgroup contained in H.

proof of Cayley's theorem: by ★, take $H = \{1\}$. $\Rightarrow A = G$. $\varphi_H : G \to S_G$.

$\ker(\varphi_H) = \bigcap_{x \in G} x1x^{-1} = \bigcap_{x \in G} xx^{-1} = \{1\}$.

by first isomorphism thm, $G \cong$ subgroup of S_G.

Corollary: If G finite group of order n and p is the smallest prime dividing $|G|$, then any subgroup of index p is normal.

10/17/2022 Monday.

Thm: $|orb(a)| = [G : G_a] = \frac{|G|}{|G_a|}$ Orbit-Stabilizer Theorem.

prove: let $\varphi : orb(x) \to G/G_x$ (coset.) $: g \cdot x \mapsto gG_x$ (Not homo since $orb(x)$ is not a group.)

well-defind: consider $g_1 \cdot x = g_2 \cdot x \Rightarrow g_1^{-1}g_2 \cdot x = g_1^{-1}g_1 \cdot x = x$. $g_1^{-1}g_2 \in G_x \Rightarrow g_2 \in g_1G_x$.

since cosets partition G. $g_1G_x = g_2G_x$.

injective: let $\varphi(g_1 \cdot x) = \varphi(g_2 \cdot x)$ for $g_1, g_2 \in G$. $g_1G_x = g_2G_x \Rightarrow g_2^{-1}g_1 \in G_x$.

$g_2^{-1}g_1 \cdot x = x \Rightarrow g_2 \cdot x = g_2 \cdot (g_2^{-1}g_1 \cdot x) = (g_2g_2^{-1}g_1) \cdot x = g_1 \cdot x$.

surjective

proof: let $H \leq G$. $[G : H] = p$.

$\{gH\}$ has p elements. $\varphi : G \to S_p$. let $k = \ker\varphi$. $[H : k] = k$.

then $[G : k] = [G : H][H : k] = pk$. $|G|/|k| = pk$. $|S_p| = p!$

by the first isomorphism thm, $G/k \cong \text{Im}\varphi \leq S_p$. by lagrange, $pk \mid p!$

so $k \mid (p-1)!$ all prime divisors of $(p-1)!$ are less than p. but p is the smallest prime (all prime factors of $k < p$.)

dividing $|G|$. $\Rightarrow$ smallest prime dividing $|G/k|$. (all prime factors of $k \geq p$.) $[G : k] = |G|/|k| = \frac{|G|}{|k|}$

Hence $k = 1$ ($p_1^0 p_2^0 \cdots p_n^0$) $\Rightarrow [H : k] = 1 \Rightarrow H = k \trianglelefteq G$.

Group acting on themselves by conjugation.

let $A=G$. let G acting on A via $g\cdot a=gag^{-1}$. $\forall g\in G, a\in A$.

check this is a group action: $g_1\cdot(g_2\cdot a)=g_1\cdot(g_2ag_2^{-1})=g_1g_2ag_2^{-1}g_1^{-1}=(g_1g_2)a(g_1g_2)^{-1}=g_1g_2\cdot a$

$1\cdot a=1\cdot a\cdot 1^{-1}=a$.

Def: two elements a and b of G are conjugate in G if $\exists g\in G$ s.t. $b=gag^{-1}$.

they are in the same orbit under the "conjugation action".

orbits under the "conjugation action" is called the conjugacy classes of G.

Rmk: ① if G is abelian, "conjugation action" is trivial. $gag^{-1}=gg^{-1}a=a$.

conjugate class of a is $\{a\}$.

② if $|G|>1$, "conjugation action" is not transitive.

$g1g^{-1}=gg^{-1}=1$. $orb(1)=\{1\}$. if $a\in Z(G)$, $gag^{-1}=gg^{-1}a=a$. $orb(a)=\{a\}$.

Define: if $S\subseteq G$ (subsets), $gSg^{-1}=\{gsg^{-1}\mid s\in S\}$. define $g\cdot S=gSg^{-1}$

two subsets S,T are conjugate in G if $\exists g\in G$ s.t. $T=gSg^{-1}$.

big./small.

$G_S=\{g\in G\mid gSg^{-1}=S\}=N_G(S)$.

prop: the number of conjugates of a subset S in a group $=[G:G_S]=[G:N_G(S)]$.

the number of conjugates of an element $s\in S\subseteq G=[G:G_s]=[G:N_G(S)]=[G:C_G(S)]$

Rmk: "Conjugation action" partitions G into conjugacy classes.

10/19/2022 Wednesday.

The class Equation: let G be a finite group, let $g_1,\cdots,g_r$ be representations of distinct conjugacy classes of G not contained in $Z(G)$, then

$|G|=|Z(G)|+\sum_{i=1}^{r}[G:C_G(g_i)]$.

$=\{g\in G\mid gx=xg\ \forall x\in G\}$. $C_G(A)=\{g\in G\mid gag^{-1}=a\ \forall a\in A\}$.

↱ $|k_i|>1$.

Proof: write $Z(G)=\{1,z_2,\cdots,z_m\}$, let g_i be a representations of k_i, a conjugacy class not in the center. then the set of conjugacy classes is $\{1\},\{z_2\},\cdots,\{z_m\},k_1,\cdots,k_r$.

Conjugacy classes partition $G\Rightarrow |G|=\sum_{i=1}^{m}1+\sum_{i=1}^{r}|k_i|=|Z(G)|+\sum_{i=1}^{r}[G:C_G(g_i)]$ ($=G_{g_i}$).

Prop: if G is abelian, $|G|=|Z(G)|$.

n odd: $\{1\}$, $\{r^{\pm 1}\}, \dots, \{r^{\pm \frac{n-1}{2}}\}$, $\{sr^i : 0 \le i \le n-1\}$.

n even: $\{1\}, \{r^{\frac{n}{2}}\}, \{r^{\pm 1}\}, \dots \{r^{\pm(\frac{n}{2}-1)}\}, \{r^{2i}s : 0 \le i \le \frac{n}{2}-1\}, \{r^{2i+1}s : 0 \le i \le \frac{n}{2}-1\}$.

Example: $D_8 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$. $Z(D_8) = \{1, r^2\}$. $= r^{-i}s$

r^j: $r^i r^j r^{-i} = r^j$. $(sr^i) r^j (sr^i)^{-1} = r^{-j}$

sr^j: $r^i sr^j r^{-i} = sr^{-i} r^j r^{-i} = sr^{j-2i}$ $(sr^i) sr^j (sr^i)^{-1} = sr^i sr^j r^{-i} s = r^{-i} r^{j-i} s = sr^{2i-j}$.

conjugacy classes are $\{r, r^3\}, \{s, sr^2\}, \{sr, sr^3\}, \{1\}, \{r^2\}$.

$C_{D_8}(x)$ for $x \in Z(D_8)$. $C_{D_8}(r) = \{1, r, r^2, r^3\}$. $|C_{D_8}(s)| = 4$. $|C_{D_8}(sr)| = 4$.

$|D_8| = |Z(D_8)| + \sum_{x=r,s,rs} [D_8 : C_{D_8}(x)]$ $8 = 2 + (\frac{8}{4} + \frac{8}{4} + \frac{8}{4})$

Thm: If p is prime and G is a group of order p^a $a \ge 1$, then G has non-trivial center.

proof: If $a = 1$. every group of prime order is cyclic $\Rightarrow$ abelian.

since $g_i \notin Z(G)$, $C_G(g_i) \neq G$ $[G : C_G(g_i)] \neq 1$.

G finite by lagrange. $|C_G(g_i)| \mid |G|$. $|C_G(g_i)| = p^n$ $n < a$. $\Rightarrow p \mid [G : C_G(g_i)] \Rightarrow p \mid \sum_{i=1}^{n} [G : C_G(g_i)]$.

as $p \mid |G|$, $p \mid |Z(G)|$. $\Rightarrow |Z(G)| \neq 1 \Rightarrow$ non-trivial.

Corollary: If $|G| = p^2$ for some prime p, then G is abelian. ($G \cong \mathbb{Z}/p^2\mathbb{Z}$ or $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$).

proof: by , $Z(G) \neq \{1\}$. $|Z(G)| = p$ or $p^2 \Rightarrow |G/Z(G)| = p$ or 1.

If p, every group of prime order is cyclic $\Rightarrow$ $G/Z(G)$ is cyclic $\Rightarrow$ G is abelian.

If 1, $|G| = |Z(G)| \Rightarrow G = Z(G) \Rightarrow G$ is abelian.

10/21/2022 Friday.

Cauchy's Theorem for abelian groups: If G is a finite abelian group and p is a prime dividing $|G|$, then G contains an element of order p.

proof: $p \mid |G| \Rightarrow |G| > 1 \Rightarrow \exists x \in G$ s.t. $x \neq 1$.

