Group:

a set G, binary operation (closed)

(1) Associative (2) Identity (3) Inverse

Subgroup:

prop: $H \leq G$ if (1) H non-empty ($e \in H$)

(2) If $a, b \in H$, $ab \in H$ (mult in G)

(3) If $a \in H$, $a^{-1} \in H$ (inverse in G)

X a set

$\underline{Sym(X)}$:= set of all bijections : $X \to X$

($Sym(X)$, composition of functions) is a group

GCD (a,b), $a,b \in \mathbb{Z}$ is a $d \in \mathbb{Z}_{\geq 0}$ s.t.

(1) $d \mid a$ and $d \mid b$, (2) if $e \mid a$, $e \mid b$, $e \mid d$

$I(a,b) = \mathbb{Z} \cdot d$

↳ Euclidean Algorithm

$$(F(m,n) = \begin{cases} (n,r),\ r = \text{rem}(r) & \text{if } n \neq 0 \\ 0 & \text{if } n = 0 \end{cases}$$

$m = qn + r,\ 0 \leq r < |n|$

Relatively prime: $\gcd(a,b) = 1$

If $\gcd(a,b) = 1$, and if $a \mid n$, $b \mid n$, then $ab \mid n$

$$\text{lcm}(a,b) = \frac{ab}{\gcd(a,b)}$$

Equivalence Relation if:

(1) Reflexive : $a \sim a$

(2) Symmetric : $a \sim b \Rightarrow b \sim a$

(3) Transitive : $a \sim b,\ b \sim c \Rightarrow a \sim c$

Congruence class: $[a]_n = \{a + kn \mid k \in \mathbb{Z}\}$

$\mathbb{Z}_n$ = set of congruence class. ($(\mathbb{Z}_n, +, \cdot)$ is a comm ring with 1)

Fermat's Little Thm:

Let p be prime, $a \in \mathbb{Z}$

(1) $a^p \equiv a \pmod{p}$

(2) if $p \nmid a$, then $a^{p-1} \equiv 1 \bmod (p)$

Isomorphism of groups

$\phi: G \to H$ is a bijection such that

$\phi(ab) = \phi(a)\phi(b)$

$D_3 \cong S_3$

Homomorphism of groups:

$\phi: G \to H$ is a function s.t. $\varphi(ab) = \varphi(a)\varphi(b)$

Image: $\varphi(G) = \{\varphi(g) \mid g \in G\} \leq H$

Kernel: $\ker(\varphi) := \{g \in G \mid \varphi(g) = e_H\} \leq G$ actually $\ker(\varphi) \trianglelefteq G$.

Prop: Hom $\varphi: G \to H$ is injective iff $K = \ker(\varphi) = \{e\}$

G a Group, $S \subseteq G$,

$\langle S \rangle := \bigcap H_i$ (all H_i s.t. $S \subseteq H_i$)

$= \{e\} \cap \{g_1 g_2 \cdots g_k \mid k \geq 1, i = 1, \dots, k, g_i \in S \text{ or } g_i^{-1} \in S\}$

Cyclic Subgroup : G - a group, $H \leq G$ is cyclic if :
$H = \langle a \rangle$ for some $a \in G$.

$\langle a, b \rangle = \{ma + nb \mid m, n \in \mathbb{Z}\} = I(a, b) = \mathbb{Z} \cdot d = \langle d \rangle$ is cyclic.

Order of elem.

$\text{order}(a) = |\langle a \rangle| = n$

If $n < \infty$ then n is the smallest integer s.t. $a^n = e$

Dihedral Group For Disk

$r_\alpha r_\beta = r_{\alpha+\beta}$ $\quad r_\alpha j_\beta = r_{\beta+\frac{\alpha}{2}}$ $\quad j_\alpha r_\beta = j_{\alpha-\frac{\beta}{2}}$ $\quad j_\alpha j_\beta = r_{2(\alpha-\beta)}$

$j_\alpha = r_{2\alpha} j_0 = j_0 r_{-2\alpha}$

Dihedral Groups

$D_n = \{e, r, \dots, r^{n-1}, j, rj, r^2j, \dots, r^{n-1}j\}$ $\quad |D_n| = 2n$

$r^n = e, \quad j^2 = e \qquad jr = r^{-1}j \Rightarrow jr^k = r^{-k}j$

$D_n = \langle r, j \rangle$

Normal Subgroup of G is a $N \leq G$ s.t.

