Section 0:

- Def: equal cardinality $\Leftrightarrow \exists$ a bijection
- Def: A is a partition $\Leftrightarrow A = A_1 \cup \cdots \cup A_n$, $\forall i,j, A_i \cap A_j = \emptyset$
- Def: Equivalance Relation $\Leftrightarrow$ $\begin{cases} a \sim a \\ a \sim b \Rightarrow b \sim a \\ a \sim b, b \sim c \Rightarrow a \sim c \end{cases}$
- Euler: $e^{i\theta} = \cos\theta + i\sin\theta$
- polar form: $z = r \cdot e^{i\theta}$
- n-th Roots of unity: $U_n = \{ e^{\frac{2\pi i k}{n}} \mid k = 0, \cdots, n-1 \}$.
- Def (Binary opt): $S \times S \to S$, $a * b$

  There are $n^{(n^2)}$ opts.

$\uparrow$ $\times$ $\uparrow$

n^2 $\quad$ n

Sec 4. group:

- Def (GP): G is a gp $\overset{\text{def}}{\Leftarrow}$ $\begin{cases} \text{associative.} \\ \exists e \\ \forall a \in G, \exists a^{-1}. \end{cases}$
- Thm 0.1: left, right cancellation: $a*b = a*c \Rightarrow b = c$

  $b*a = c*a \Rightarrow b = c$

Sec 5. Subgp:

- Def: $H \subseteq G$ is a subgp of $(G, *)$ $\Leftrightarrow$ 1. H is closed under $*$
  2. H is a gp

  $(H \neq \emptyset)$
- Thm (5.14): H is a subgp of G $\Leftrightarrow$ 1, H is closed under $*$
  2. e of G is in H
  3. $\forall a \in H, \exists a^{-1}$
- Ex: H, K are subgp of G. prove $H \cap K$ is subgp of G.

· Def: cyclic gp $\langle a\rangle \overset{\text{def}}{\iff} \langle a\rangle = \{a^n \mid n\in\mathbb{Z}\}$

· Thm: $\langle a\rangle$ is the smallest subgp of G. every subgp contain a contain $\langle a\rangle$

· Def (order of $\langle a\rangle$) : smallest positive integer n s.t $a^n = e$

· Thm 6.1 : cyclic gp is abelian

· Thm : $\forall n\in\mathbb{N}$, $\exists q, 0\le r<m$, $m\in\mathbb{N}$, s.t. $n = m\cdot q + r$.

· Thm 6.6 : subgp of cyclic gp is cyclic.

· proof : $H\le G$.

Case 1 : $H = \langle e\rangle$. obviously H is a subgp of G

Case 2 : $H\neq\langle e\rangle$, claim $H = \langle a^m\rangle$. s.t. m is ... $a^m = e$, $a^m\in H$.

Trivial : $\langle a^m\rangle \in H$

for element $a^n\in G$: $\exists m, r\in\mathbb{N}$. $n = m\cdot r + q$

$\therefore a^r = (a^n)(a^{-mq}) \in H$

$\because r = 0$ $\therefore n = mq$ for some q.

$\therefore a^n = (a^m)^q \in \langle a^m\rangle$ $\therefore H\le\langle a^m\rangle$

proved!

· Corollay 6.7 : subgp of $\mathbb{Z}$ is $n\mathbb{Z}$

To Subgp

- $H\le G$, $|G| = n$, $|H| = m \Rightarrow n = m\cdot d$, $d\in\mathbb{Z}$.
- $a, b\in G$. ab, ba has equal order.

8. gp of permutation.

- Def 8.3 : permutation of set $A \overset{\text{def}}{\iff} \phi : A\to A$, ϕ is bijection.