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

$N \trianglelefteq G \Rightarrow |G/N| = [G : N] = \frac{|G|}{|N|}$

by induction on $|G|$. If $|G| = p$. every group of prime order is cyclic. $\Rightarrow |x| = p$.

If $|G| > p$. If $p \mid |x|$. $|x| = pn$ $|x^n| = \frac{|x|}{\gcd(|x|, n)} = p$. we have an element of order p. ($|N| = |x|$)

If $p \nmid |x|$. let $N = \langle x \rangle$. every subgroup of abelian group is normal. $N \trianglelefteq G$.

$|G/N| = \frac{|G|}{|N|}$ $x \neq 1 \Rightarrow |N| \neq 1 \Rightarrow |G/N| < |G|$ $p \nmid |N| \Rightarrow p \mid |G/N|$.

induction assumption on G/N. $\exists \bar{y} = yN$ s.t. $|\bar{y}| = p$.

$\bar{y}^p = \bar{1} \Rightarrow y^p \in N$ (cyclic) $\bar{y} \neq \bar{1} \Rightarrow y \notin N$ $\Rightarrow \langle y^p \rangle \neq \langle y \rangle \Rightarrow |y^p| < |y|$

$|y^p| = \frac{|y|}{p} \Rightarrow p \mid |y|$.

$\gcd(|y|, p) = 1$ or p

Def: let G be a group and p be a prime.

A group of order p^d for some $d \geq 0$ is called a **p-group**. Subgroups of G that are p-groups are called **p-subgroups**.

If G is a group of order $p^d m$, where $p \nmid m$ then a subgroup of order p^d is called a **Sylow p-subgroup** of G.

The set of sylow p-subgroups of G is denoted as $Syl_p(G)$ and the number of sylow p-subgroups of G is denoted as $n_p(G)$.

Thm (Sylow 1): existence of sylow p-subgroup
let G be a group of order $p^d m$ where $p \nmid m$, $\exists$ sylow p-subgroup. ($Syl_p(G) \neq \phi$)

Thm (Sylow 2): if P is a sylow p-group of G and Q is any p-subgroup of G, $\exists g \in G$ s.t. $Q \leq gPg^{-1}$. (Q is contained in some conjugate of P). any two sylow p-subgroups of G are conjugate in G.

Thm (Sylow 3): $n_p(G) = kp+1$
$n_p(G) \equiv 1 \pmod p$. $n_p(G) = [G : N_G(P)]$. $n_p(G) \mid m$.

10/24/2022 Monday.

Proof of sylow 1: by induction on $|G|$.

Base Case: $|G| = 1$

induction hypothesis: Sylow p-group exist for all group of order $< |G|$.

- if $p \mid |Z(G)|$, by lemma, $\exists x \in Z(G)$ s.t. $|x| = p$. let $N = \langle x \rangle$.

let $\bar{G} = G/N$ $|G| = p^d m$, $|N| = p \Rightarrow |\bar{G}| = p^{d-1} m$ by hypothesis, $\exists \bar{P} \leq \bar{G}$ s.t. $|\bar{P}| = p^{d-1}$

by Fourth Isomorphism thm, $\bar{P} = A/N$. ($\Rightarrow$ subgroup of G/N)

Any subgroup of $Z(G)$ is normal. $\frac{|A|}{|N|} = |A/N| = |\bar{P}| = p^{d-1} \Rightarrow |A| = p \cdot p^{d-1} = p^d \Rightarrow A$ is a sylow p-subgroup of G. ($\Rightarrow$ subgroup of G containing N)

- if $p \nmid |Z(G)|$, $|G| = |Z(G)| + \sum_{i=1}^{r} [G : C_G(g_i)]$

if $p \mid [G : C_G(g_i)]$ $\forall g_i$, $p \mid |Z(G)|$ contradicts. so for some i, $p \nmid [G : C_G(g_i)]$

for this i, let $H = C_G(g_i)$ $p \nmid \frac{p^d m}{|C_G(g_i)|}$ $|H| = |C_G(g_i)| = p^d k$. $p \nmid k$. otherwise, $p \mid \frac{p^d m}{|C_G(g_i)|}$

since $g_i \notin Z(G)$, $|G| \neq |C_G(g_i)| \Rightarrow |H| = |C_G(g_i)| < |G|$.

by induction hypothesis, H has a p-sylow subgroup Q of order p^d.

since $H \leq G$, Q is a sylow p-subgroup of G.

Example: S_3

$|S_3| = 6 = 2^1 \times 3 = 3^1 \times 2$. by sylow 1. $\exists$ subgroup of order $2, 3$. (sylow 2-subgroup. / sylow 3-subgroup.)

sylow 2-subgroup: $\langle (1\ 2) \rangle, \langle (2\ 3) \rangle, \langle (1\ 3) \rangle$.

sylow 3 $\Rightarrow$ # sylow 2-subgroup $\equiv 1 \pmod 2$

sylow 3-subgroup: $\langle (1\ 2\ 3) \rangle = \langle (1\ 3\ 2) \rangle$

sylow 3 $\Rightarrow$ $1 \equiv 1 \pmod 3$

10/26/2022 Wednesday.

Rings

A ring R is a set with two binary operations + and × satisfying (Addition and multiplication might be weird in some cases.)

① $(R, +)$ is an (abelian) group. ($(R, \times)$ is monoid.)

② × is associative $(a \times b) \times c = a \times (b \times c)$

③ The distributive law holds $(a+b) \times c = (a \times c) + (b \times c)$ $a \times (b+c) = (a \times b) + (a \times c)$

④ R contains multiplicative identity $1 \in R$ $1 \times a = a \times 1 = a$ $\forall a \in R$ 0 is additive identity.

Def: A ring is called commutative if multiplication is commutative.

Rmk: $1 \in R \Rightarrow (R, +)$ is abelian. $(1+1) \times (a+b) = 1 \times (a+b) + 1 \times (a+b) = a+b+a+b$. $) =$
$(1+1) \times (a+b) = (1+1) \times a + (1 \times 1) \times b = a+a+b+b$

Example: Zero Ring $\{0\}$ $0 = 1$. Not a field.

$(\mathbb{Z}, +, \times)$ Ring ✓ Commutative ✓. Not a field.

$(\mathbb{Q}, +, \times), (\mathbb{R}, +, \times), (\mathbb{C}, +, \times)$ Ring ✓ Commutative ✓. Field.

$(\mathbb{Z}/n\mathbb{Z}, +, \times)$ Ring ✓ Commutative ✓. field iff n is prime.

$a \in \{1, \dots, p-1\}$
$\gcd(a, p) = 1$
$\exists u, v$ s.t. $au + pv = 1$
$au \equiv 1 \pmod p \Rightarrow u$ is the inverse.

$\mathbb{Z}/6\mathbb{Z}$ Not a field.

Let R be a ring. $M_n(R)$ Ring ✓ for $n \geq 2$, not commutative.

Def: A ring R is called a division ring if every nonzero element $a \in R$ has a multiplicative inverse. ($\exists b \in R$ s.t. $ab = ba = 1$).

Def: A commutative division ring is called a field.

Let X be a nonempty set and A a ring. The collection of set maps $f: X \to A$ is a ring.

$(f+g)(x) = f(x) + g(x)$ + $fg(x) = f(x)g(x)$ ×

ring axioms hold since A is a ring. $1 \in R$ is the constant fn. $\forall x \in X$, $1(x) = 1$.

R is commutative iff A is.

Lemma: R a ring, then

① $0a=a0=0 \ \forall a\in R$. pf: $0a=(0+0)a=0a+0a \Rightarrow 0a=0$

② $(-a)b=a(-b)=-(ab) \ \forall a,b\in R$. pf: $ab+(-a)b=(a-a)b=0b=0 \Rightarrow -(ab)=(-a)b$.

③ $(-a)(-b)=ab$ pf: $(-a)(-b)+a(-b)=(-a+a)(-b)=0(-b)=0 \Rightarrow (-a)(-b)=-a(-b) \overset{②}{=} --(ab)=ab$

④ $-a=(-1)a$ pf: $(-1)a+(1)a=(-1+1)a=0a=0 \Rightarrow (-1)a+a=0 \Rightarrow (-1)a=-a$.

10/28/2022 Friday.

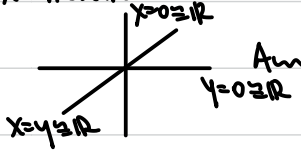
Direct Products.

Let $(G_1,*_1,\cdots,(G_n,*_n)$ be groups.