$gNg^{-1} = N$ for all $g \in G$.

$\parallel$

$\{gng^{-1} \mid n \in N\}$

prop. just show $gNg^{-1} \subseteq N$, it gives the other side automatically

example $\langle r \rangle \trianglelefteq D_3$ but $\langle j \rangle$ is not normal in D_3.

$rjr^{-1} = r^2j \notin \{e, j\}$

Cosets : $H \leq G$, $a \in G$

Left H coset : $gH = \{gh \mid h \in H\} \subseteq G$

Right H coset : $Hg = \{hg \mid h \in H\} \subseteq G$

$\Rightarrow$ partition of G.

prop: $H \leq G$, If X, Y are two cosets of G, then either

$X \cap Y = \emptyset$ or $X = Y$ $\Rightarrow$ partition

prop: followings are equal. $H \leq G$, $a, b \in G$.

(1) $a \in bH$ (2) $b \in aH$ (3) $aH = bH$

(4) $a^{-1}b \in H$ (5) $b^{-1}a \in H$

Lagrange Thm:

If G finite group, $H \leq G$, then $|H|$ divides $|G|$

Order Thm:

If G finite group, $g \in G$, then $o(g) = |\langle g \rangle|$ divides $|G|$.

The index of a subgroup $H \leq G$ is the number of left H cosets.

$$\text{index} = [G:H].$$

If $|G| < \infty$, $[G:H] = \frac{|G|}{|H|}$

Prop: If $G/Z(G)$ is cyclic, then G is abelian.

prop: followings equal:

(1) H is a normal subgroup

(2) left H cosets are the same as right H cosets ☆

(3) Every left H-coset is contained in a right H-coset

prop: If $H \leq G$ and $[G:H]=2$, $H \trianglelefteq G$.

prop: If $G/Z(G)$ is cyclic, G is abelian.

Generalized Lagrange: $G \geq H \geq K$

Then $[G:K] = [G:H][H:K]$

Quotient Group : $H \le G$

$G/H := \{aH \mid a \in G\}$ = set of all left H-coset in G.

Quotient function : $\pi : G \to G/H$ is a hom.

$\pi(g) :\to gH$

$\ker(\pi) = \{g \in G \mid \pi(g) = e_{G/H}\} = \{g \in G \mid \pi(g) = eH = H\} = H$

$\ker(\pi) \trianglelefteq G \Rightarrow H \trianglelefteq G$ (this is a motivation)

☆ $H \trianglelefteq G \to (G/H, \cdot)$ is a group

Ex) $G = \mathbb{Z}$, $H = \mathbb{Z} \cdot n$, $G/\mathbb{Z} \cdot n = \mathbb{Z}_n$

Cycle conjugation formula: $\tau = (a_1 a_2 \dots a_k) \in S_n$

$\sigma, \tau \in S_n$, $\sigma \tau \sigma^{-1} = (\sigma(a_1) \sigma(a_2) \dots \sigma(a_k)) \in S_n$

Fact: τ and $\sigma \tau \sigma^{-1}$ has the same cycle type.

Obs: A subgroup $H \leqslant S_n$ is normal iff whenever $g \in H$, then so is every element with the same cycle type.

Homomorphism Thm:

Given
- group G, $N \trianglelefteq G$
- homomorphism $\varphi : G \to H$, s.t. $N \subseteq \ker(\varphi)$

Then $\exists$ hom. $\varphi' : G/N \to H$

$$aN \mapsto a$$

and $\ker(\varphi') = \ker(\varphi)/N = \{aN \mid aN \in K\}$

$$\begin{tikzcd}
G \arrow[r, "\varphi"] \arrow[d, "\lambda"'] & H \\
G/N \arrow[ur, "\varphi'"'] &
\end{tikzcd}$$

Isomorphism Theorem :

hom thm, but use surjective hom. $G \twoheadrightarrow H$,

and use $N = \ker(\varphi)$

Correspondence Thm : $N \trianglelefteq G$

$$\{\text{subgroup of } G/N\} \xleftrightarrow{\text{bijection}} \left\{\begin{matrix}\text{subgroup of } G \\ \text{which contains } N\end{matrix}\right\}$$

$$\begin{tikzcd}
G \arrow[r, two heads] & G/N \\
A \arrow[u, hook, "\leq"] \arrow[r, leftrightarrow] & B \arrow[u, hook, "\leq"']
\end{tikzcd}$$