- Thm 8.5: $S_A := \{\text{all permutation of } A\}$. S_A is a gp with opt composition.
- Def 8.6: $A = \{1 \cdots n\}$. S_A is called symmetric gp on n. Denote as S_n.
  - $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \cdots & \cdots & \cdots & \cdots \end{pmatrix}$
  - total permutations: $|S_n| = n!$
  - $n \geq 3$. S_n is not abelian

9. Orbits, Cycles, Alternating Gp.

- Orbit: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 5 & 6 & 4 \end{pmatrix}$ 4 orbits: $\{1\}, \{2\}, \{3\}, \{4, 5, 6\}$.
- Cycle: $\sigma \in S_n$ s.t.
  - Case 1: e
  - Case 2: σ has a unique orbit with more than 1 elements.

  notation: $(3, 6, 5)$
- Def: 2 cycles are disjoint.
- 2 disjoint cycles are commutative.
- Thm 9.8: Every permutation is a product of disjoint cycles.
- Def: order of a cycle with len k is k.
- $\sigma = \tau_1 \cdots \tau_k$, are disjoint cycles. then σ has order: $\gcd(l_1, \cdots, l_k)$
  - $\tau_1 \cdots \tau_k$ has order $l_1 \cdots l_k$.
- Def 9.11: transposition $\Leftrightarrow$ cycle of len 2

S_n has $\binom{n}{2} = \frac{n(n-1)}{2}$ transpositions

- Formula: $(a_1, \cdots, a_n) = (a_1, a_n)(a_1, a_{n-1}) \cdots (a_1, a_2)$
- Corollary 9.12: permutation S_m $(m \geq 2)$ is a product of transpositions

Eg: $(1,3,6,4,2)(5,8,7)$

$\sigma = (12)(14)(16)(13)(57)(58)$

$\sigma^{-1} = (58)(57) \cdots (14)(12)$

- Def 9.18: even permutation $\Leftrightarrow$ σ is product of even number permutation

  odd ... $\Leftrightarrow$ ... odd ...
- Thm 9.15: S_n can be either expressed as a product of even number transposition or ... odd ...

  proof: let $\sigma = \tau_1 \cdots \tau_k$, $\sigma = u_1 \cdots u_m$ we want to prove $k.m.$ are both even or odd.

  we define $\{\tau_i\}_{i=1}^{k}$, $\{u\}_{i=1}^{m}$ are row operation for matrix A here. , which can swap 2 rows in A

  we know $\sigma(A) = \tau_1 \cdots \tau_k(A)$, then $\det(A) = (-1)^k \det(A)$

  $\sigma(A) = u_1 \cdots u_m(A)$, then $\det(A) = (-1)^m \det(A)$

  $\therefore (-1)^k \det A = (-1)^m \det A \Rightarrow (-1)^k = (-1)^m$

  $\therefore$ $k.m$ are both even or odd.

- Symmetric gp of a finite structure with n elements is always subgp of S_n.
- Denote $A_n := \{$all even permutation of $S_n\}$.
- Thm 9.20: A_n is a subgp of S_n. order of A_n is $\frac{1}{2}n!$

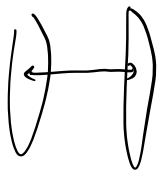
  Show ①: let $\phi: A_n \to S_n \setminus A_n$, $\phi(\sigma) = (1,2)\sigma$

  ϕ is bijection. $\therefore |A_n| = \frac{1}{2}|S_n| = \frac{1}{2}n!$
- Def 9.21: A_n is called Alternating gp

· Sec 10. Coset. Thm of Lagrange.

· Def 10.2: (coset) $H \leq G$, H is a subgp of G

1. Left coset: $a \in G$, $aH = \{ah \mid h \in H\}$
2. right coset: $a \in G$, $Ha = \{ha \mid h \in H\}$.



· Every coset aH has the same number of elements as H. ①

Trivial proof: $\{ah_1, \cdots, ah_k\}$ are distinct by cancellation law.

· aH, bH are cosets, we claim: $aH = bH$ or $aH \cap bH = \phi$. ②

pwf: If $aH \cap bH \neq \phi$, we need to prove $aH = bH$.

$\exists c \in aH \cap bH$, $\therefore \exists h_1, h_2 \in H$, s.t. $c = ah_1 \in aH$, $c = bh_2 \in bH$.

$\therefore ah_1 = bh_2 \Leftrightarrow a = bh_2 h_1^{-1}$

$\therefore ah = bh_2 h_1^{-1} h \in bH$. Similarly, every $bh \in aH$.

$\therefore aH \subseteq bH$, $bH \subseteq aH$ $\therefore ah = bh$.

this claim $\Rightarrow G = a_1H \cup a_2H \cup \cdots \cup a_mH$.