Def: The direct product $(G_1\times\cdots\times G_n,*)$ is the set of n-tuples $(g_1,\cdots,g_n)$ where $g_i\in G_i$ with operation defined componentwise $(g_1,g_2,\cdots,g_n)*(h_1,h_2,\cdots,h_n)=(g_1*_1h_1,g_2*_2h_2,\cdots,g_n*_nh_n)$.

Prop: if $G_1,G_2,\cdots,G_n$ are groups, their direct product is a group of order $|G_1|\times|G_2|\times\cdots\times|G_n|$. $G_1\times G_2\times\cdots\times G_n$ contains an isomorphic copy of each G_i.

Ex. $\mathbb{R}\times\mathbb{R}$



Any line through the origin is a copy of $\mathbb{R}$.

Prop: Let $G_1,\cdots,G_n$ be groups and let $G=G_1\times\cdots\times G_n$.

① for each fixed i, $G_i\cong\{(1,\cdots,1,g_i,1,\cdots,1)\mid g_i\in G_i\}$.

identifying G_i with this subgroup gives $G_i\trianglelefteq G$ and $G/G_i\cong G_1\times\cdots\times G_{i-1}\times G_{i+1}\times\cdots\times G_n$.

② for each fixed i, $\pi_i:G\to G_i:(g_1,\cdots,g_n)\mapsto g_i$ is a surjective homomorphism with kernel $\ker\pi_i=\{(g_1,\cdots,g_{i-1},1,g_{i+1},\cdots,g_n)\mid g_j\in G_j\ \forall j\neq i\}\cong G_1\times\cdots\times G_{i-1}\times G_{i+1}\times\cdots\times G_n$.

③ if $x\in G_i$, $y\in G_j$, $i\neq j$, then $xy=yx$. [$x=(1,\cdots,1,g_i,1,\cdots,1)$ $y=(1,\cdots,1,g_j,1,\cdots,1)$]

pf: ① by subgroup criterion, $H=\{(1,\cdots,1,g_i,1,\cdots,1)\mid g_i\in G_i\}\leq G$.

$\varphi:G_i\to H:g_i\mapsto(1,\cdots,1,g_i,1,\cdots,1)$ is an isomorphism $\Rightarrow$ we can define G_i with H.

$\pi:G\to G_1\times G_2\times\cdots\times G_{i-1}\times G_{i+1}\times\cdots\times G_n$ $(g_1,\cdots,g_n)\mapsto(g_1,\cdots,g_{i-1},g_{i+1},\cdots,g_n)$ is homomorphism and surjective. $\ker\pi=\{(g_1,\cdots,g_n)\mid g_j=1\ \forall j\neq i\}=G_i\Rightarrow G_i\trianglelefteq G$. kernel of homomorphism.

by 1st isomorphism thm, $G/G_i\cong G_1\times\cdots\times G_{i-1}\times G_{i+1}\times\cdots\times G_n$.

(G_i: ker. G/G_i: Im.)

(a,b)

Let P and Q be Sylow p-subgroups of prime order p. $P \cap Q \leq P$
by lagrange, $|P \cap Q| \mid |P| \Rightarrow |P \cap Q| = p$ or 1. P, Q distinct $\Rightarrow |P \cap Q| = 1$.

Prop: $G = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ p is a prime then G has exactly p+1 subgroups of order p.

proof: every non-identity element in G has order p and each generates a cyclic subgroup of order p. by Lagrange, distinct subgroups of order p intersect trivially. So p^2-1 nonidentity element are partitioned into subsets of size p-1. Hence $\frac{p^2-1}{p-1} = p+1$ subgroups of order p.

#non-identity elements in a (cyclic) subgroup of order p.

Fundamental theorem of finitely generated abelian groups

Def: A group G is finitely generated if there is a finite subset A of G s.t. $G = \langle A \rangle$.

if G is finitely generated and G is abelian, $A = \{a_1, \cdots, a_n\}$, every element x can be written as $x = a_1^{\lambda_1} \times a_2^{\lambda_2} \cdots \times a_n^{\lambda_n}$ $\lambda_i \in \mathbb{Z}$. (direct product).

Def: if all the a_i are of infinite order, then G is a free abelian group of rank n.

Example: $\mathbb{Z}^r = \overbrace{\mathbb{Z} \times \cdots \mathbb{Z}}^{r}$ $\mathbb{Z}^r$ is a free abelian group of rank r.

Def: $x \in G$ is called torsion if it is of finite order. Denote the subgroup of torsion elements by $TG < G$, called torsion subgroup.

if $TG = \{id\}$, G is called torsion-free. if $TG = G$, G is torsion.

Thm: let G be a finitely generated abelian group. then

① $G \cong \mathbb{Z}^r \times \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_s\mathbb{Z}$. s.t. $r, n_i \in \mathbb{Z}$, $r \geq 0$, $n_i \geq 2$ $\forall i$. $n_{i+1} \mid n_i$ for $1 \leq i \leq s-1$.

② the expression is unique.

Def: r is called the rank and n_i are called the invariant factors of G.

Rmk: Two finitely generated abelian groups are isomorphic if they have the same rank and list of invariant factors.

A finitely generated group is finite if its rank = 0.

Thus we can list all finite abelian groups of a given order n. $\Rightarrow$ enumerate $n_1, \cdots, n_s$ s.t. ① $n_j \geq 2$ for $1 \leq j \leq s$ ② $n_{i+1} \mid n_i$ $1 \leq i \leq s-1$ ③ $n_1 n_2 \cdots n_s = n$

if $p \mid n$, $p \mid n_i$ for some i $\Rightarrow p \mid n_j$ $\forall j \leq i \Rightarrow p \mid n_1$ (largest invariant factor.) every prime factor of n divides n_1. if n is the product of distinct primes, $n = n_1$.

Corollary: if n is a product of distinct primes, up to isomorphism the only (finite) abelian group of order n is $\mathbb{Z}/n\mathbb{Z}$.

Ex. $n=180=2^2\cdot 3^2\cdot 5$

possible n_1 values: ① $n_1=2^2\cdot 3^2\cdot 5=180$ ② $n_1=2^2\cdot 3\cdot 5=60$ ③ $n_1=2\cdot 3^2\cdot 5=90$ ④ $n_1=2\cdot 3\cdot 5=30$

determine the possible $n_2, n_3\cdots$ for each n_1 ① $G\cong \mathbb{Z}/180\mathbb{Z}$. ② $G\cong \mathbb{Z}/60\mathbb{Z}\times \mathbb{Z}/3\mathbb{Z}$.

③ $G\cong \mathbb{Z}/90\mathbb{Z}\times \mathbb{Z}/2\mathbb{Z}$. ④ $G\cong \mathbb{Z}/30\mathbb{Z}\times \mathbb{Z}/6\mathbb{Z}$. (2,3,6)

another way:

Thm: If G is an (finite) abelian group of order $n>1$ $n=p_1^{d_1}\cdots p_k^{d_k}$

(1) $G\cong A_1\times\cdots\times A_k$ $|A_i|=p_i^{d_i}$

(2) for each $A_i\in\{A_1,\cdots,A_k\}$ $A_i\cong \mathbb{Z}/p_i^{\beta_1}\mathbb{Z}\times\cdots\times\mathbb{Z}/p_i^{\beta_t}\mathbb{Z}$. $\beta_1\geq\beta_2\geq\cdots\geq\beta_t\geq 1$. and $\beta_1+\beta_2+\cdots+\beta_t=d_i$.

this decomposition is unique.

Ex. $|G|=180=2^2\cdot 3^2\cdot 5$ $G\cong A_1\times A_2\times A_3$ $|A_1|=2^2$ $|A_2|=3^2$ $|A_3|=5$

$A_1\cong \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/4\mathbb{Z}$ $A_2\cong\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$. or $\mathbb{Z}/9\mathbb{Z}$. $A_3\cong\mathbb{Z}/5\mathbb{Z}$.

Hence $G\cong\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}\cong\mathbb{Z}/30\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$.

$G\cong\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/9\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}\cong\mathbb{Z}/90\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$.

$G\cong\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}\cong\mathbb{Z}/60\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$.

$G\cong\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/9\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}\cong\mathbb{Z}/180\mathbb{Z}$.

prop: If $m,n\in\mathbb{Z}^+$, $\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}\cong\mathbb{Z}/mn\mathbb{Z}$ iff $\gcd(m,n)=1$.

10/31/2022 Monday.

Def: Let R be a ring.

① A nonzero element a of R is called a zero-divisor if $\exists$ nonzero $b\in R$ s.t. $ab=0$ or $ba=0$.

