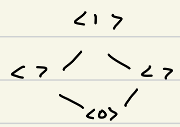
STRATEGIES

- Show uniqueness : let x_1, x_2 both be the ___, and show $x_1 = x_2$.
- Show inverse : manipulate equation to get e
- Show $o(xy) \mid o(x)o(y)$: show $xy^{o(x)o(y)} = e$
- Find order of element (x, y, z) in $\mathbb{Z}_a \times \mathbb{Z}_b \times \mathbb{Z}_c$: $o((x,y,z)) = \operatorname{lcm}(o(x), o(y), o(z))$ where $o(x) = \dfrac{a}{(a,x)}$
- Prove set equality : show $A \subseteq B$ and $B \subseteq A$

  ↳ let $x \in A$.

  show $x \in B$. Thus, $B \subseteq A$

- Prove iff : $\Rightarrow$ and $\Leftarrow$ direction
- Prove subgroup :
  1) nonempty
  2) closed under $*$
  3) closed under inverses
- Find subgroups of $(\mathbb{Z}_n, +)$ → divisors of n →



Section 0: Sets + Induction

- Thm 0.1

  Let S, T be sets. $S \subseteq T$ iff $S \cap T = S$

Section 1: Binary Operations

- symmetric difference of A and B $(A \Delta B)$: the set of elements that belong to either A or B, but not both;

  $A \Delta B = (A - B) \cup (B - A)$ or $(A \cup B) - (A \cap B)$

  - $A \Delta A = \emptyset$
  - $A \Delta \emptyset = A$

Section 2: Groups

- group: ① G is a set, and $*$ is a $\underbrace{\text{binary operation}}^{\text{bin op}}$ on G.

  ② $*$ is associative [ie, $a*(b*c) = (a*b)*c$]

  ③ $\exists\, e \in G$ s.t. $\forall\, g \in G$, $ge = eg = g$ → identity element

  ④ $\forall\, g \in G$, $\exists\, g^{-1} \in G$, s.t. $gg^{-1} = g^{-1}g = e$ → inverse

  Then, $(G, *)$ is a group.

- abelian group: if the group is commutative (ie, $ab = ba$)

Section 3: Thms

- Thm 3.1

  If G is a group, then e is unique.

- Thm 3.2

  If G is a group and $g \in G$, then g has a unique inverse.

- Thm 3.3

  If G is a group and $g \in G$, then $(g^{-1})^{-1} = g$.

- Thm 3.4

  If G is a group and $x, y \in G$, then $(xy)^{-1} = y^{-1} * x^{-1}$.

- Thm 3.5

  Let G be a group and $x, y \in G$. Suppose that either $xy = e$ or $yx = e$. Then, $y = x^{-1}$.

- Thm 3.6

  Let G be a group, and $x, y, z \in G$. Then,

  left cancellation: if $xy = xz$, $y = z$.
  right cancellation: if $yx = zx$, $y = z$.

Section 4: Powers of an Element

- $x^0 = e$
- $x^n = \underbrace{(x)(x)\cdots(x)}_{n \text{ times}}$ for $n \in \mathbb{Z}^+$
- $x^{-n} = (x^{-1})(x^{-1})\cdots(x^{-1})$ for $n \in \mathbb{Z}^+$
  $= (x^{-1})^n$

- Thm 4.1

  Let G be a group, and $x \in G$. Let $m, n \in \mathbb{Z}$. Then:

  1. $x^m \cdot x^n = x^{m+n}$
  2. $(x^n)^{-1} = x^{-n}$
  3. $(x^m)^n = x^{mn}$

- If G is a group and $x \in G$, then x is of finite order if $\exists$ a positive integer n s.t. $x^n = e$.
  If such an integer exists, then the smallest such integer is the order of x $\rightarrow$ $O(x) = n$.

  - If x is not of finite order, then x is of infinite order $\rightarrow$ $O(x) = \infty$
  - If $O(x) = 1$, $x = e$.
  - Cor 4.6: If $G = \langle x \rangle$, $|G| = O(x)$

- gcd(m, n): greatest common divisor

- Euclidean Algo

  Ex. Compute (1071, 462).

  (1) $1071 = 2 \cdot 462 + 147$

  (2) $462 = 3 \cdot 147 + 21$

  (3) $147 = 7 \cdot 21 + 0$

  $(m, n) = 21$

- Thm 4.2

  If $m, n \in \mathbb{Z}$, not both 0, there $\exists$ ints x, y s.t. $mx + ny = \gcd(m, n)$

- Thm 4.3

  If $r, s, t \in \mathbb{Z}$, $r \mid st$ and $\gcd(r, s) = 1$. Then, $r \mid t$.
  ↳ relatively prime

PROBLEM: Fix $n \in \mathbb{Z}^+$, $m \in \mathbb{Z}_n$.
Then, $O(m) = \frac{n}{\gcd(m,n)}$

Thm 4.4

Let G be a group and $x \in G$. Then,

1. $O(x) = O(x^{-1})$
2. If $O(x) = n$ and $x^m = e$, then $n \mid m$.
3. If $O(x) = n$ and $(m,n) = d$, then $O(x^m) = \frac{n}{d}$.