$(N \subseteq A)$

$B \leq G/N \to \pi^{-1}(B)$

$\pi^{-1}(B) = \{g \in G \mid \pi(g) \in B\} \leq G$

Ex) $G = \mathbb{Z}$, $N = \mathbb{Z}6$

Factorization Thm:

If $N \leq K \leq G$, N, K normal in G,

Then surjective $\varphi: G/N \twoheadrightarrow G/K$
$$xN \mapsto xK$$

By iso thm, $\exists$ $(G/N)/(K/N) \cong (G/N)$ as $\ker(\varphi) = K/N$

use $xK = K \Rightarrow x \in K$

Product Subset: $A, B \subseteq G$,

$AB := \{ab \mid a \in A, b \in B\} \subseteq G$ $BA := \{ba \mid a \in A, b \in B\} \subseteq G$

If $A, B \leq G$, then $AB \leq G$ iff $AB = BA$.

$$|AB| = \frac{|A|\,|B|}{|A \cap B|}$$

Diamond Isomorphism Thm :

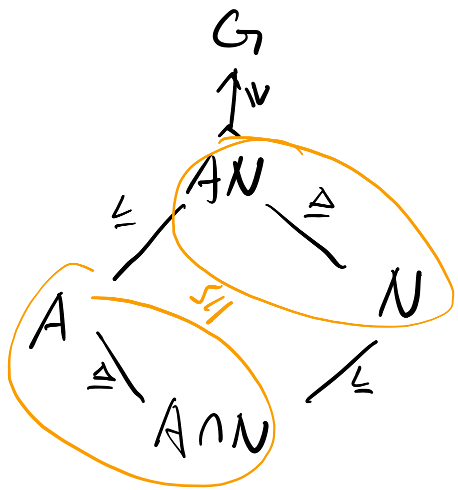
Given group G, $A \leq G$, $N \trianglelefteq G$. Then:

(1) $AN = NA$

(2) $AN \leq G$, $N \trianglelefteq AN$

(3) $A \cap N \trianglelefteq A$

(4) $AN/N \cong A/A\cap N$



Direct Product : $G \times H = \{(g,h) \mid g \in G, h \in H\}$

operation : $(g_1, h_1) \cdot (g_2, h_2) = (g_1 g_2, h_1 h_2)$

Identity : (e_G, e_H) Inverse : $(a,b)^{-1} = (a^{-1}, b^{-1})$

$|G \times H| = |G|\,|H|$

$(G \times H, \text{component-wise} \cdot)$ is a group

Chinese Remainder Thm:

If $a, b \geq 1$, $\gcd(a,b) = 1$, then have isomorphism:

$\gamma: \mathbb{Z}_m \xrightarrow{\cong} \mathbb{Z}_a \times \mathbb{Z}_b$, $m = ab$ by $[x]_m \longmapsto ([x]_a, [x]_b)$

Reverse: If $\gcd(a,b) > 1$, then $\mathbb{Z}_a \times \mathbb{Z}_b \not\cong \mathbb{Z}_{ab}$

Also, $\Phi(m) \cong \Phi(a) \times \Phi(b)$ under same condition.

Also CRT:

If $a, b \geq 1$, $\gcd(a,b) = 1$, $m := ab$. For any $\alpha, \beta \in \mathbb{Z}$, $\exists x \in \mathbb{Z}$

s.t. $x \equiv \alpha \bmod a$ and $x \equiv \beta \bmod b$

and any such x's (x_1, x_2), $x_1 \equiv x_2 \bmod (m)$

Recognition Thm For Direct Product

Group G, $A, B \le G$, and if :

(1) A, B normal in G (2) $A \cap B = \{e\}$ (3) $AB = G$

Then $\exists$ isomorphism φ : $A \times B \xrightarrow{\cong} G$ by $(a,b) \longmapsto ab$

Automorphism : is an iso. $\varphi : G \to G$

$$\mathrm{Aut}(G) := \{\varphi : G \to G \text{ automorphism}\} \le \mathrm{Sym}(G)$$

By lagrange, $|\mathrm{Aut}(G)|$ divides $|\mathrm{Sym}(G)| = |G|!$

$$\Phi(n) \cong \mathrm{Aut}(\mathbb{Z}_n)$$

$[a] \to \gamma_a$ ← automorphism.