② A nonzero element u of R is called a unit in R if $\exists v\in R$ s.t. $uv=vu=1$. The set of units $R^\times$. ← group under $\times$

Def: A field F is a commutative ring with $1\neq 0$ s.t. every nonzero element is a unit.

Lemma: A zero divisor can't be a unit.

proof: Suppose $a\in R$, $a\in R^\times$ and $\exists b$ s.t. $ab=0$ $a\in R^\times\Rightarrow\exists v\in R$ s.t. $va=1$

$(va)b=v(ab)=v(0)=0$ $(va)b=1b=b\Rightarrow b=0$ contradicts.

Ex. ① In $\mathbb{Z}$, no 0-divisor, only units are ± 1.

② in $\mathbb{Z}/n\mathbb{Z}$, every nonzero element is either a unit or a 0-divisor.

proof: $[a]\in\mathbb{Z}/n\mathbb{Z}$. if $\gcd(n,a)=1$ $\exists x,y$ s.t. $ax+ny=1$ $ax\equiv 1 \bmod n\Rightarrow [a][x]=[1]$

otherwise, let $b=\frac{n}{\gcd(a,n)}$ $\gcd(n,a)>1$ $[b]\neq[n]=[0]$.

$ab=\frac{a}{\gcd(a,n)}n=[0]$.

Def: A commutative ring R with $1\neq 0$ is called an integral domain if it has no zero-divisors.

think of as integers.

prop: Let R be a ring without zero-divisors. Let $a,b,c\in R$, if $ab=ac$, then either $a=0$ or $b=c$.

pf: $ab=ac \Rightarrow ab-ac=0 \Rightarrow a(b-c)=0 \Rightarrow$ either $a=0$ or $b=c$.

Cor. Any finite integral domain is a field.

pf. let $a\neq 0\in R$. define $R\to R$. $x\mapsto ax$.

injective since if $ax_1=ax_2 \Rightarrow x_1=x_2$

surjective since finite $\Rightarrow \exists b$ s.t. $ab=1 \Rightarrow a$ is a unit $\Rightarrow$ every nonzero element is a unit.

Def: A subring of a ring R is an additive subgroup of R that is closed under multiplication and contains the multiplicative identity.

S is a subring if ① $[S\neq\phi]$ $0\in S$ ② $\forall a,b\in S$ $a-b\in S$

③ $\forall a,b\in S$, $ab\in S$ ④ $1\in S$.

Ex. 1) $\mathbb{Z}\subset\mathbb{Q}\subset\mathbb{R}$.

2) if R is a subring of a field F then R is an integral domain.

pf: R is a subring of $F \Rightarrow R$ is a ring and R is commutative. $a,b\in R\subset F \Rightarrow ab=ba$.

if $a\neq 0$, $a\in R\subseteq F$, a is a unit in F.

if $\exists b\neq 0\in R$ s.t. $ab=0$, $\exists b\neq 0\in F$ s.t. $ab=0$ contradicts since a can't be a zero-divisor.

11/02/2022 Wednesday.

Polynomial Ring.

largest n s.t. $a_n\neq 0 \Rightarrow$ degree n. $a_n=1 \Rightarrow f$ is monic

Def: let R be a commutative ring with $1\neq 0$, then $R[x]$ is the set of polynomials with coeffs in R. $R[x]=\{a_0+a_1x+\cdots+a_nx^n \mid a_i\in R\}$.

Operations: $(a_0+a_1x+\cdots+a_nx^n)+(b_0+b_1x+\cdots+b_nx^n)=(a_0+b_0)+(a_1+b_1)x+\cdots+(a_n+b_n)x^n$.

$(a_0+a_1x+\cdots+a_nx^n)(b_0+b_1x+\cdots+b_nx^n)=(a_0b_0)+(a_1b_0+a_0b_1)x+\cdots+(a_nb_n)x^{2n}=\sum_{i=0}^{k}a_ib_{k-i}x^k$

Thus, $R[x]$ is a ring

prop: R is a subring of $R[x]$.

Ex. ① $\mathbb{Z}[x]\subseteq\mathbb{Q}[x]\subseteq\mathbb{R}[x]$.

subring.

↳ Coeffs (0,1,2)

② $\mathbb{Z}/3\mathbb{Z}[X]$ $p(x)=x^2+2x+1$ $q(x)=x^3+x+2$

$p(x)+q(x)=x^3+x^2+3x+3=x^3+x^2$ only "reduce" at the final step.

$p(x)q(x)=x^5+2x^4+2x^3+4x^2+5x+2=x^5+2x^4+2x^3+x^2+2x+2$.

③ x^2+1 in $\mathbb{Z}[x]$ "irreducible"

x^2+1 in $\mathbb{C}[x]$ $=(x+i)(x-i)$

x^2+1 in $\mathbb{Z}/2\mathbb{Z}[x]=(x+1)^2=x^2+2x+1$.

R[x] inherits properties from R.

Prop: Let R be an integral domain, let $p(x), q(x)$ be nonzero elements of $R[x]$, then

1) $\deg(p(x)q(x))=\deg(p(x))+\deg(q(x))$.

2) $(R[x])^\times=R^\times$.

3) $R[x]$ is an integral domain.

pf: (1) $p(x)=a_nx^n+\cdots+a_0$ $q(x)=b_mx^m+\cdots+b_0$ $a_n\neq 0$ $b_m\neq 0 \Rightarrow \deg(p(x))=n$. $\deg(q(x))=m$.

$p(x)q(x)=a_nb_mx^{n+m}+\cdots+a_0b_0$ $a_nb_m\neq 0$ since R is an integral domain. $\deg=n+m$.

(3) $p(x)\neq 0$ $q(x)\neq 0 \Rightarrow p(x)q(x)\neq 0$

(2) If $p(x)$ is a unit of $R[x]$, $\exists q(x)$ s.t. $p(x)q(x)=1$.

$\deg(p(x))+\deg(q(x))=\deg(1)=0 \Rightarrow \deg(p(x))=\deg(q(x))=0 \Rightarrow p(x), q(x)$ are constants.

$p(x), q(x)$ are constants and $p(x)q(x)=1 \Rightarrow p(x), q(x)\in R^\times$.

If $a,b\in R^\times$, $ab=1 \Rightarrow ab=1$ in $R[x] \Rightarrow a,b\in R[x]^\times$.

Rmk: If R has zero divisors then so does $R[x]$.

If S is a subring of R, $S[x]$ is a subring of $R[x]$.

Question 1. Prove that $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/mn\mathbb{Z}$ iff $\gcd(m,n) = 1$.

let $\langle x \rangle = \mathbb{Z}/m\mathbb{Z}$ ($|x|=m$) $\langle y \rangle = \mathbb{Z}/n\mathbb{Z}$ ($|y|=n$). $\ell = \text{lcm}(m,n)$ $(x^\ell, y^\ell) = (1,1)$

if $\gcd(m,n) \neq 1$, $|(x,y)| < \ell$.

if $\gcd(m,n) = 1$, $|xy| = mn$ $|\langle xy \rangle| = mn$ $\langle xy \rangle \leq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \Rightarrow \langle xy \rangle = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. $\Rightarrow$ cyclic.

Question 2. Let p, q be distinct primes, show that every group of order $p^2q \neq 12$ has a normal Sylow subgroup.

$p > q$ $n_p \equiv 1 \pmod p$ $n_p \mid q$. $\Rightarrow n_p = 1 \Rightarrow$ Normal.

$p < q$. $n_q = 1$ done! $n_q = p$ or p^2 $n_q \equiv 1 \pmod q$. $\Rightarrow n_q = p^2 \Rightarrow p^2 = 1 + kq \Rightarrow (p+1)(p-1) = kq$

$q \mid p+1 \Rightarrow q = 3$ $p = 2$.
only possibility.

Question 3. Let $|G| = pqr$ $p < q < r$ are primes. Prove that G has a normal Sylow subgroup for either p, q, or r.
$n_p = 1$

$n_r \equiv 1 \pmod r$ $n_r \mid pq$. $n_r = 1$ $n_r = pq$. $pq(r-1)$ elements of order r. $p(q-1)$ elements of order q.

$pq(r-1) + p(q-1) > pqr$. $r(q-1) + q(p-1) + pq(r-1) > pqr$.

Question 4. Find all Sylow-2 subgroups and Sylow-3 subgroups of $S_3 \times S_3$.
4 9

$|S_3 \times S_3| = 6 \times 6 = 2^2 \cdot 3^2$. Sylow 2-subgroup. Sylow 3-subgroup.

$n_2 = \{1, 3, 9\}$ $n_3 = \{1, 4\}$. $((1\,2), e), ((e, (1\,2))$ $((1\,2\,3), e)$ $(e, (1\,3\,2))$
$1 \to 3$

Question 5. Suppose G is a group which acts on a set A. Let G_a denote the stabilizer of a in G. Prove that if $g \in G$ then $G_{g \cdot a} = gG_a g^{-1}$.