- a group is cyclic if $\exists$ an element $x \in G$ s.t. $G = \{x^n \mid n \in \mathbb{Z}\} = \langle x \rangle$

  ↳ generator

- For any $x, y \in \mathbb{Z}$, $x \equiv y \pmod{n}$ if x and y have same remainder mod n

  ↳ congruent

- Thm 4.5

  Let $G = \langle x \rangle$. If $O(x) = \infty$, then $x^i = x^j$ iff $i = j$.
  If $O(x) = n$, then $x^i = x^j$ iff $i = j \pmod{n}$

- the order of group G is the number of elements $\in G = |G|$

- Thm 4.7

  Every cyclic group is abelian.

  cor 4.6: if $G = \langle x \rangle$, $|G| = O(x)$

Section 5: Subgroups

- a subset H of a group G is called a subgroup of G if H is a group wrt G

- Thm 5.1

  Let H be a nonempty subset of G. Then, H is a subgroup of G if:

  1. $\forall a, b \in H$, $ab \in H$ — closed under multiplication
  2. $\forall a \in H$, $a^{-1} \in H$ — closed under inverse

- FACT: If G is a group and $g \in G$, then $\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$ is a subgroup of G

- Thm 5.2

  Let G be a cyclic group. Then, every subgroup of G is cyclic.

- if G is a group, then the center of G is $Z(G) = \{g \in G \mid \forall x \in G, gx = xg\}$

  ↓ elements $\in G$ that commute w/ everything

  - G is abelian iff $Z(G) = G$.
  - $Z(G)$ always has e, $\neq \emptyset$

- Thm

  Let G be a group. Then, $Z(G)$ is a sg of G.

- Thm 5.3

  Let G be a group, H be a finite, nonempty subset. Then if H is closed under $*$, H is a sg of G.

- Thm 5.4

  Let H and K be sgs of group G. Then :

  ① $H \cap K$ is always a sg.

  ② $H \cup K$ is a sg iff $H \subseteq K$ or $K \subseteq H$. → get back H, K

- Thm 5.5

  Let $G = \langle x \rangle$ be a cyclic group of order n.

  ① Then, $\forall\, m \in \mathbb{Z}^+$, G has a sg of order m iff $m \mid n$.

  ② If $m \mid n$, then G has a unique sg of order m.

  ③ 2 powers x^r, x^s generate the same sg of G iff $\gcd(n,r) = \gcd(n,s)$

- Cor 5.6

  If $G = \langle x \rangle$, $o(x) = n$, and $d_1, d_2, \dots d_r$ is a complete list of the divisors of n, then $\langle x^{d_1} \rangle, \langle x^{d_2} \rangle, \dots, \langle x^{d_r} \rangle$ is a complete list of the sgs of G.

- Thm 5.7

  Let $G = \langle x \rangle$ be an infinite cyclic group. Then, $\langle e \rangle$, $\langle x \rangle$, $\langle x^2 \rangle$, $\langle x^3 \rangle$, ... are all the distinct sgs of G.

Section 6 : Direct Powers of Groups

Let $G \times H$ denote the set of ordered pairs (g,h) with $g \in G$ and $h \in H$.
So $G \times H = \{(g,h) \mid g \in G \text{ and } h \in H\}$.

Remaining step : find binary operation $\rightarrow (g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2)$

using bin op from G

from H

Since G, H are group, $G \neq \emptyset$, $H \neq \emptyset$. So, $G \times H \neq \emptyset$. $(e_G, e_H) \in G \times H$

PROVE ONTO: 1. Let $t \in T$.
2. Solve $f(s) = t$ for s. → scratchwork
3. Let $s \in S$.
4. Show $f(s) = t$.

Thm 6.1

Let $G = G_1 \times G_2 \times \cdots \times G_n$

① If $g_i \in G_i$ for $1 \le i \le n$, and each g_i has finite order, then $o((g_1, g_2, \cdots g_n)) = \text{lcm}(o(g_1), o(g_2), \cdots o(g_n))$

② If each G_i is cyclic of finite order, then G is cyclic iff $\forall i \neq j$, $\gcd(|G_i|, |G_j|) = 1$

↓ size of group is relatively prime

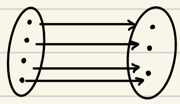
Section 7: Functions

- Def: if S and T are sets, then a function f from S to T, $f: S \to T$, is a rule to assign to each $s \in S$ a unique $f(s) = t \in T$

  ↓ domain ↓ codomain

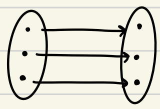
Surjective

- f is onto if $\forall t \in T$, $\exists s \in S$ s.t. $f(s) = t$
  - i.e, every $t \in T$ is reached



injective

- f is one-to-one if whenever $s_1, s_2 \in S$, s.t. $s_1 \neq s_2$, then $f(s_1) \neq f(s_2)$
  - i.e, every $t \in T$ is only reached once



- image of f: $\text{Im}(f) = \{f(s) \mid s \in S\} \subseteq T$
  - f is onto when $\text{Im}(f) = T$

- bijection: if $f: S \to T$ is onto and 1-1

- identity function of $f: S \to S$: given by $f(s) = s$
  - $g \circ f = f \circ g$
  - $\forall s \in S$, $(g \circ f)(s) = g(f(s)) = g(s)$. Similarly, $(f \circ g)(s) = f(g(s)) = f(s)$. Check this!

- inverse: Assume that f is 1-1 and onto. Then, $f^{-1}(t) = s \iff f(s) = t$

  ↳ defined on all of T, since onto

- Let X be any nonempty set and $S_X = \{f: X \to X \mid f \text{ is } 1\text{-}1, \text{ onto}\}$

  ↓ invertible

  Then, $(S_X, \circ)$ is a group.

  ↳ composition of functions

Section 8: Symmetric Groups

- Def: If X is a nonempty set and $f: X \to S$ is 1-1 and onto, then f is a permutation

- Def: The group $(S_X, \circ)$ is the symmetric group on X.