$\downarrow$

$\gamma_a([x]) = [ax]$

Semi-direct Product

Given A, N groups, $\gamma : A \to \mathrm{Aut}(N)$ homo.
$a \to \gamma_a$

γ has properties:

① $\gamma_a(n_1 n_2) = \gamma_a(n_1)\gamma_a(n_2)$

② $\gamma_{a_1 a_2}(n) = \gamma_{a_1}(\gamma_{a_2}(n))$

③ $\gamma_e = id$, $\gamma_{a^{-1}} = (\gamma_a)^{-1}$

product $G := N \rtimes_\gamma A$

Set : $G = N \times A = \{(n,a), n \in N, a \in A\}$

Operation: $(n_1, a_1) \cdot (n_2, a_2) = (n_1 \gamma_{a_1}(n_2), a_1 a_2)$

This is a group! Identity (e_N, e_A) Inverse : $(n,a)^{-1} = (\gamma_{a^{-1}}(n^{-1}), a^{-1})$

Recognization Theorem for Semi-direct Product

Group G, $A \le G$, $N \trianglelefteq G$, $A \cap N = \{e\}$, $NA = G$

Then $N \rtimes_\gamma A \cong G$ by $(n,a) \mapsto na$

where $\gamma : A \to \mathrm{Aut}(N)$ by $\gamma_a(n) = ana^{-1} \in N$, $a \in A$, $n \in N$

Classification of Finite / Finitely Generated Abelian Group.

Elementary Divisor Form:

$$G \cong \mathbb{Z}_{p_1^{r_1}} \times \mathbb{Z}_{p_2^{r_2}} \times \cdots \mathbb{Z}_{p_k^{r_k}}$$

$|G| = 24 = 2 \times 2 \times 2 \times 3$, G abelian. Then G must be one of following:

$$\mathbb{Z}_{2^3} \times \mathbb{Z}_{3^1} \cong \mathbb{Z}_{24} \qquad \mathbb{Z}_{2^2} \times \mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_2 \times \mathbb{Z}_{12} \qquad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_6$$

Invariant Factor Form:

$$G \cong \mathbb{Z}_{a_1} \times \mathbb{Z}_{a_2} \times \cdots \mathbb{Z}_{a_s}, \qquad a_i \mid a_{i+1}$$

Example G abelian, IF: 5, 25, 50, 36000

Transformation: IF $\Longleftrightarrow$ ED :

Given IF : 5, 25, 50, 36000

① list from small to large

IF	ED		
5			5^1
25			5^2
50	2^1		5^2
36000	2^5	3^2	5^3

② ↗ factor them

Given ED: $2^1, 2^5, 3^2, 5^1, 5^2, 5^2, 5^3$

① align them small to large

ED			$\Rightarrow$
		5^1	Z^{5}
		5^2	Z^{25}
2^1		5^2	Z^{50}
2^5	3^2	5^3	Z^{36000}

② multiply

Group Action

A group action by G on X (X is a set, G group)

is a homomorphism $\varphi: G \to Sym(X)$

$$g \to \varphi(g)$$
$$\downarrow$$
$$\varphi(g)(x) \in X$$
$$\parallel$$
$$gx$$

simplify

Orbit is a subst of X:

$O(x) = \{gx \mid g \in G\}$ for some $x \in X$.

orbits partition X into pairwise disjoint and nonempty subsets

Action is transitive if there is only one orbit $O(x) = X$

Stabilizer: $Stab(x) = Stab_G(x) = \{g \in G \mid gx = x\}$ "g that fixes x"

$Stab(x) \leq G$.

If $y = gx$, $x, y \in X$, $g \in G$, then $Stab(y) = g\, Stab(x)\, g^{-1}$

Action $\varphi: G \to Sym(X)$, then $ker(\varphi) = \{g \in G \mid gx = x \ \forall x \in X\}$

$$= \bigcap_{x \in X} Stab(x) \trianglelefteq G$$

Action is faithful if $ker(\varphi) = \{e\}$

Orbit Stabilizer Theorem : G acts on X

If $x \in X$, then there is a bijection

$$\partial : G/H \longrightarrow O(x) \quad , H = \mathrm{Stab}(x)$$

by

$$gH \longrightarrow gx$$

$$\Rightarrow |O(x)| = [G : \mathrm{stab}(x)] = \frac{|G|}{|\mathrm{stab}(x)|}$$

↳ if $|G| < \infty$

Cayley Theorem

Every finite group G is isomorphic to a subgroup of some symmetric group S_n

Conjugate action

$C: G \to Sym(X)$, $G = X$

$C(g)(x) = gxg^{-1}$ $\quad$ $C(g)$ is an auto.