$G_a = \{g \in G \mid g \cdot a = a\}$. $G_{ga} = \{g \in G \mid g \cdot g \cdot a = g \cdot a\}$.

$h \cdot g \cdot a = g \cdot a \Rightarrow g^{-1} h g \cdot a = a \Rightarrow g^{-1} h g \in G_a \Rightarrow g^{-1} h g = g_1 \Rightarrow h = g g_1 g^{-1} \Rightarrow h \in g G_a g^{-1}$

Question 6. Let G be the group $\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$, find the order of the subgroup of G generated by the element $(5,5)$.

$|(5,5)| = \text{lcm}(|5|, |5|)$ $|5| = \frac{10}{\gcd(5,10)} = 2$ $|5| = \frac{12}{\gcd(5,12)} = 12$.

$= \text{lcm}(2, 12) = 12$.

Question 7. Compute the number of orbits of the action of S_3 on $\{1,2,3\}$.

$|\text{orb}(1)| = |\{g \in G \mid g \cdot 1 = 1\}|$ $|\text{orb}(a)| = \frac{|G|}{|G_a|}$.

Question 8. Let G be a group of order 15. Determine the possible class equations for G.

Abelian $|Z(G)| = |G| = 15$. $Z(G) = 3$ 5. $G/Z(G)$ prime $\Rightarrow$ cyclic $\Rightarrow$ G abelian.

$Z(G) = 1$ $3+3+3+5 = 14$. $3 \equiv 1 \bmod 5$.

Question 9. Find the number of non-isomorphic abelian groups of order 270 and list the element of highest order contained in each one.

Question 10. Let R be a ring, show that if $u \in R^\times$, then $-u \in R^\times$.

Question 11. Find the units and zero divisors of $\mathbb{Z}/15\mathbb{Z}$.

1, 2, 4, 7, 8, 11, 13, 14. 3, 5, 6, 9, 10, 12

Question 12. Find the number of elements of order 7 in a group of order $168 = 2^3 \cdot 3 \cdot 7$. You may assume the group has no nontrivial proper normal subgroups.

Question 13. Prove that $\mathbb{Z}/2\mathbb{Z}$ is isomorphic to S_2.

$\varphi : \mathbb{Z}/2\mathbb{Z} \to S_2$ homo.

$|\mathbb{Z}/2\mathbb{Z}| = |S_2| = 2$. surjective.

Question 14. Let p be a prime, and let G be a group of order p. Let X be a set with $p - 1$ elements. Prove that the only group action of G on X must be the trivial action i.e., the one for which $g \cdot x = x$ for all $g \in G$ and all $x \in X$.

$|G| = |Orb(x)||Gx|$. trivial: $|G| = |Gx|$.

nontrivial: $p = 1$ 1.. $\downarrow$ > 1 $< p-1$.

Question 15. Let G be a group and let $H \leq G$ be a subgroup with $[G : H] = n < \infty$. Prove that there exists a normal subgroup N of G such that $N \leq H$ and $[G : N]$ divides $n!$.

A = left coset. $|A| = [G:H] = n$.

$\varphi: G \to S_n$ $\ker(\varphi) = N$ (largest $\trianglelefteq$.) $\Rightarrow N \leq H$

$G/N \cong$ subgroup of S_n $[G:N] \mid n!$

Question 16. Find the conjugacy classes of D_{12}.

6. $\{1\}$ $\{r^3\}$ $\{sr, sr^3, sr^5\}$ $\{s, sr^2, sr^4\}$ $\{r, r^5\}$ $\{r^2, r^4\}$

Question 17. Let G be an infinite group whose only normal subgroups are the trivial group and the group itself. Let H be proper subgroup of G. Prove that $[G : H] = \infty$.

Question 18. Let G be the symmetric group S_n acting on the set $\{1, 2, 3, \ldots, n\}$, and let $g \in S_n$ be the n-cycle $(1\,2\,3 \cdots n)$. Prove that $C_{S_n}(g) = \langle g \rangle$.

11/09/2022 Wednesday.

Ring Homomorphism.

Def: Let R, S be rings. A **ring homomorphism** is a map $\varphi: R \to S$ satisfying

(1) $\varphi(a+b) = \varphi(a) + \varphi(b)$

(2) $\varphi(ab) = \varphi(a)\varphi(b)$

Def: $\ker\varphi = \{r \in R \mid \varphi(r) = 0\}$. ($0$: additive identity.) additive group homomorphism.

Def: A bijective ring homomorphism is an isomorphism.

Example: ① $\pi: \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$

$\pi(a+b) = [a+b] = [a] + [b] = \pi(a) + \pi(b)$ $\quad \pi(ab) = [ab] = [a][b] = \pi(a)\pi(b)$.

$\ker\pi = n\mathbb{Z}$. *not a subring. no multiplicative identity.

② $\varphi: (\mathbb{Q}[x]) \to \mathbb{Q}: p(x) \mapsto p(0)$ constant term of p.

$\varphi(p(x)+q(x)) = p(0)+q(0) = \varphi(p(x)) + \varphi(q(x))$ $\quad \varphi(p(x)q(x)) = p(0)q(0) = \varphi(p(x))\varphi(q(x))$.

$\ker\varphi$ = polys with constant term 0.

Non-Examples: Let $n \in \mathbb{Z}$. $M_n: \mathbb{Z} \to \mathbb{Z}: x \mapsto nx$ Additive group homomorphism only.

$M_n(x+y) = n(x+y) = nx+ny = M_n(x) + M_n(y)$

$M_n(xy) = nxy \neq M_n(x) M_n(y) = n^2xy$. Ring homo iff $n = n^2$ i.e. $n = 0$ or 1.

prop: ① $\ker\varphi$ is an additive subgroup of R.

② if $a \in \ker\varphi$, then $ra, ar \in \ker\varphi$ $\forall r \in R$.

pf: if $r \in R$, $\varphi(ra) = \varphi(r)\varphi(a) = \varphi(r)\cdot 0 = 0$. $ra \in \ker\varphi$.

$\varphi(ar) = \varphi(a)\varphi(r) = 0 \cdot \varphi(r) = 0$ $ar \in \ker\varphi$.

Quotient Ring.

Let $\varphi: R \to S$ be a surjective ring homomorphism with $\ker\varphi = I$. ($S = \varphi(R)$)

$R/I \cong S$ $\quad r + I \mapsto \varphi(r)$ want R/I to be a ring.

$(r_1+I) + (r_2+I) \to \varphi(r_1) + \varphi(r_2) = \varphi(r_1+r_2)$ $\quad$ ($:= (r_1+r_2)+I$)

$(r_1+I) \times (r_2+I) \to \varphi(r_1)\varphi(r_2) = \varphi(r_1r_2)$ $\quad$ ($:= r_1r_2 + I$.)

Def: $(r+I) + (s+I) = r+s+I$ $\quad (r+I) \times (s+I) = rs+I$.

Def: Let R be a ring. $I \subseteq R$ is called an ideal of R if ① $(I, +) \leq (R, +)$

② $\forall r \in R, i \in I, ri \in I, ir \in I$.

Corollary: A subset $I \subseteq R$ is an ideal iff it is the kernel of some ring homomorphism.

11/14/2022 Monday.

Thm: if $\varphi: R \to S$ is a ring homomorphism, then $R/\ker(\varphi) \cong \varphi(R)$.

Ex. ① $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$. kernel of $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$.

② $R = \mathbb{Z}[x]$ let $I := \{\sum_{i=0}^{n} a_i x^i \mid a_0 = a_1 = 0\}$. polys whose terms are of at least degree 2.

Claim: I is an ideal.

proof: $(I, +) \leq (R, +)$ closed under addition; contains identity; inverse $(g^{-1} := -g)$.

$\forall f(x) \in \mathbb{Z}[x]$ $f(x) \cdot I \in I$ $I \cdot f(x) \in I$.

two polys $p(x)$ and $q(x)$ are in the same coset of I iff they differ by a poly with $a_0 = a_1 = 0$ $p(x) + I = q(x) + I \iff p(x) - q(x) \in I \iff p(x) - q(x)$ has $a_0 = a_1 = 0$.

the complete set of representatives of R/I is given by poly $ax + b$ $(\overline{(ax+b)+I} = \overline{ax+b})$ in $\mathbb{Z}[x]/I$, $\bar{x} \cdot \bar{x} = \bar{x}^2 = 0$ since $\bar{x}^2 \in I$. ($\bar{x}^2$ ~ degree 2.) $\Rightarrow R/I$ has zero divisors even if $R = \mathbb{Z}[x]$ does not.