· Lagrange Thm: $H \subseteq G$ is a subgp of G. then $|H|$ divides $|G|$.

pwf: from claim ① ②. we know: $G = a_1H \cup a_2H \cdots \cup a_mH$. and $|a_1H| = \cdots = |a_mH| = |H|$

$\therefore |G| = m|H|$ $\therefore$ proved!

· Corollary 10.11: Every gp of prime order is cyclic.

pwf: let $|G| = p$. p is a prime. let $a \in G$, $a \neq e$, then $\langle a \rangle \in G$ is a subgp of G.

$\langle a \rangle$ contain e, a $\therefore |\langle a \rangle| \geq 2$.

By Lagrange Thm: $|\langle a \rangle|$ is a divisor of $|G|$ $\therefore |\langle a \rangle|$ is 0 or p.

$\therefore |\langle a \rangle| = p$ $\therefore \langle a \rangle = G$

· Thm 10.12: $a \in G$. $|\langle a \rangle|$ divides $|G|$

Trivial: $\langle a \rangle \subseteq G$ is a subgp of G. $\therefore |\langle a \rangle|$ divides $|G|$

· Def 10.13: $H \subseteq G$ is subgp of G. index $(G:H) \Leftrightarrow$ number of left cosets of H in G.

(that is $(G:H) = \frac{|G|}{|H|}$)

· Def 11.2 : (Direct product groups)

$G_1 \times \cdots \times G_n$ is a gp under $* : (a_1, \cdots, a_n)(b_1, \cdots, b_n) = (a_1 b_1, \cdots, a_n b_n)$

· If $G = \langle a \rangle$, $G' = \langle b \rangle$. $|\langle a \rangle| = m$, $|\langle b \rangle| = n$. if m, n relatively prime $\Rightarrow G \times G'$ is a cyclic gp.

proof : $(a, b) \in G \times G'$ $|\langle (a,b) \rangle| = m \cdot n$, and $|G \times G'| = m \cdot n$ $\therefore |\langle a, b \rangle| = |G \times G'|$

$\therefore \langle a, b \rangle = G \times G'$

· Def : S is a subset of G . S generates G if $\forall g \in G$. $g = a_1^{k_1} a_2^{k_2} \cdots a_m^{k_m}$ $(k_1 \cdots k_m \in \mathbb{Z},$ $a_1 \cdots a_m \in S)$

· Def: Finite generate gp $G \overset{\text{def}}{\Leftrightarrow} \exists$ finite S generates G.

· Thm 11.12 : Every finite generated abelian G is isomorphic to $\mathbb{Z}_{p_1^{n_1}} \times \mathbb{Z}_{p_2^{n_2}} \times \cdots \times \mathbb{Z}_{p_n^{n_m}} \times \mathbb{Z} \times \mathbb{Z} \cdots \mathbb{Z}$

G is finite $\Leftrightarrow$ there is no $\mathbb{Z} \times \mathbb{Z} \cdots \times \mathbb{Z}$.

Sec 13. Homomurphism.

· Def 13.1 : $\phi : G \to G'$ is a homomorphism $\overset{\text{def}}{\Leftrightarrow}$ $\phi(ab) = \phi(a)\phi(b)$ (opt in G / opt in G')

· Def : $\phi : G \to G'$ is a isomorphism $\overset{\text{def}}{\Leftrightarrow}$ $\phi(ab) = \phi(a)\phi(b)$, ϕ is bijection.

· G, G' have equal prime order $\Rightarrow$ isomorphism.

· Thm 13.12 : $\phi : G \to G'$ is hom. then
1. $e \in G$ is identity $\Rightarrow \phi(e) = e'$ is identity in G'
2. $a \in G \Rightarrow \phi(a^{-1}) = \phi(a)^{-1}$
3. $H \subseteq G$ is subgp $\Rightarrow \phi(H)$ is subgp of G'
4. $K' \subseteq G'$ is subgp $\Rightarrow \phi^{-1}(K')$ is subgp of G

proof: 1. $\phi(a) = \phi(a \cdot e) = \phi(a) \cdot \phi(e) \Rightarrow \phi(a)^{-1} \cdot \phi(a) = \phi(e)$ $\therefore e' = \phi(e)$ is identity of

2. $e' = \phi(e) = \phi(aa^{-1}) = \phi(a)\phi(a^{-1})$ $\therefore \phi(a^{-1}) = \phi(a)^{-1}$

3. let H be a subgp of G. for any $\phi(a) \cdot \phi(b) \in \phi[H]$:

$\phi(a) \cdot \phi(b) = \phi(ab) \in \phi[H]$ $\therefore \phi[H]$ is closed.

the fact $e' = \phi(e)$, $\phi(a^{-1}) = \phi(a)^{-1}$ show $\phi[H]$ is a subgp of G'.