  - Thm (Cayley)

    Every group is a subgroup of a symmetric group.

- Assume X is finite $\longrightarrow$ it's okay
  - if $|X| = n$, we can assume that $X = \{1, 2, 3, \dots, n\}$. In this case, we write S_n for S_X.

- Given a $f \in S_n$, we represent f by an array $\rightarrow$ $f = \begin{pmatrix} 1 & 2 & 3 \dots & n \\ f(1) & f(2) & f(3) \dots & f(n) \end{pmatrix}$ domain / codomain

Ex. $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \in S_4$ $\qquad$ $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} \in S_4$

composition : $f \circ g = f(g(x)) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}$

Ex. $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$ $\longrightarrow$ just swaps 1 and 2 $= (1, 2)$

cycle notation: 1 2 3 4

Ex. Let $f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1, 2, 3)$ "ghost arrows", not actually written down

Ex. $f \circ g = (1, 2) \circ (3, 4)$

Ex. Compute $(1, 2, 3) \circ (7, 3, 2) \circ (1, 5)$ Assume n is the highest value.

$$\| $$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 7 & 3 & 4 & 2 & 6 & 1 \end{pmatrix} = (1, 5, 2, 7)$$

- Def : Two cycles, $(x_1, x_2, \dots, x_r)$ and $(y_1, y_2, \dots, y_s)$ are disjoint if $\{x_1, x_2, \dots, x_r\} \cap \{y_1, y_2, \dots y_s\} = \emptyset$

  ↪ Then, they commute.

- Thm 8.1

  Let $f \in S_n$. Then, $\exists$ disjoint cycles $f_1, f_2, \dots f_m$ s.t. $f = f_1 \circ f_2 \circ \dots \circ f_m$.

- Thm 8.2

  If $n \geq 2$, then any cycle in S_n can be written as the product of transpositions (2-cycles)

  - Proof : $(x_1, x_2, \ldots, x_r) = (x_1, x_r) \circ (x_1, x_{r-1}) \circ \ldots \circ (x_1, x_2)$ → textbook

    $= (x_1, x_2) \circ (x_2, x_3) \circ \ldots \circ (x_{r-2}, x_{r-1}) \circ (x_{r-1}, x_r)$ → Prof's way

  - cycles are not disjoint + not unique!

  - Ex. $f = (1, 3, 7, 9) = (1, 9) \circ (1, 7) \circ (1, 3)$ → r-1 transpositions to represent r-cycle

    $= (1, 3) \circ (3, 7) \circ (7, 9)$

- Thm 8.3

  If $n \geq 2$, then any element of S_n can be written as a product of transpositions.

  - Proof : follows from Thm 8.1 + 8.2.

- Def : A permutation is even if it can be written as a product of an even # of transpositions.

  ↳ odd, product of an odd # of transpositions

- Thm 8.4

  No permutation is BOTH odd and even.

  - Alternating Subgroup of S_n

    - For $n \geq 2$, let $A_n = \{ f \in S_n \mid f \text{ is even} \}$

    - Thm 8.5

      Let $n \geq 2$, then A_n is a subgroup of S_n, s.t. $|S_n| = n!$ and $|A_n| = \frac{n!}{2}$.

  - FACTS

    - Let $f \in S_n$ be an r-cycle. Then, $o(f) = r$.
    - If f and g are disjoint cycles, then $fg = gf$.
    - If $f = f_1 f_2 \ldots f_m$ is a product of disjoint cycles, then $o(f) = \text{lcm}(o(f_1), o(f_2), \ldots, o(f_m))$.
    - The identity is f, or $(a, b, c) \circ (c, b, a)$
    - inverse if $f = (abc) \rightarrow (cba)$

      $f = (ab)(cd) \rightarrow (dc)(ba)$

  - P_n, if $n \geq 3$: $f = (1, 2, \ldots, n)$

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n-2 & n-1 & n \\ 1 & n & n-1 & n-2 & & 4 & 3 & 2 \end{pmatrix}$$

  - $Z(D_n) = \begin{cases} \{e\} & n = \text{odd} \\ \{e, f^{\frac{n}{2}}\} & n = \text{even} \end{cases}$ → for any D_n, $f^n = e$, $g^2 = e$, $f^i g = g f^{-i}$

extend idea of equality

Section 9: Sets (Equivalence Relations + Cosets)

- **Def:** A relation R on set S is a set of ordered pairs of elements in S.
  If $s_1, s_2 \in S$, and $(s_1, s_2) \in R$, then $s_1 R s_2$ or $s_1 \sim s_2$
  related to

- **Def:** A relation R on set S is an equivalence relation if

  ① Reflexive : $\forall s \in S,\ sRs$. $a = a$

  ② Symmetric : If $s_1 R s_2$, then $s_2 R s_1$. if $a = b$, then $b = a$

  ③ Transitive : If $s_1 R s_2$ and $s_2 R s_3$, then $s_1 R s_3$. if $a = b$ and $b = c$, then $a = c$

- **Def:** Let s be a set, and R be an ER on S. Then, for any $s \in S$, $\bar{s} = \{x \in S \mid xRs\}$.
  $\bar{s}$ is the equivalence class of s under R.

- **Thm 9.1**

  Let R be an ER on S. Then every element in S is in exactly 1 equivalence class under R.
  The equi. classes under R partition S into a family of mutually disjoint nonempty sets.