Def: let I, J be ideals of R.

① The sum of I and J is $I + J = \{a + b \mid a \in I, b \in J\}$.

② The product of I and J is the set of all finite sums of elements of the form ab with $a \in I$, $b \in J$. i.e. $IJ = \{\sum_{i=1}^{n} a_i b_i \mid a_i \in I, b_i \in J\}$. $n \geq 1$

③ for $n \geq 1$, define the n^{th} power of I, denoted I^n to be the set consisting of all finite sums of elements of the form $a_1 \cdots a_n$ with $a_i \in I$ $\forall i$.

i.e. $I^n = \{\sum_{i=1}^{k} a_{i1} \cdots a_{in} \mid a_{ij} \in I\}$.

Rmk: ① $I + J$ and IJ are ideals.

$I + J$ is the smallest ideal containing both I and J, and $IJ \subseteq I \cap J$.

② $\{ab \mid a \in I, b \in J\}$ is not necessarily closed under addition $\Rightarrow$ Not an ideal in general.

Example: in $\mathbb{Z}$, let $I = 6\mathbb{Z}$, $J = 10\mathbb{Z}$. $I + J = \{6x + 10y \mid x, y \in \mathbb{Z}\}$.

$\forall a \in I + J$, $\gcd(6, 10) = 2 \mid a \Rightarrow I + J \subseteq 2\mathbb{Z}$.

$2 = 6 \times 2 + 10 \times -1 \Rightarrow 2 \in I + J \Rightarrow 2\mathbb{Z} \in I + J \Rightarrow 2\mathbb{Z} = I + J \Rightarrow 2\mathbb{Z} = 6\mathbb{Z} + 10\mathbb{Z}$.

this is true in general. $m\mathbb{Z}+n\mathbb{Z}=\gcd(m,n)\mathbb{Z}$.

$\bar{I}\bar{J}$ = finite sums of elts of the form $6x\cdot 6y=6\cdot 6xy$. $\Rightarrow \bar{I}\bar{J}=6\cdot\mathbb{Z}$.

11/16/2022 Wednesday.

Ex. $I=\{$polynomials with even constant term$\}\subset\mathbb{Z}[X]$.

$X^2+4\in I\cdot I$ can't write X^2+4 as a single product of 2 elements in I. $\Rightarrow \bar{I}\bar{J}=\{\sum_{i=1}^{n}a_ib_i\}\neq\{a_ib_i\}$. ($x,z\in I$)

Prop: Suppose R is a commutative ring.

(1) Let $A\subset R$ be a subset. (A) = ideal generated by A = the smallest ideal of R containing A.
$= \text{ideal}\bigcap_{I\supseteq A} I$.

(2) An ideal generated by a single element is called a principal ideal (a).

(3) An ideal generated by a finite set is called finitely generated.

If $A=\{a_1,\cdots,a_n\}$, write $(a_1,\cdots,a_n)$.

$(a_1,\cdots,a_n)=\{r_1a_1+\cdots+r_na_n \mid r_i\in R, a_i\in A, n\in\mathbb{Z}^+\}$.

↳ trivial ideal

Ex. (1) $0=(0)$ $R=(1)$ principal ideal.

(2) in $\mathbb{Z}$, $n\mathbb{Z}=(n)$ and every ideal of $\mathbb{Z}$ is of this form.

$\Rightarrow$ every ideal of $\mathbb{Z}$ is principal $(m,n)=(\gcd(m,n))$.

(3) in $\mathbb{Z}[X]$, the ideal $(2,X)$ is not principal.

Proof: $(2,X)=\{2p(X)+Xq(X) \mid p(X),q(X)\in\mathbb{Z}[X]\}$.

$=2a_0+2a_1X+2a_2X^2+\cdots+2a_nX^n+Xb_0+Xb_1X+\cdots+Xb_nX^n$

$=2a_0+(2a_1+b_0)X+(2a_2+b_1)X^2+\cdots$ even constant term $\Rightarrow (2,X)\neq\mathbb{Z}[X]$.

Suppose $(2,X)=(a(X))$. Since $2\in(a(X))$, $\exists p(X)$ s.t. $2=a(X)p(X)$ ($(a(X))=\{ra(X)\mid r\in R\}$.)

$a(X)$ and $p(X)$ have degree 0. $\Rightarrow a(X),p(X)=\{\pm1,\pm2\}$.

$a(X)\neq\pm1$ since $(a(X))\neq\mathbb{Z}[X]$.

If $a(X)=\pm2$, since $X\in(a(X))$, $\exists q(X)\in\mathbb{Z}[X]$ s.t. $X=\pm2\cdot q(X)$

$q(X)$ has integer coeff. $\Rightarrow$ contradicts.

Prop: I an ideal of R ① $I=R\Leftrightarrow I$ contains a unit.

② If R is commutative: R field $\Leftrightarrow$ its only ideals are (0) and R.

Proof: ① $\Rightarrow$: if $I=R$, I contains 1 which is a unit.

$\Leftarrow$: let u be a unit in I with inverse v. $\forall r\in R, r=r\cdot 1=r(vu)=(rv)u\in I \Rightarrow R=I$.

② $\Rightarrow$: if R is a field, every nonzero element is a unit

if I has nonzero elements, $I=R$. if not, $I=(0)$.

$\Leftarrow$: let $u\neq 0\in R$, $(u)=R$, $1\in(u)\Rightarrow \exists v$ s.t. $1=uv \Rightarrow u$ is a unit $\Rightarrow R$ is a field.

Cor: If R is a field, then any nonzero ring homomorphism from R to another ring is an injection.

pf: $\ker\varphi$ is an ideal of $R \Rightarrow \ker\varphi=0$ or R. φ is not the zero homomorphism $\Rightarrow \ker\varphi=0$.

11/18/2022 Friday. ring with unique maximal ideal $\Rightarrow$ local.

Def: An ideal M of R is maximal if $M\neq R$ and the only ideals containing M are M and R.
i.e. if $M\subseteq I\subseteq S$ and I is an ideal, $I=S$ or $I=M$.

Existence of Maximal ideal:

Let R be a ring. Every ideal $I\neq R$ is contained in a maximal ideal of R.

Zorn's lemma: Let $(A,\leq)$ be a partially ordered set s.t. every ordered chain ($X_1\subseteq X_2\subseteq\cdots$, infinite/finite.) has an upper bound (subset) in A, then A has a maximal element.

proof: Let R be a ring, ideal $I\neq R$ (proper ideal.) Let $S=\{k \mid k \text{ an ideal}, I\subseteq k\subsetneq R\}$ ordered by inclusion.

Consider a chain $C: J_1\subseteq J_2\subseteq\cdots$ in S. Let $J=\bigcup_{J_i\in C} J_i$

J is an ideal of R, J contains I, $J\neq R$ (if $J=R$, $1\in J\Rightarrow \exists J_i$ s.t. $1\in J_i \Rightarrow R=J_i$. contradicts).

J is in S and J contains all $J_i \Rightarrow J$ is an upper bound for C in S.

by Zorn's lemma, $\exists m\in S$ that is maximal $\Rightarrow$ a maximal proper ideal containing I.

Prop: (R is commutative) M is a maximal ideal if R/M is a field.

proof: ideals of R containing M correspond bijectively to ideals of R/M.

M maximal $\Rightarrow$ only ideals of R/M are (0) and R/M. $\Rightarrow R/M$ is a field.

Ex. ① $n\mathbb{Z}\subset\mathbb{Z}$. is maximal $\Leftrightarrow \mathbb{Z}/n\mathbb{Z}$ is a field $\Leftrightarrow n$ is prime. ($n\neq 1$)

② $(2,X)\subset\mathbb{Z}[X]$ is maximal since $\mathbb{Z}[X]/(2,X)\cong\mathbb{Z}/2\mathbb{Z}$.

$\varphi:\mathbb{Z}[X]\to\mathbb{Z}/2\mathbb{Z}: P(X)\mapsto P(0) \bmod 2$.

③ (X) in $\mathbb{Z}[X]$ is not maximal since $\mathbb{Z}[X]/(X) \cong \mathbb{Z}$ ↷ not a field. $\varphi: \mathbb{Z}[X] \to \mathbb{Z}: p(X) \mapsto p(0)$

Also since $(X) \subset (2, X) \subset \mathbb{Z}[X]$

Def: Assume R is commutative, an ideal P is called a prime ideal if $P \neq R$ and whenever the product ab of $a, b \in R$ is an element of P, $a \in P$ or $b \in P$. (or both)

Rmk: prime ideals of $\mathbb{Z}$ are $p\mathbb{Z} = (p)$ (p prime) And (0).