$x \in X = G$, $Cl(x) = \{gxg^{-1} \mid g \in G\} \subseteq G$ $\quad$ conjugacy class of x $\simeq$ Orbit

centralizer: $Cent(x) = \{g \in G \mid gxg^{-1} = x\} \leq G$ $\quad$ $\simeq$ stabilizer

$$\ker(c) = \{g \in G \mid gx = xg \;\; \forall x \in G\}$$
$$= \bigcap_{x \in G} Cent(x)$$

orbit / stab thm here: $\quad |Cl(x)| = \dfrac{|G|}{|Cent(x)|}$ $\quad |G| < \infty$

Burnside Formula: If G acts on X, and $|G| < \infty$, $|X| < \infty$,

then the number of orbits $= \frac{1}{|G|} \sum_{g \in G} |Fix(g)|$

Define $X^G = \{x \in X \mid gx = x$ for all $g \in G\} \subseteq X$

$= \bigcap Fix(g)$

$\hookrightarrow Fix(g) = \{x \in X \mid gx = x\}$

p-group : is a group of order p^k.

p-group Fixed Point Thm.

$$|X^G| \equiv |X| \mod p$$

Cauchy Theorem: If prime p divides $n = |G|$,

then G has an element of order p.

Classification of Group of order $2p$. (p prime).

$\mathbb{Z}_{2p} \cong \mathbb{Z}_2 \times \mathbb{Z}_p$ or $\mathbb{Z}_{2p} \cong D_p$

of order pq, $p > q$ prime.

(1) $q \nmid p-1$ $\mathbb{Z}_{pq} \cong \mathbb{Z}_p \times \mathbb{Z}_q$

(2) $q \mid p-1$ $\exists$ non-trivial homomorphism γ

Ring

R, a set with operation $+$, $\cdot$ s.t.

(1) $(R, +)$ is an abelian group

(2) mult is associative $(ab)c = a(bc)$ $\forall a, b, c \in R$

(3) distributive low $(a+b)c = (a+c) + (b+c)$

$a(b+c) = (ab) + (ac)$

Ring with identity : $\exists\, 1 \in R$ s.t. $1a = a = a1$ for all $a \in R$

Commutative ring : $\forall a, b \in R$, $ab = ba$

$a \in R$ is a unit if $\exists\, b \in R$ s.t. $ab = 1 = ba$

Field : comm. ring with 1. such that every non-zero elem. is a unit

Subring, prop: $S \subseteq R$ is a subring iff:

Ex) $R = \mathbb{Z}$, $S = \mathbb{Z}2$

(1) $0 \in S$ $(S \neq \emptyset)$

(2) if $a, b \in S$, $a+b, ab \in S$

(3) if $a \in S$, then $-a \in S$

Define $R[x]$ to be the set of expressions:

$$f = \sum_{k=0}^{n} a_k x^k$$

Such $R[x]$ is a polynomial ring

deg(f) := largest integer n s.t. $a_n \neq 0$.

If K = field, $p, d \in K$, $\deg(d) > 0$, then $\exists$ unique $q, r \in K[x]$ s.t.

(1) $P = dq + r$

(2) $\deg(r) < \deg(d)$

$$\frac{P}{d} = q + \frac{r}{d}$$

Homomorphism of Rings $\varphi: R \to S$ is function s.t.

(1) $\varphi: (R,+) \to (S,+)$ is a group hom.

(2) $\varphi(ab) = \varphi(a)\varphi(b) \quad \forall a,b \in R.$

Iso. of Rings : Hom. that φ is a bijection.

Substitution Principle Given $\varphi: R \to S$ a unital ring hom. and $c \in S$

Then $\exists$ unique ring homo.

$$\varphi_c : R[x] \to S$$

S.t. (1) $\varphi_c(r) = \varphi(r)$ if $r \in R \subseteq R[x]$

(2) $\varphi_c(x) = c$ (x itself is a polynomial)

If $R=S$, $\varphi: R \to R$ is id, $\varphi_c(f) = ev_c(f) = \sum_{k=0}^{n} a_k c^k \in R$

Ideal $I \subseteq R$ s.t.