- **Thm 9.2**

  For any group G and subgroup H, the relation $\equiv_H$ is an equi. relation on G.

  $$x \equiv_H y \iff xy^{-1} \in H$$

- **Def:** if H is a subgroup of G, then by right coset of H in G, we mean a subset of the form

  $$Ha, \text{ where } a \in G \text{ and } Ha = \{ha \mid h \in H\}$$
  fix an a

- **Thm 9.3**

  Let H be a subgroup of G. For $a \in G$, let $\bar{a}$ denote the equi. class of a under $\equiv_H$ relation. Then,
  $\bar{a} = Ha$ (right coset is equi. class).
  $= \{g \in G \mid g \equiv_H a\}$

- **Cor. 9.4**

  Let H be a sg of G, and $a, b \in G$. Then, $Ha = Hb \iff ab^{-1} \in H$ ← coset criterion

- **Cor**

  Notice that $H = He = Ha \overset{\text{iff}}{\iff} ea^{-1} \in H \overset{\text{iff}}{\iff} a^{-1} \in H$. $\boxed{Ha = He \iff a \in H}$

Section 10: Counting Elements in a Finite Group

- **Thm 10.1 (Legrange)**

  Let G be a finite group. Let H be a sg of G. Then, $|H| \mid |G|$

  - **Lem 10.2**

    Let Ha and Hb be right cosets of H in G. Then, there is a 1-1 correspondence btwn elements of Ha and Hb. → Ha and Hb have the same size.

- Def: If S and T are sets and $\exists f: S \to T$, f is 1-1 and onto, then $|S| = |T|$ and S and T have the same cardinality.

- **Thm 10.3**

  Let H be a sg of G. The number of and right left cosets of H in G is $[G:H]$. called the INDEX

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

- **Thm 10.4**

  Let G be a finite group, and $x \in G$. Then $o(x) \mid |G|$. Consequently, $x^{|G|} = e \quad \forall x \in G$.

- **Thm 10.5**

  Let G be a group. Suppose $|G|$ is prime. Then, G is cyclic. Moreover, any element of G, other than e, is a generator of G.

- **Thm**

  If G is a group s.t. $|G| \leq 5$, then G is abelian.

- **Thm 10.6 (Fermat's)**

  Let p be a prime + suppose $a \in \mathbb{Z}$ s.t. $p \nmid a$. Then, $a^{p-1} \equiv 1 \mod p$.

  Proof: $\bar{a} \in \mathbb{Z}_p \setminus \{0\}$. $O(\bar{a}) \mid p-1 = |\mathbb{Z}_p \setminus \{0\}| \Rightarrow (\bar{a})^{p-1} = 1$

  $\Rightarrow a^{p-1} \equiv 1 \mod p$

- Def: the eq. class $\bar{a}$ of $a \in G$ under R is the conjugancy class of a, and consists of all the conjugates of a. Thus, $\bar{a} = \{xax^{-1} \mid x \in G\}$

Thm 10.7

Let G be a group and define a relation on G by aRb iff $\exists x \in G$ s.t. $a = xbx^{-1}$.

Then, R is an ER. → must be reflexive, symmetric, transitive

- **Lem 10.8**

  Let G be a finite group. Let $a \in G$. Then, the num of distinct conjugates of a, ie $|\bar{a}|$, in G is exactly the index of the centralizer in G, ie $[G: Z(a)]$.

Thm 10.9 (class Eq)

- Let G be a finite group, and $\{a_1, a_2, \dots, a_k\}$ consist of 1 element from each conjugency class containing at least 2 elements.

  Then, $|G| = |Z(G)| + [G: Z(a_1)] + [G: Z(a_2)] + \dots + [G: Z(a_k)]$.

  ↓

  centralizer of a_1

Section 11 : Normal Subgroups

- **Def** : Let H be a sg of G. Then, H is a normal sg in G if $\forall h \in H$ and $g \in G$, $ghg^{-1} \in H$. (i.e, $gHg^{-1} \subseteq H$). Note: it does not have to be that $ghg^{-1} = h$.

- **Thm 11.1**

  Let H be a sg of G. Then, the following are equivalent:

  1. H is normal in G. → show this !
  2. $\forall g \in G$, $gHg^{-1} = H$
  3. $\forall g \in G$, $gH = Hg$.

  know this.

- **Thm 11.2**

  Let G be a group. Any sg of $Z(G)$ is normal in G.

- **Notation**
  - If H is normal in G, write $H \triangleleft G$.

- **Thm 11.3**

  Let H be a sg of G s.t. $[G:H] = 2$. Then, H is normal in G.

- **Thm 11.4**

  Let G be a group, H a sg of G, and $g \in G$. Then, gHg^{-1} is a sg of G w/ the same cardinality as H.

- **Cor. 11.5**

  If H is a sg of G and there is no other sg of G w/ the same size as H, then H is normal in G.

- **Thm 11.6** → denotes the set of right cosets of H in G

  Let $H \triangleleft G$. Then, G/H is a group under the bin. op. $Ha * Hb = H(ab)$

- **Def** : The group $\underbrace{G/H}_{\text{read "G mod H"}}$ is called the quotient group of G by H.

- **Thm 11.7**

  Let G be a finite, abelian group and suppose $p \mid |G|$ and p is prime. Then, G has a sg of order p.

Are these groups isomorphic?

1. Does it fit a thm?
2. If not, find a map φ that is hom, 1-1, onto

Section 12: Homomorphisms

- Let G and H be groups. $\varphi : G \to H$ is a homomorphism if $\forall\, a, b \in G$, $\varphi(ab) = \varphi(a)\varphi(b)$.
- A hom. is an isomorphism if it is 1-1 and onto
- Fact: $G \cong G$.