Prop: R commutative ring, P is a prime ideal $\Leftrightarrow$ R/P is an integral domain.

Proof: P is a prime ideal $\Leftrightarrow P \neq R$, $ab \in P \Rightarrow a \in P$ or $b \in P$.

Consider R/P. Let $\bar{a} = a + P$. $\bar{b} = b + P$. $a \in P \Leftrightarrow \bar{a} = 0$

P is prime ideal $\Leftrightarrow \bar{R} \neq \bar{0}$; whenever $\overline{ab} = \bar{a}\bar{b} = 0$, $\bar{a} = 0$ or $\bar{b} = 0$. ($\bar{R} \neq \bar{0}$ since $P \neq R$.) $\Leftrightarrow R/P$ is an integral domain. (no zero divisor).

Corollary: R commutative: Every maximal ideal is prime. Not conversely.

Proof: M maximal $\Rightarrow R/M$ field $\Rightarrow R/M$ integral domain $\Rightarrow M$ prime ideal.

Ex. ① ideals (p) in $\mathbb{Z}$ are both maximal ideals AND prime ideals.

(0) in $\mathbb{Z}$ is prime but Not maximal.

② (X) in $\mathbb{Z}[X]$ is prime but Not maximal.

(0) in $\mathbb{Z}[X]$ is prime but Not maximal.

③ R commutative Ring. $\varphi: R[X] \to R: f(X) \mapsto f(0)$. $\ker\varphi = (X)$ $R[X]/(X) \cong R$. $(X) = \{xr(x) \mid r(x) \in R[X]\}$.

11/21/2022 Monday.

Euclidean Domain. Principal Ideal Domain (PID) Unique Factorization Domain (UFD).

Def: let R be an integral domain. Any function $N: R \to \mathbb{Z}^+ \cup \{0\}$ with $N(0) = 0$ is called a norm. measure of size in R.

Def: R is a Euclidean domain if $\exists$ a norm N on R s.t. for any $a, b \in R$ with $b \neq 0$ $\exists q, r \in R$ with $a = qb + r$ with $r = 0$ or $N(r) < N(b)$.

Euclidean domains are integral domains w/ division algorithm.

Ex. (0) Fields are Euclidean domains.

for $a, b \neq 0 \in F$, $a = qb + 0$ take $q = ab^{-1}$. (define $N(a) = 0$ for $a \in F$).

(1) $\mathbb{Z}$ is a Euclidean domain with norm given by $N(a) = |a|$.

(2) if F is a field, $F[X]$ is a Euclidean domain with norm $N(p(x)) = \deg(p(x))$.

Prop: Every ideal in a Euclidean domain is principal.

Pf: If $I=(0) \Rightarrow$ principal.

Assume $I \neq (0)$, let d be any nonzero element of minimal norm in I. $d \in I \Rightarrow (d) \subseteq I$.

WTS $I \subseteq (d)$. Let a be any element $\in I$ with $a = qd + r$ $r=0$ or $N(r) < N(d)$.

then $r = a - qd \in I$ d is of minimal norm $\Rightarrow r=0$ (can't be $N(r)<N(d)$)

$a = qd \in (d) \Rightarrow I \subseteq (d)$

Ex. $R = \mathbb{Z}[X]$ $(2, X)$ is not principal $\Rightarrow R = \mathbb{Z}[X]$ is Not a Euclidean domain.

Def. R a commutative ring. $a, b \in R$. $b \neq 0$.

1) a is a multiple of b if $\exists x \in R$ s.t. $a = xb$. We say $b \mid a$ b divides a.

2) a greatest common divisor of a and b is a nonzero element d s.t.

① $d \mid a$ and $d \mid b$ ② if $d' \mid a$ and $d' \mid b$, then $d' \mid d$.

Rmk: $b \mid a \Leftrightarrow a \in (b) \Leftrightarrow (a) \subset (b)$.

Rewrite ① $(a, b) \subset (d)$. ② if $(a, b) \subset (d') \Rightarrow (d) \subset (d')$.

Def: A principal ideal domain (PID) is an integral domain in which every ideal is principal.

Cor. Every Euclidean domain is a PID.

Ex. (1) Every field is a PID.

(2) $\mathbb{Z}[X]$ is not a PID $(2, X)$.

Prop. Every nonzero prime ideal in a PID is maximal.

Proof: Let (p) be a nonzero prime ideal. Let (m) be such that $(p) \subset (m)$.

Want to show $(m) = R$ or $(m) = (p)$.

$p \in (m) \Rightarrow \exists r \in R$ s.t. $p = rm$. p is prime, $rm \in (p) \Rightarrow$ either $r \in (p)$ or $m \in (p)$.

If $m \in (p)$, $(m) \subset (p) \Rightarrow (m) = (p)$.

If $r \in (p)$, $r = ps$ for some $s \in R$. $p = rm = psm \Rightarrow p - psm = 0 \Rightarrow p(1 - sm) = 0$.

R integral domain, $(p) \neq (0) \Rightarrow 1 - sm \in (m) \Rightarrow (m) = R$.

Def: Let R be an integral domain, $r \in R$.

① r is irreducible if it is nonzero, not a unit, if $r = ab$ for $a, b \in R \Rightarrow$ at least one of a, b is a unit. Otherwise, r is reducible.

② p s.t. $0 \neq p \in R$ is called **prime** if (p) is a prime ideal.

③ a and b are **associates** if $a = ub$ for some $u \in R^\times$.

Prop: In an integral domain, if $p \neq 0$ is prime then p is irreducible.

Pf: Suppose p is prime, (p) is a prime ideal. $p = ab \in (p) \Rightarrow$ either $a \in (p)$ or $b \in (p)$.

if $a \in (p)$, $\exists r \in R$ s.t. $a = pr \Rightarrow p = ab = prb \Rightarrow rb = 1 \Rightarrow b$ is a unit.

Prop: In a PID, a nonzero element is prime iff it is irreducible.

Pf: $\Leftarrow$: if M is an ideal containing (p), PID $\Rightarrow M = (m)$, $p \in (m) \Rightarrow p = mr$ for some $r \in R$.

p is irreducible, r is a unit or m is a unit. $\Rightarrow (p) = (m)$ or $(m) = (1) = R$.

any ideal containing (p) is (p) or $R \Rightarrow (p)$ is maximal $\Rightarrow (p)$ is prime. $\Rightarrow p$ is prime.

Def: A **unique factorization domain (UFD)** is an integral domain R in which every nonzero nonunit element satisfies

① $r = p_1 \cdots p_n$ $p_i \in R$ are irreducible.

② the decomposition is unique up to associates.

i.e. if $r = q_1 q_2 \cdots q_m$ and q_i irreducible then $m = n$ and there is a re-ordering s.t. p_i and q_i are associates.

Ex. (1) Any field is a UFD.

(2) $\mathbb{Z}$ is a UFD.

Non-Ex: $\mathbb{Z}[2i] = \{a + 2bi \mid a, b \in \mathbb{Z}\}$ $i^2 = -1$.

$4 = 2 \cdot 2 = -2i \cdot 2i$ $i \notin \mathbb{Z}[2i] \Rightarrow i$ not a unit $\Rightarrow 2$ and $-2i$, 2 and $2i$ not associates.

Thm: Every PID is a UFD.

Prop: In a UFD, a nonzero element is prime iff it is irreducible.

Thm. Field $\subset$ Euclidean Domains $\subset$ PID $\subset$ UFD $\subset$ integral Domains.

Ex. $\_ \subset \mathbb{Z} \subset \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right] \subset \mathbb{Z}[x] \subset \mathbb{Z}[\sqrt{-5}]$

Polynomial Rings.

Thm. Let F be a field. The poly ring $F[x]$ is a Euclidean domain.

if $a(x), b(x) \in F[x]$, $b(x) \neq 0$, there are unique $q(x)$ and $r(x)$ in $F[x]$ s.t. $a(x) = q(x)b(x) + r(x)$ with $r = 0$ or $\deg(r(x)) < \deg(b(x))$.

Cor. if F is a field, $F[x]$ is a PID and a UFD.

Ex. $\mathbb{Q}[x]$. $(2,x)$ is principal in $\mathbb{Q}[x]$ because 2 is a unit in $\mathbb{Q}[x]$.

Def: The poly ring in $x_1 \cdots x_n$ with coeffs in R is $R[x_1, \cdots, x_n]$.

Idefine inductively $R[x_1, \cdots, x_n] = R[x_1, \cdots, x_{n-1}][x_n]$.)

Idements look like sums of $a x_1^{d_1} \cdots x_n^{d_n}$ $a \in R$, $d_i \geq 0$, with degree $\sum_{i=1}^{n} d_i = d$.)

the degree of a poly in $R[x_1, \cdots, x_n]$ is the largest degree among its monomials.