4. let K' be a subgp of G'. Suppose $a, b \in \phi^{-1}(K')$. Then $\phi(a) \cdot \phi(b) \in K'$ since K' is a subgp

$\phi(ab) = \phi(a) \cdot \phi(b) \in K'$ $\therefore ab \in \phi^{-1}(K')$ $\therefore \phi^{-1}(K')$ is closed.

$e = \phi^{-1}(e') \in \phi^{-1}[K']$. if $a \in \phi^{-1}[K']$, then $\phi(a) \in K'$. $\phi(a^{-1}) = \phi(a)^{-1} \Rightarrow a^{-1} \in \phi^{-1}(K')$

$\therefore \phi^{-1}[K']$ is a subgp of G.

Def 13.13: (kernal) $\phi: G \to G'$ is hom. The subgp $\phi^{-1}(e') = \{a \in G \mid \phi(a) = e'\}$ is kernel of ϕ.

Denoted as $\ker(\phi)$

Thm 13.15: $\phi: G \to G'$ is hom. $H = \ker(\phi)$. $b \in G'$. $\phi^{-1}(b) = \{a \in G \mid \phi(a) = b\}$

then it has 2 cases: 1. $\phi^{-1}(b) = \emptyset$

2. $\phi^{-1}(b) \neq \emptyset$, let $a \in \phi^{-1}(b)$. then $\phi^{-1}(b) = aH$

proof: Suppose $\phi^{-1}(b) \neq \emptyset$. we claim $\phi^{-1}(b) = aH$. (that's to prove $\phi^{-1}(b) \subseteq aH$, $aH \subseteq \phi^{-1}(b)$)

1. $ah \in aH$. $\phi(ah) = \phi(a)\phi(h) = b$ $\therefore ah \in \phi^{-1}(b)$ $\Rightarrow aH \in \phi^{-1}(b)$

2. let $L \in \phi^{-1}(b)$. $\phi(a^{-1}L) = \phi(a^{-1}) \cdot \phi(L) = \phi(a)^{-1} \cdot \phi(L) = b^{-1}b = e'$

$\therefore a^{-1}L \in H$. $\Rightarrow L = a(a^{-1}L) \in aH$ $\therefore \phi^{-1}(b) \subseteq aH$.

Corollary 13.16: $\phi: G \to G'$ is hom. ϕ is 1-to-1 $\Leftrightarrow \ker(\phi) = \{e\}$

Ex: $\phi: G \to G'$ is hom. G, G' are finite and ϕ is surjective. prove: $|G'|$ divides $|G|$.

Def 13.19: H is normal subgp $\Leftrightarrow \forall g \in G, gH = Hg$

Lemma: H is normal $\Leftrightarrow \forall g \in G, h \in H, ghg^{-1} \in H$

proof: 1. ($\Rightarrow$): $gh \in gH = Hg$ $\therefore \exists h' \in H, gh = h'g$, $\therefore ghg^{-1} = h'gg^{-1} = h' \in H$.

2. ($\Leftarrow$): claim $\forall a \in G, aH = Ha$. (prove $aH \subseteq Ha$ and $aH \supseteq Ha$)

① ($aH \subseteq Ha$): $\exists h', h \in H, aha^{-1} = h' \Rightarrow ah = h'a \in Ha$ $\therefore aH \subseteq Ha$

② ($Ha \subseteq aH$): $\exists h', h \in H, aha^{-1} = h' \Rightarrow h'a = ah \in aH$ $\therefore Ha \subseteq aH$

$\therefore aH = Ha$

$\therefore$ proved!