- Thm 12.1
  1. Let $\varphi : G \to H$ and $\psi : H \to K$ be homs. Then $\psi \circ \varphi : G \to K$ is a hom.
  2. If φ and ψ are isomorphisms, then so is $\psi \circ \varphi : G \to K$.
  3. If $\varphi : G \to H$ is an iso., so is $\varphi^{-1} : H \to G$.

- Cor

  $\cong$ is an equiv. relation on the set of all groups.

- Thm 12.2

  Let $n \in \mathbb{Z}^+$ and let G be a cyclic group of order n. Then, $G \cong (\mathbb{Z}_n, \oplus)$. Consequently, any 2 cyclic groups of order n are isomorphic.

- Thm 12.3

  Let G be an infinite cyclic group. Then, $G \cong (\mathbb{Z}, +)$. Consequently, any 2 infinite cyclic groups are iso

- Thm 12.4

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

  1. $\varphi(e_G) = e_H$
  2. $\forall x \in G$ and $n \in \mathbb{Z}$, $\varphi(x^n) = [\varphi(x)]^n$
  3. If $o(x) = n$, $o(\varphi(x)) \mid o(x)$.

- Thm 12.5

  Let $\varphi : G \to H$ be an iso. Then,

  4. $\forall x \in G$, $o(x) = o(\varphi(x))$
  5. $|G| = |H|$
  6. G is abelian iff H is abelian

- Thm 12.6

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

  1. If K is a sg of G, then $\varphi(K) = \{\varphi(k) \mid k \in K\}$ is a sg of H.
  2. If J is a sg of H, then $\varphi^{-1}(J) = \{g \in G \mid \varphi(g) \in J\}$ is a sg of G.
  3. If $J \trianglelefteq H \Rightarrow \varphi^{-1}(J) \trianglelefteq G$.
  4. If φ is onto and $K \trianglelefteq G$, $\varphi(K) \trianglelefteq H$.

- Thm 12.7 (Cayley's)

  If G is a group, then G is isomorphic to a sg of $S_G = \{f : G \to G \mid f \text{ is 1-1 and onto}\}$.

Section 13 : Homomorphisms + Normal Subgroups

- Suppose $H \lhd G$. There is always a hom. $\rho : G \to G/H$, given by $\rho(g) = Hg$
  ↳ "rho"

  - like a reduction map → $[\rho(g_1 g_2) = H(g_1 g_2) = Hg_1 Hg_2 = \rho(g_1)\rho(g_2)]$
  - ρ is surjective (onto), is a function that gives you cosets

- Def : if $\varphi : G \to K$ is a hom., then the kernel of φ is $Ker(\varphi) = \{g \in G \mid \varphi(g) = e_K\}$.

- Thm 13.1

  For any hom $\varphi : G \to K$, $Ker(\varphi) \lhd G$.

- Thm 13.2 (Fundamental Thm on Group Homs)

  Let $\varphi : G \to K$ be a surjective group hom. Then, $K \cong G/Ker(\varphi)$.

- Thm 13.3

  Let $\varphi : G \to K$ be a surj hom. There is a 1-1 correspondence btwn sgs of K and sgs of G that contain $Ker(\varphi)$.
  I.e, there is a bijective map $\Psi : \{\text{sgs of } K\} \to \{H \mid H \text{ is a sg of } G, Ker(\varphi) \leq H\}$.
  ↳ $\Psi(J) = \varphi^{-1}(J)$

- Thm 13.4 (2^{nd} Hom Thm)

  Let H and K be sgs of G. Assume $K \lhd G$. Then, $H/H \cap K \cong HK/K$, where $HK = \{hk \mid h \in H, k \in K\}$.

- Thm 13.5 (3^{rd} Hom Thm)

  Suppose $H \lhd K \lhd G$ and $H \lhd G$. Then, $K/H \lhd G/H$ and $(G/H)/(K/H) \cong G/K$.

Section 14 : Direct Products + Finite Abelian Groups → no HW from this section

- Thm 14.1

  Suppose A, B are sgs of G s.t. $A \lhd G$, $B \lhd G$. Also, $G = AB = \{ab \mid a \in A, b \in B\}$. Also, $A \cap B = \{e\}$.
  Then, $G \cong A \times B$.

- Thm 14.2 (Fund. Thm on Finite Abelian Groups)

  Let G be a nontrivial finite abelian group. Then, $G \cong$ direct product of finitely many nontrivial cyclic groups of prime power order. The prime powers that occur are uniquely determined by G.

- Cor 14.3

  Let A, B be finite abelian groups. Then $A \cong B$ iff invariants of A = invariants of B.

- Cor 14.5

  Let G be an abelian group of order n and $m \in \mathbb{Z}^+$ s.t. $m \mid n$. Then, G has a sg of order m.

Section 15 : Sylow Thms → no HW

- Thm 15.1

  Let G be a finite group. p a prime, $k \in \mathbb{Z}^+$.

  1. If $p^k \mid |G|$, then G has a sg of order p^k.

Section 16 : Rings

- **Def** : Suppose R is a set with 2 bin ops, $+$ and $\cdot$

  Suppose further that 1) $(R, +)$ is an abelian group

  2) $\cdot$ is associative

  3) $\forall r_1, r_2, r_3 \in R$, $r_1(r_2 + r_3) = r_1 r_2 + r_1 r_3$ and $(r_1 + r_2) r_3 = r_1 r_3 + r_2 r_3$

  Then, $(R, +, \cdot)$ is a ring.