Ex. $\mathbb{Z}[x,y]$ $p(x,y) = 2x^3 + xy - y$ $\deg(p(x,y)) = 3$.

$q(x,y) = 5x^4 + x^2y^3 + x$ $\deg(q(x,y)) = 5$.

11/28/22 Monday.

Ex. $\mathbb{Q}[x]$ is a PID

$\mathbb{Q}[x,y] = \mathbb{Q}[x][y]$ not a PID. e.g. (x,y) is not principal. $\mathbb{Q}[x]$ not a field.

Thm: R is a UFD $\iff$ $R[x]$ is a UFD.

mrk: a poly ring in any number of variables in a UFD is also a UFD. ($R[x_1, \cdots, x_n]$)

Ex. $\mathbb{Z}[x]$ UFD, $\mathbb{Z}[x,y]$ UFD but not PIDs.

Gauss's Lemma: (let R be UFD. let F be the smallest ring containing R in which all nonzero elements of R are units (field of fractions of R). (let $p(x) \in R[x]$. if $p(x)$ is reducible in $F[x]$, $p(x)$ is reducible in $R[x]$.

Corollary: let R be a UFD. suppose the gcd of the coeff of $p(x) \in R[x]$ is 1, then $p(x)$ is irreducible in $R[x]$ iff $p(x)$ is irreducible in $F[x]$.

pf: $\Rightarrow$: Gauss's Lemma. (contrapositive.)

$\Leftarrow$: gcd of coeff of $p(x)$ is 1 $\Rightarrow$ if $p(x)$ is reducible in $R[x]$, then $p(x) = a(x)b(x)$ where neither $a(x)$ nor $b(x)$ are constant poly in $R[x]$. $\Rightarrow$ $p(x)$ is reducible in $F[x]$.

mrk: if $p(x)$ is monic and irreducible in $R[x]$, then $p(x)$ is irreducible in $F[x]$.

Prop: let F be a field. $p(x) \in F[x]$. $p(x)$ has a factor of degree 1 iff $p(x)$ has a root in F.

pf: $\Rightarrow$: $p(x) = (x-2)p'(x) \Rightarrow p(2) = 0$.

$\Leftarrow$: since $F[x]$ is a ED, by the division algorithm, $p(x) = q(x)(x-2) + r$.

Suppose $p(2) = 0$. $\Rightarrow r = 0 \Rightarrow (x-2)$ is a factor.

Cor: A poly of degree 2 or 3 over a field F is reducible. $\Leftrightarrow$ it has a root in F.

Eisenstein's Criterion: P is a prime ideal of an integral domain R. Let $f(x)=x^n+\cdots+a_0$ be a poly in $R[x]$ of deg $n\geq 1$. Suppose $a_{n-1},\cdots,a_0\in P$ and $a_0\notin P^2$, then $f(x)$ is irreducible in $R[x]$.

Eisenstein's Criterion for $\mathbb{Z}$: Let p be a prime in $\mathbb{Z}$. Let $f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_0$ $(n\geq 1)$ in $\mathbb{Z}[x]$. Suppose $p|a_i$ for $0\leq i\leq n-1$ but $p^2\nmid a_0$, then $f(x)$ is irreducible in $\mathbb{Z}[x]$. $\Rightarrow f(x)$ is irreducible in $\mathbb{Q}[x]$.

Ex. ① $x^4+10x+5$. Eisenstein with $p=5\Rightarrow$ irreducible.

② x^n-p Eisenstein with $p\Rightarrow$ irreducible for all n.

③ $x^4+1\Rightarrow x\mapsto x+1$. $x^4+4x^3+6x^2+4x+2$ Eisenstein with $p=2\Rightarrow$ irreducible.

11/30/22 Wednesday.

Field Extensions.

Def: If K is a field containing a subfield F, then K is an extension field of F, denoted $K|F$ or $\overset{K}{|}F$.

The degree of $K|F$ denoted $[K:F]$ is the dimension of K as a vector space over F.

i.e. $\dim_F K=[K:F]$.

Think: A basis of K over F is a subset $\{x_1,\cdots,x_n\}\subseteq K$ s.t. every $x\in K$ can be uniquely expressed as a linear combination $\lambda_1x_1+\lambda_2x_2+\cdots+\lambda_nx_n$ where $\lambda_i\in F$.

Ex. 1) $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2$. $\{1,\sqrt{2}\}$ $a+b\sqrt{2}$. $a,b\in\mathbb{Q}$.

2) $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]=3$. $\{1,\sqrt[3]{2},\sqrt[3]{2^2}\}$. $a+b\sqrt[3]{2}+c\sqrt[3]{2^2}$ $a,b,c\in\mathbb{Q}$.

3) $[\mathbb{Q}(w):\mathbb{Q}]=2$. $w=\frac{1}{2}+\frac{\sqrt{3}}{2}i$. $\{1,w\}$. $w^3=1$, $w\neq 1\Rightarrow\frac{w^3-1}{w-1}=0\Rightarrow w^2+w+1=0\Rightarrow w^2=-1-w$.

Lemma: Let $\varphi:F\to F'$ be a homomorphism of fields, then φ is either identically 0 or it is injective, so the image of φ is either 0 or is isomorphic to F.

Thm: Let F be a field, $p(x)\in F[x]$ an irreducible polynomial, then there exist a field K containing an isomorphic copy of F in which $p(x)$ has a root. (i.e. $K|F$ s.t. $p(x)$ has a root.).

Pf: Consider $K=F[x]/(p(x))$.

$p(x)$ irreducible $\Rightarrow (p(x))$ prime ideal $\Rightarrow$ since in PID, $(p(x))$ maximal ideal $\Rightarrow K$ is a field.

Consider $\pi:F[x]\to F[x]/(p(x))=K$. $\varphi=\pi|_F:F\to F[x]/(p(x))$.

Since $\varphi(F) \neq 0$ b/c $\varphi(1)=1$, $\varphi(F) \cong F$. $\Rightarrow k$ contains an isomorphic copy of F.

Suppose $\overline{x}=\pi(x)$. $p(\overline{x}) = \overline{p(x)} = p(x) \bmod (p(x)) = 0$. ($\pi$ homomorphism) $\Rightarrow k$ contains a root of $p(x)$.

Thm Let $p(x) \in F[x]$ be irreducible of degree n. Let $k = F[x]/(p(x))$. Let $\theta = x \bmod (p(x)) \in k$. Then the elements $\{1, \theta, \theta^2, \dots, \theta^{n-1}\}$ are a basis for k as a vector space over F. Hence $[k:F]=n$ and $k = \{a_0 + a_1\theta + a_2\theta^2 + \cdots + a_{n-1}\theta^{n-1} \mid a_0, \dots, a_{n-1} \in F\}$.

pf: Let $a(x) \in F[x]$. $F[x]$ is a Euclidean Domain $\Rightarrow a(x) = q(x)p(x) + r(x)$ where $r(x)=0$ or $\deg(r(x)) < \deg(p(x))$.

$a(x) \equiv r(x) \bmod (p(x)) \Rightarrow$ every residue class in k is represented by a poly of degree $< n$.

So $\{1, \theta, \theta^2, \dots, \theta^{n-1}\}$ spans k. (↱ images of $1, x, x^2, \dots, x^{n-1}$ under the quotient.)

Suppose not lin. indep. i.e. $\exists b_0, \dots, b_{n-1} \in F$ not all zeros s.t. $b_0 + b_1\theta + b_2\theta^2 + \cdots + b_{n-1}\theta^{n-1} = 0$ in k. (↱ $0 \bmod (p(x))$) i.e. $p(x) \mid b_0 + b_1\theta + \cdots + b_{n-1}\theta^{n-1}$ $\deg(p(x)) = n > n-1 \Rightarrow$ contradicts.

Think: Elements of $F[x]/(p(x))$ are polys of degree $< n$ in θ s.t. $\theta \in k$ with $p(\theta)=0$.

Ex. 1) $\mathbb{R}[x]/(x^2+1)$ $\theta^2+1=0 \Rightarrow \theta = i$ $\{1, i\}$. $\Rightarrow \mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$

2) $\mathbb{Q}[x]/(x^2+1) \cong \mathbb{Q}(i) = \{a+bi : a, b \in \mathbb{Q}\}$

3) $\mathbb{Q}[x]/(x^3-2)$ by Eisenstein, x^3-2 irreducible. $\mathbb{Q}[x]/(x^3-2) \cong \{a+b\theta+c\theta^2 \mid a, b, c \in \mathbb{Q}\}$. $\theta^3 = 2$.