Ex: $SL(n, \mathbb{R}) = \{A \in GL(n, \mathbb{R}) \mid \det(A) = 1\}$. prove: SL is normal gp of GL

prove: $\phi: GL(n, \mathbb{R}) \to \mathbb{R}^*$, $\phi(A) = \det(A)$ $\therefore SL = \ker(\phi)$

we want to show: $g \in GL$. $h \in SL$. $ghg^{-1} \in SL$

$\therefore \det(ghg^{-1}) = \det(g)\det(h)\det(g^{-1}) = 1$

$\therefore ghg^{-1} \in SL$

Corollary 13.20: $\phi: G' \to G$ is hom. $\ker(\phi)$ is normal gp of G

Proof: $g \in G$. $h \in \ker(\phi)$

$\phi(ghg^{-1}) = \phi(g)\phi(h)\phi(g^{-1}) = e'$ $\therefore ghg^{-1} \in \ker(\phi)$ $\therefore \ker(\phi)$ is normal gp

Sec 14. Factor Groups:

- Thm 14.4, 14.5: G gp. H is normal gp of G, G/H is the set of left cosets of H.

  then: G/H is a gp with binary opt defined by $(aH)(bH) = (ab)H$.

  G/H is called factor gp.

- Thm 14.9: H is normal gp of G. $\varphi: G \to G/H$, $\varphi(a) = aH$. then φ is hom

- Thm 14.11: (Fundamental Hom Thm)

  let $\phi: G \to G'$ be a hom. $\ker(\phi) = H$. Then.

  1. $\phi(G)$ is a subgp of G'
  2. $\mu: G/H \to \phi(G)$, $\mu(gH) = \phi(g)$ is well-defined and μ is isomorphic
  3. $\varphi: G \to G/H$. $\varphi(g) = gH$ is hom. then $\forall g$. $\phi(g) = \mu\varphi(g)$

- Ex: prove $\mathbb{C}^*/U_n$ is isomorphic to $\mathbb{C}^*$

  proof: let $\phi: \mathbb{C}^* \to \mathbb{C}^*$, $\phi(a) = a^n$. we know ϕ is hom. ϕ is onto. that is $\phi(\mathbb{C}^*) = \mathbb{C}^*$

  $\ker(\phi) = \{a^n = 1 \mid a \in \mathbb{C}^*\} = U_n$

  $\therefore \mathbb{C}^*/U_n$ is iso to $\mathbb{C}^*$

- Thm 14.13: $H \subseteq G$ is a subgp. Then: $\forall g \in G, h \in H$, $ghg^{-1} \in H \Leftrightarrow H$ is normal.

- Def 14.15: isomorphism $\phi: G \to G$ is called automorphism.

  inner isomorphism: $i_g: G \to G$, $i_g(x) = gxg^{-1}$

Sec 16. Group Action on a Set.

- Def 16.1: X is a set. G is a gp. Action of G on X: $\cdot : G\times X \to X$, such that.

  1. $ex = x$. $\forall x \in X$
  2. $(g_1g_2)\cdot x = g_1(g_2 x)$ $\forall g_1, g_2 \in G$, $x \in X$

  we wall X is a G-set or G acts on X

- Denote $G_x = \{g \in G \mid gx = x\}$.

- Thm 16.12: X is a G-set. $x \in X$. then G_x is a subgp of G.

  (which is called isotropy subgp of x)

  proof: let $x \in X$. $g_1, g_2 \in G_x$. then $g_1 x = x$, $g_2 x = x$ $\therefore (g_1g_2)x = g_1 x = x$ $\therefore g_1g_2 \in G_x$ $\therefore G_x$ close

  $ex = x$. $\therefore e \in G_x$.

  for $g \in G_x$, then $gx = x$ $\therefore x = ex = g^{-1}gx = g^{-1}x$ $\therefore g^{-1} \in G_x$.

  $\therefore G_x$ is a subgp of G.

- Def 16.15: let X be a G-set. $x \in X$. orbit of x $\overset{\text{def}}{\iff} G\cdot x = \{gx \mid g \in G\}$

- Thm 16.16: let G be a finite gp. X be a G-set, then $\forall x \in X$, $|G\cdot x| \cdot |G_x| = |G|$

  proof: define $\psi : G/G_x \to G\cdot x$, $\psi(gG_x) = gx$

  we need to prove: ψ is well-defined

  ψ is bijection

  $\therefore |G\cdot x| = |G/G_x| = \dfrac{|G|}{|G_x|}$

- Def 18.1: A ring $(R, +, \cdot)$ $\overset{\text{def}}{\iff}$ 1. $(R, +)$ is abelian gp
  2. $\cdot$ is associative
  3. for $a, b, c \in R$: $a\cdot(b+c) = a\cdot b + a\cdot c$, $(b+c)\cdot a = b\cdot a + c\cdot a$.