- commutative ring : if $\cdot$ is commutative
- additive identity is denoted 0_R.
- If $\exists$ a mult. identity, we denote it 1_R, which is called the unity of R. R is a ring w/ unity.

- **Def** : Let R be a ring and $a \in R$. We say that a is a zero-divisor if $\exists$ $b \in R$ s.t. $b \neq 0_R$ and either $ab = 0_R$ or $ba = 0_R$. The element a is said to be nilpotent if $\exists$ $n \in \mathbb{Z}^+$ s.t. $a^n = 0_R$.

  - 0 can be a zero-divisor
  - Every nilpotent element is a zero-divisor

- **Def** : Suppose R is a ring w/ unity. We say $a \in R$ is a unit if $\exists$ $b \in R$ s.t. $ab = ba = 1_R$.

- **Thm 16.1**

  Let R be a ring, $a, b \in R$. Then,
  1) $a \cdot 0_R = 0_R \cdot a = 0_R$
  2) $a(-b) = (-a)(b) = -(ab)$
  3) $(-a)(-b) = ab$
  4) $\forall m \in \mathbb{Z}$, $m(ab) = (ma)b = a(mb)$
  5) $\forall n, m \in \mathbb{Z}$, $mn(ab) = (ma)(nb)$

- Cor 16.2 : Let R be a nontrivial ring w/ unity. Then, $0_R \neq 1_R$

- Cor 16.3 : Let R be a nontrivial ring w/ unity and $u \in R$ be a unit. Then, u is NOT a zero-divisor.

- Cor 16.4 : If $b, c \in R$, $b - c = b + (-c)$. $\forall a \in R$, $a(b-c) = ab - ac$ and $(b-c)a = ba - ca$. ☆ distributive laws

- **Def** : An integral domain is a commutative ring w/ unity in which $0_R \neq 1_R$ and there are no nontrivial 0-divisors.

- **Thm 16.5**

  Let R be a ring, and $a, b, c \in R$. Assume $a \neq$ zero-divisor. Then, if $ab = ac$, $b = c$.

- **Def** : R is called a division ring (if you throw away 0 and get a group under mult) if R has a unity $1_R \neq 0$ and every nonzero element of R is a unit.

  A commutative division ring is called a field.

- **Thm 16.7**

  Every finite integral domain is a field. (See Thm 5.3)

Section 17: Subrings, Ideals (Normal subrings), Quotient Rings

- **Def**: Let $(R, +, \cdot)$ be a ring. A subset S of R is a subring of R if $(S, +, \cdot)$ is a ring.

- **Thm 17.1**

  Let $(R, +, \cdot)$ be a ring. Let S be a subset of R. Then, S is a subring of R iff

  1) $(S, +)$ is a sg of $(R, +)$. → nonempty is built in
  2) S is closed under mult ($\forall s_1, s_2 \in S$, $s_1 s_2 \in S$).

- **Cor 17.2**

  Let $(R, +, \cdot)$ be a ring and let S be a nonempty subset of R. Then, S is a subring of R iff
  1) $\forall s_1, s_2 \in S$, $s_1 - s_2 \in S$.
  2) $\forall s_1, s_2 \in S$, $s_1 s_2 \in S$.

- **Def**: a subring S of R is an ideal of R (think of it as a normal subring) if $\forall s \in S$, $r \in R$, $rs, sr \in S$.

- **Thm 17.3**

  Let $(R, +, \cdot)$ be a ring and S be an ideal of R. Then, the set R/S of right additive cosets of S in R is a ring under the op $(S+a)(S+b) = S + (a+b)$ and $(S+a)(S+b) = S + ab$.

- **Thm 17.4**

  Let R be a ring and S be a nonempty subset of R. Then, S is an ideal of R, denoted I, iff

  1) $\forall s_1, s_2 \in S$, $s_1 - s_2 \in S$.
  2) $\forall r \in R$, $s \in S$, $rs, sr \in S$. → sticky property

- **Cor**: If F is a field, the only ideals of F are $\{0\}$, F.

- **Def**: Let R be a ring. Then, R is an improper ideal of R. The trivial ideal is $\{0_R\}$.

- **Def**: Let R be a ring, I an ideal of R. Then, I is prime if whenever $a, b \in R$ and $ab \in I$, then at least a or $b \in I$.
  (Prime means $ab \in p\mathbb{Z} \iff a \in p\mathbb{Z}$ or $b \in p\mathbb{Z}$.)

- **Thm 17.5**

  Let R be a ring and I an ideal. Then, R/I has no nontrivial 0-divisors iff I is prime.

- **Cor 17.6**

  Let R be any comm. ring w/ unity. Then, R/I is an integral domain iff I is a prime ideal.

- **Def**: An ideal I in a ring R is called maximal if I is a proper ideal and $\nexists$! other proper ideal J s.t. $I \subsetneq J$.

- **Thm 17.7**

  Let R be a comm. ring w/ unity. If I is an ideal in R, then R/I is a field iff I is maximal.

- **Cor 17.8**

  Let R be a comm. ring w/ unity. Then, every maximal ideal of R is a prime ideal.

Section 18: Ring Homomorphisms

- **Def**: Let R, S be rings, and $\varphi: R \to S$ be a function. Then, φ is a (ring) hom. if

1) $\forall\, a, b \in R$, $\varphi(a+b) = \varphi(a) + \varphi(b)$
2) $\forall\, a, b \in R$, $\varphi(ab) = \varphi(a)\varphi(b)$

From 1), if $\varphi: R \to S$ is a ring hom, then $\varphi: (R,+) \to (S,+)$ is a group hom.
Then, $\varphi(0_R) = 0_S$ and $\forall n \in \mathbb{Z}$ and $a \in R$, $\varphi(na) = n\varphi(a)$.