(1) $I \leq R$

(2) $a \in I$, $r \in R \Rightarrow ar, ra \in I$

$\varphi: R \to S$ a hom. Then $\ker(\varphi) = \{r \mid \varphi(r) = 0\}$ is an ideal.

If $\{I_\alpha\}$ is a collection of all ideals in R, $I = \bigcap_\alpha I_\alpha$ is an ideal.

$S \subseteq R$, define $(S) := \bigcap I$ s.t. $S \subseteq I$ is an ideal in R.

"ideal generated by S"

$$(S) = \{0\} \cup \{a_1 s_1 b_1 + \dots + a_k s_k b_k \mid k \geq 1, s_1, \dots, s_k \in S, a_i, b_i \in R\}$$

Principle ideal: Ideal I s.t. $I = (r)$ for single $r \in R$. so

$$(r) = \{0\} \cup \{a_1 r b_1 + \dots + a_k r b_k \mid a_i, b_i \in R\}$$

If R comm. $(r) = \{ar \mid a \in R\}$

If K field. Only ideals are $\{0\}$ and K

$$\{0\} = (0) \qquad K = (1)$$

$R = \mathbb{Z}$, all ideals are in form $(d) = \mathbb{Z}d \longrightarrow$ all principle

prop : K field, $R = K[x]$. Every ideal in R is principle.

If $I \subseteq R$, $\exists$ unique f s.t $(f) = I$ and either $f=0$ or f is monic.

$\Downarrow$

$a_n = 1$

Quotient Ring : I ideal in R.

$R/I = \{a + I \mid a \in R\}$ set of I-coset

Homomorphism Theorem

Let $\varphi : R \to S$ be a ring hom. $I \subseteq R$ an ideal

If $I \subseteq \ker(\varphi)$, then $\exists$ a ring hom. $\bar{\varphi} : R/I \to S$ s.t. $\bar{\varphi}(a+I) = \varphi(a)$

$$\begin{tikzcd} R \arrow[r, "\varphi"] \arrow[d, "\pi"'] & S \\ R/I \arrow[ur, "\bar{\varphi}"'] & \end{tikzcd}$$

Iso: surjective φ, $I = \ker(\varphi)$.

Domain: R is a comm. ring with 1. s.t.

(1) $1 \neq 0$ (2) If $a, b \in R \setminus \{0\}$, then $ab \in R \setminus \{0\}$

R - Domain has four types of elements:

- $0 \in R$
- units: $u \in R^\times$
- reducible: $a \in R$, $a \neq 0$, $a \notin R^\times$, $\exists\, b, c \in R$, $b, c \notin R^\times$ s.t. $a = bc$
- irreducible: $a \in R$, $a \neq 0$, $a \notin R^\times$, a not reducible.

Gaussian Integers: $R = \mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$ domain

Norm Function: $N(a+bi) = a^2 + b^2 = (a+bi)(a-bi)$

If $z, w \in \mathbb{Z}[i]$, $N(zw) = N(z) N(w)$

If $p \in \mathbb{N}$ is a prime, then p is reducible in $\mathbb{Z}[i]$ iff $p = a^2 + b^2$, $a, b \in \mathbb{Z}$.

a is irreducible if whenever $b | a$, either b is a unit or $b \sim a$

$p \in R$ is a prime if $\forall a, b \in R$, if $p | ab$, then either $p | a$ or $p | b$.

prop: If $p \in R$-domain is a prime, then p is irreducible.

Principle Ideal Domain: a domain R s.t. every ideal is a principle ideal.

Ex Field K, $\mathbb{Z}$, $\mathbb{Z}[i]$, non-PID: $\mathbb{Z}[x]$, $\mathbb{Z}[\sqrt{-5}]$, $K[x,y]$

In PID, irreducible $\Longleftrightarrow$ prime

<u>Thm</u>: Every irreducible $u \in R = \mathbb{Z}[i]$ is the same up to units to:

(1) $u = 1+i$ (lies over 2)

(2) For p prime, $p \equiv -1 \mod 4$, $u = p$ (lies over p)

(3) For p prime, $p \equiv 1 \mod 4$, $u = a+bi$ or $u = a-bi$ where $a^2+b^2 = p$, $a > b > 0$, $a, b \in \mathbb{Z}$.