- Def (Commutative Ring): $\cdot$ is commutative. i.e. $a\cdot b = b\cdot a$ $\forall a, b \in R$

- Def (direct product ring): $R_1 \times \cdots \times R_n$. s.t. $(a_1, \cdots, a_n) + (b_1 \cdots b_n) = (a_1+b_1, \cdots, a_n+b_n)$

  $(a_1, \cdots, a_n)\cdot(b_1, \cdots b_n) = (a_1b_1, \cdots, a_nb_n)$

- Thm 18.8: 0 is additive identity. then: 1. $0a = a0 = 0$
  2. $a(-b) = (-a)b = -(ab)$
  3. $(-a)\cdot(-b) = a\cdot b$

· Def 16.9 : $\phi: R \to R'$ is hom $\overset{\text{def}}{\Leftarrow}$ 1. $\phi(a+b) = \phi(a) + \phi(b)$
2. $\phi(ab) = \phi(a) \cdot \phi(b)$

· Eg: $\phi: \mathbb{Z} \to \mathbb{Z}_n$. $\phi(a) = a \bmod n$. . ϕ is Ring hom.

· Def 16.12 : $\phi: R \to R'$ is iso $\overset{\text{def}}{\Leftarrow}$ ϕ is onto and 1-to-1.

· Def 16.14: Ring with unity $\Leftrightarrow$ if ring has a multiplicative identity. Celeste 1, called unity

· Def 18.1b: let R with $1 \neq 0$. $u \in R$ is unit $\overset{\text{def}}{\Leftarrow}$ $\exists u' \in R$, s.t $u \cdot u' = u' u = 1$.

Division Ring $\overset{\text{def}}{\Leftarrow}$ every non-zero element in R is a unit.

Field $\overset{\text{def}}{\Leftarrow}$ A commutative division ring

i.e. Field $\Leftrightarrow$ 1. R has unity $1 \neq 0$
2. R is commutative ring
3. R has inverse for every non-zero elements.

· Def : R is a commutative ring, a is a 0-divisor $\Leftrightarrow$ 1. $a \neq 0$
2. $\exists b \in R. b \neq 0. ab = 0$

· Def 19.6: Ring D is integral domain $\Leftrightarrow$ 1. D is commutative ring
2. D has unity $1 \neq 0$
3. D has no 0-divisors.

· Thm 19.9: Every field F is an integral domain

proof: we need to prove there is no 0-divisors in F.

let $a, b \in F$. suppose $a \neq 0$. $ab = 0 \Rightarrow \frac{1}{a}(ab) = 0 \Rightarrow b = 0$

∴ if $ab = 0$, a or b must be 0 ∴ there is no 0-divisors in F.

∴ proved!

· Thm 19.11: Every finite integral domain is a field.

proof: we need to prove for every element in integral domain D has an inverse.

let $0, 1, a_1, \cdots a_n$ be all the elements in D. for $a \in D$

then $a \cdot 1, a a_1, \cdots a a_n$ are distinct by cancellation law.

∴ $\exists a_i$. s.t $a a_i = 1$. since · is commutative $a a_i = a_i a = 1$

∴ every element in D has a multiplicative inverse.

· Corollary 19.12: If p is a prime, then $\mathbb{Z}_p$ is a field.

trivially: $\mathbb{Z}_p$ is a integral domain. then $\mathbb{Z}_p$ is a field.

Sec 20. Fermat's. Euler's Thm.

· Thm 20.1: $a \in \mathbb{Z}$. a is not multiple of prime p, then: $a^{p-1} \equiv 1 \pmod p$

($a^{p-1}-1$ divides p) ⟺ equivalent.

· Corollary 20.2: $a \in \mathbb{Z}$. p is prime. then $a^p - a$ is multiple of p

proof of corollary 20.2: (Induction)

for $a=1$: $a^p - a = 1^p - 1 = 0 \cdot p$

for $a > 1$: assume $n^p - n$ is a multiple of p. claim: $(n+1)^p - (n+1)$ is a multiple of p

$$(n+1)^p - (n+1) = \sum_{i=1}^{p-1} \binom{p}{i} n^i + n^p - n$$

$\binom{p}{i}$, $n^p - n$ are multiple of p.