- **Thm 18.1**

Let $\varphi: R \to S$ be a ring hom. Then,
1) $\varphi(0_R) = 0_S$
2) $\varphi(na) = n\varphi(a)$ $\forall n \in \mathbb{Z}$, $a \in R$
3) $\varphi(a^n) = \varphi(a)^n$ $\forall\, n \in \mathbb{Z}^+$, $a \in R$
4) If R and S have unity and $\varphi(1_R) = 1_S$, then $\forall$ unit $u \in R$, $\varphi(u)$ is a unit in S and $\varphi(u^{-1}) = \varphi(u)^{-1}$.

- **Thm 18.2**

Let R, S be rings w/ unity and $\varphi: R \to S$ be a ring hom. Then,
1) if φ is onto, then $\varphi(1_R) = 1_S$.
2) if S is a division ring + $\varphi(1_R) \neq 0_S$, then $\varphi(1_R) = 1_S$.
3) if S is an integral domain + $\varphi(1_R) \neq 0_S$, then $\varphi(1_R) = 1_S$.

- **Thm 18.3**

Let R, S, and T be rings, $\varphi: R \to S$ and $\psi: S \to T$ be ring homs. Then,
1) $\psi \circ \varphi: R \to T$ is a hom
2) if φ, ψ are isos, then so is $\psi \circ \varphi$.
3) if φ is an iso, then so is φ^{-1}

Thm 18.4

Let $\varphi: R \to T$ be a hom. Then,
1) if S is a subring of R, then $\varphi(S) = \{\varphi(s) \mid s \in S\}$ is a subring of T.
2) if U is a subring of T, then $\varphi^{-1}(U) = \{r \in R \mid \varphi(r) \in U\}$ is a subring of R.
3) if U is an ideal of T, then $\varphi^{-1}(U)$ is an ideal of R.
4) if φ is onto and S is an ideal of R, then $\varphi(S)$ is an ideal of T.

- **Thm 18.5**

If $\varphi: R \to T$ is an onto ring hom, then $R/\ker(\varphi) \cong T$. Moreover, if $P: R \to R/\ker(\varphi)$, there is an isomorphism $\overline{\varphi}: R/\ker(\varphi) \to T$ s.t. $\overline{\varphi} \circ P = \varphi$.

Section 19 : Polynomials

- Notation : 1) Variables are $X, Y, Z, \ldots$
  2) If R is a ring, then by a poly. w/ coeffs from R, we mean an infinite formal symbol $a_0 + a_1X + a_2X^2 + \ldots$, where each $a_i \in R$ and $\exists$ some $n \in \mathbb{Z}^+ \cup \{0\}$ s.t. $\forall\, i > n$, $a_i = 0_R$.
  3) The a_i's are the coeffs of the poly.
  4) If $a_n \neq 0$ and $a_i = 0$ $\forall\, i > n$, then we write our poly. as $a_0 + a_1X + \ldots + a_nX^n$.
  5) 2 poly, $f(X)$ and $g(X)$, are equal if $\forall\, i$, $a_i = b_i$ (a_i, b_i are coeffs)

  6) Poly's w/ coeffs from R are functions from $R \to R$. For any $r \in R$, define a function by $f(r) = a_0 + a_1r + a_2r^2 + \ldots + a_nr^n \in R$.

  7) 2 diff poly's can give the same function.

Ex. Let $R = \mathbb{Z}_3$ (field). Let $f(X) = 0$, $g(X) = X^3 - X$. Recall in $\mathbb{Z}_p$, $x^p = x$.
$\forall\, r \in R$, $g(r) = r^3 + 2r = 0$.

Ex. $R[X] = \{$ poly's $\in X$ w/ coeffs $\in R\}$, where $f(X) = a_0 + a_1X + a_2X^2 + \ldots$,
$g(X) = b_0 + b_1X + b_2X^2 + \ldots$

$R[X]$ is a ring under coeff addition, mult, where $c_n = a_0b_n + a_1b_{n-1} + a_2b_{n-2} + \ldots + a_{n-1}b_1 + a_nb_0 = \sum_{i=0}^{n} a_ib_{n-i}$

What can we say abt $R[X]$, given info abt R?
- If R has a unity, then so does $R[X]$: $1_{R[X]} = 1_R + 0X + 0X^2 + \ldots$
- If R is a domain, so is $R[X]$.
  ↳ comm. ring w/ unity, no nontrivial 0-divisors

Proof: Let $f(X), g(X) \in R[X]$. Suppose $a_n, b_m \neq 0$. Then, $(fg)(X) = c_0 + c_1X + \ldots + c_{m+n}X^{m+n}$, $c_{m+n} \neq 0$. So, $(fg)(X) \neq 0_{R[X]}$.

- Def : Let $f(X) = a_0 + a_1X + a_2X^2 + \ldots + a_nX^n$, w/ $a_n \neq 0$. The int n is the degree of f and denoted $\deg(f) = n = \deg(f(X))$.

  Note: $\deg(0_{R[X]}) =$ DNE.

- Thm 19.1

  If R is a domain and $f(X), g(X) \in R[X]$ and $f(X) \neq 0$, $g(X) \neq 0$, then $\deg(f(X)g(X)) = \deg(f(X)) + \deg(g(X))$.

- Thm 19.2

  Let F be a field and $f(X), g(X) \in F[X]$. If $g(X) \neq 0$, then $\exists$ $q(X), r(X) \in F[X]$ s.t. $f(X) = q(X)g(X) + r(X)$ and either $r(X) = 0$ or $\deg(r(X)) < \deg(g(X))$.

  Note: the units in $F[X]$ are the deg 0 poly.

- **Def**: Let R be a ring and $f(x) \in R[x]$. An element $r \in R$ is called a root / zero of $f(x)$ if $f(r) = 0$.

- **Thm 19.3**

  Let F be a field, $a \in F$, $f(x) \in F[x]$. Then $f(a) = 0$ iff $x - a \mid f(x)$.

- **Cor 19.4**

  Let F be a field, $f(x) \in F[x]$ w/ $\deg(f) = n$. Then, $f(x)$ has at most n roots.

- **Cor 19.5**

  Let F be an infinite field, S an infinite subset of F. If $f(x) \in F[x]$ s.t. $\forall s \in S$, $f(s) = 0$, then $f(x) = 0$.

- **Cor 19.6**

  Let F be an infinite field and $S \subseteq F$ s.t. $|S| = \infty$. Suppose $f(x), g(x) \in F[x]$ s.t. $\forall s \in S$, $f(s) = g(s)$. Then, $f(x) = g(x)$ [as polynomials].

- **Def**: Let F be a field, $f(x) \in F[x]$ s.t. $f(x)$ is a nonconstant poly. The poly. f is irreducible (over F) if f cannot be written as the product of 2 nonconstant poly. I.e, f is irr. if whenever $f(x) = g(x)h(x)$, either $\deg(g) = 0$ or $\deg(h) = 0$.

  Ex. In $\mathbb{R}[x]$, $x^2 + 1$ is irr. (no roots $\rightarrow$ cannot factor $\rightarrow$ irr). It is a unit!

  Ex in $\mathbb{C}[x]$, $x^2 + 1$ is NOT irr.

  Ex. In $\mathbb{Z}_5[x]$, $x^2 + 1$ is NOT irr, bc $f(2) = 2^2 + 1 = \bar{5} = 0$. we have our root.
  $\hookrightarrow$ $x^2 + 1 = (x-2)(x-3)$

- **Thm 19.7**

  Let F be a field and $f(x) \in F[x]$ s.t. $f(x)$ is nonconstant. Then, $\exists$ irr. poly's $f_1(x), f_2(x), \ldots, f_k(x) \in F[x]$ s.t. $f(x) = f_1(x) f_2(x) \cdots f_k(x)$.

- **Thm 19.8** ☆

  Let F be a field and $f(x) \in F[x]$ s.t. $\deg(f) = 2$ or 3. Then, f is reducible iff $f(x)$ has a root in F.

- **Thm 19.11**

  Let $f(x) = a_0 + a_1 x + \ldots + a_n x^n \in \mathbb{Z}[x]$ Suppose p is a prime in $\mathbb{Z}$ s.t. $p \mid a_0$, $p \mid a_1$, $\ldots$, $p \mid a_{n-1}$, $p \nmid a_n$ and $p^2 \nmid a_0$. Then, $f(x)$ is irr in $\mathbb{Q}[x]$. It is Eisenstein at p.

- **Ex**: $f(x) = 2x^5 + 9x^4 + 3x^3 + 15x + 12 \in \mathbb{Z}[x]$. $f(x)$ is Eisenstein at $p = 3$. So, $f(x)$ is irr over $\mathbb{Q}$.

- **Ex**: $x^2 - 2$ is Eisenstein at $p = 2$. So $x^2 - 2$ is irr in $\mathbb{Q}[x]$.

- **Ex**: $f(x) = x^4 + 1$.

  Suppose $f(x)$ is irr. Then $f(x) = \overset{\in \mathbb{Q}[x] \ni}{g_1(x) g_2(x)}$ w/ $\deg(g_1), \deg(g_2) > 0$. Then, $f(x) + 1 = g_1(x+1) g_2(x+1)$.
  $f(x+1) = (x+1)^4 + 1$
  $= x^4 + 4x^3 + 6x^2 + 4x + 2$ is Eisenstein at 2 and irr in $\mathbb{Q}[x]$. So, $f(x)$ must also be irr.

- Thm 19.12 ☆ Prof's favorite, might appear on exam

Let p be a prime. For $m \in \mathbb{Z}$, let $\overline{m}$ be the remainder of dividing m by p (i.e. m mod p).
Let $f(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n \in \mathbb{Z}[x]$ be a nonconstant poly. Let $\overline{f}(x) = \overline{a}_0 + \overline{a}_1 x + \dots + \overline{a}_n x^n$ $\in \mathbb{Z}_p[x]$.

Then, if $\overline{f}(x)$ is irreducible in $\mathbb{Z}_p[x]$ and $\deg(f) = \deg(\overline{f})$, then $f(x)$ is irr. in $\mathbb{Q}[x]$.

↳ stronger than being irr in $\mathbb{Q}[x]$

I.e, $f(x) = g_1(x) g_2(x) \iff \overline{f}(x) = \overline{g}_1(x)\overline{g}_2(x)$.

Section 20: From Poly's to Fields

- Thm 20.1

  If F is a field, every ideal of $F[x]$ is principal.

  → R a comm. ring w/ 1. Let $a \in R$. Then, $aR = \{ar \mid r \in R\}$.

- Thm 20.2

  Let F be a field, $f(x) \in F[x]$. Then, $(f(x))$ is maximal iff $f(x)$ is irreducible.