$\therefore (n+1)^p - n+1$ is a multiple of p

· Thm 20.6: let $G_n := \{$ non-0-divisors in $\mathbb{Z}_n \}$, G_n is a gp under multiplication modulo n.

proof: (1) prove G_n is closed: let $a, b \in G_n$. if $ab \notin G_n$. then $\exists c \in \mathbb{Z}_n, c \neq 0$. s.t. $(ab) \cdot c = 0$

$\because b \in G_n \quad \therefore bc \neq 0$ by def. $\quad \therefore a = 0$, which is a contradiction with $a \in G_n$

$\therefore G_n$ is closed.

(2) Obviously. $1 \in G_n$.

(3) claim $\forall a \in G_n$. $\exists$ inverse. let $a \in G_n$

let $1, a_1, \dots, a_r$ be elements in G_n. then $1 \cdot a, \dots, a_r \cdot a$ are distinct.

$\therefore \exists a_i$, s.t. $a_i a = 1$. since $\cdot$ is commutative. $\therefore a a_i = 1$

$\therefore$ exist inverse for a

$\therefore$ for every elements in G_n, there exists an inverse

$\therefore$ proved!

· Def:

Euler phi-function: $\phi(n) :=$ number of non-zero elements in $\mathbb{Z}_n$ that is not 0-divisor.

⟺ $\phi(n) :=$ number of elements in $\{1, \dots n-1\}$ are relatively prime to n.

$\phi(n) = |G_n|$

· Thm 20.8 (Euler's Thm): If $a \in \mathbb{Z}$, a is relative prime to n, then $a^{\phi(n)}-1$ is divisible by n.
($a^{\phi(n)}-1$ is multiple of n or $a^{\phi(n)} \equiv 1 \pmod n$)

· How to compute $\phi(n)$? (1) $\phi(mn)=\phi(m)\cdot\phi(n)$
(2) $\phi(p^k)=p^k-p^{k-1}$

· Euler' Thm implies Fermat's Little Thm.

Sec 21. The field of Quotients of an Integral Domain.

· F is a field, R is a subring of F. $1 \in R$. then R is an integral domain.

⇒ Every integral domain is contained in a field as a subring.

· Def: The smallest field that contains a given integral domain D ⇔ field of quotients of D

Sec 26. Homomorphisms and Factor Rings.

· Def 26.1: $\phi: R \to R'$ is hom $\overset{\text{def}}{\Leftrightarrow}$ $\phi(a+b)=\phi(a)\cdot\phi(b)$, $\phi(ab)=\phi(a)\phi(b)$. $\forall a,b \in R$.

· Def (subring): R is a ring. $S \subseteq R$ is a subset. then S is a subring ⇔ S is closed under $+,\cdot$.
$(S,+,\cdot)$ is a ring.

· Thm 26.3: $\phi: R' \to R$ is hom, then: 1. $\phi(0)=0'$
2. $\phi(-a)=-\phi(a)$, $\forall a \in R$.
3. $S \subseteq R$ is subring ⇒ $\phi(S)$ is subring of R'
4. $S' \subseteq R'$ is subring ⇒ $\phi^{-1}(S')$ is subring of R.

· Def 26.4: $\phi: R \to R'$ is ring hom, then $\phi^{-1}(0')=\{a \in R \mid \phi(a)=0\}$ is called kernel of ϕ.
denoted as $\ker(\phi)$

· Thm: ϕ is a ring hom, $\ker(\phi)$ is a subring.

· Def (Ideal): R is a ring, subset $I \subset R$ is called an ideal $\overset{\text{def}}{\Leftrightarrow}$ 1. I is an subgp of $(R,+)$
2. $\forall a \in R, b \in I$.

· Corollary 26.14: I is an ideal of R. then R/I is a ring under $+,\cdot$.

R/I is called the factor ring of R by I.

· Thm 26.17 (Fundamental Homomorphism Thm): Let $\phi: R \to R'$ be a ring hom with kernel N.

then $\phi(R)$ is a subring of R'. $\mu: R/N \to \phi(R)$, $\mu(a+N) = \phi(a)$.

μ is well-defined, and is an isomorphism of rings.