# * Group Theory Factoids:

- Euler $\varphi$ $f^n$ - # $\mathbb{Z}^+$ $a \le n$ s.t. $(a,n)=1$

$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}$

$\varphi(n) = \varphi(p_1^{\alpha_1})\,\varphi(p_2^{\alpha_2}) \ldots \varphi(p_s^{\alpha_s})$

$\varphi(n) = p_1^{\alpha_1 - 1}(p_1 - 1)\, p_2^{\alpha_2 - 1}(p_2 - 1) \ldots p_s^{\alpha_s - 1}(p_s - 1)$.

- $\mathbb{Z}/n\mathbb{Z} \to \{\bar{0}, \bar{1}, \bar{2}, \ldots \overline{n-1}\}$

$\bar{a} + \bar{b} = \overline{a+b}$ $\quad \bar{a} \cdot \bar{b} = \overline{ab}$

- $(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} \text{ s.t. } \exists \bar{c} \text{ s.t. } \bar{a}\cdot\bar{c} = \bar{1}\}$

$= \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} \mid (a,n) = 1\}$

# $S_n$ - Symmetric groups:-

- $S_n$ non-ab for $n \ge 3$
- disjoint cycles commute
- $n \ge m$ # of $m$-cycles in $S_n$ is

$$= \frac{n(n-1)\ldots(n-m+1)}{m}.$$

# Group Act^ns :-

$g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$

& $1 \cdot a = a$

$a \in A$ = a set on which $G$ acts.

# Cyclic groups & subgroups :- $H = \langle x \rangle$

- $Z_n \to$ Cyclic group of order $n$, written multiplicatively

- $G$ = group $x \in G$ & $a \in \mathbb{Z} - \{0\}$

(i) if $|x| = \infty \Rightarrow |x^a| = \infty$

(ii) if $|x| = n < \infty \Rightarrow |x^a| = \dfrac{n}{(n,a)}$

(iii) if $|x| = n$, $a \mid n \Rightarrow |x^a| = \dfrac{n}{a}$.

# let $H = \langle x \rangle$.

(i) if $|x| = \infty \Rightarrow H = \langle x^a \rangle$ iff $a = \pm 1$.

(ii) if $|x| = n < \infty \Rightarrow H = \langle x^a \rangle$ iff $(a,n) = 1$

& # generators of $H = \varphi(n)$.

Ex.) $\mathbb{Z}/12\mathbb{Z} \to \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{11}\}$.

(a) $\mathbb{Z}/12\mathbb{Z} = \langle \bar{1} \rangle = \langle \bar{5} \rangle = \langle \bar{7} \rangle = \langle \overline{11} \rangle$ (order 12)

(b) $\langle \bar{2} \rangle = \langle \overline{10} \rangle$ order 6

(c) $\langle \bar{3} \rangle = \langle \bar{9} \rangle$ — 4

(d) $\langle \bar{4} \rangle = \langle \bar{8} \rangle$ — 3

(e) $\langle \bar{6} \rangle$ — 2

(f) $\langle \bar{0} \rangle$ — 1.

Inclusions:-

$\langle \bar{a} \rangle \le \langle \bar{b} \rangle$

iff $(b, 12) \mid (a, 12)$

# Quotient Groups & Homomorphisms:

$G/K = \{gK \mid g \in G\}$

$G \backslash K = \{Kg \mid g \in G\}$ , K normal in G.

if $G/K = G\backslash K \rightarrow K \trianglelefteq G$. &

if $N \trianglelefteq G \rightarrow gng^{-1} \in N \; \forall n \in N, g \in G$

$\varphi : G_1 \to G_2$ $\quad \varphi(xy) = \varphi(x)\varphi(y)$

$\rightarrow$ homomorphism.

# Lagrange's Theorem: G = Finite group.

$H \le G \rightarrow |H| \mid |G|$.

& # of left cosets of $H$ in $G$ $= \dfrac{|G|}{|H|} = [G:H]$.

- $H \le G$, $K \le G \rightarrow HK = \{hk \mid h \in H, k \in K\}$

- $|HK| = \dfrac{|H||K|}{|H \cap K|}$

- $HK \le G$ iff $HK = KH$.

# Isomorphism theorems:

(1) $\varphi : G \to H$ homomorphism

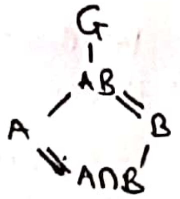
(i) $\ker\varphi \trianglelefteq G$ & (ii) $G/\ker\varphi \cong \varphi(G)$.

(i) $\varphi$ injective iff $\ker\varphi = \{1\}$.

(ii) $|G : \ker\varphi| = |\varphi(G)|$

Scanned by CamScanner

② Dimond isomorphism thm :-




$A, B \leq G$ & $A \leq N_G(B)$

$\Rightarrow$ $AB \leq G$, $B \trianglelefteq AB$, $A \cap B \trianglelefteq A$

& $AB/B \simeq A/A\cap B$.

---

③ 3rd iso. thm : $H, K \leq G$, $H \leq K$

$\dashv$ $K/H \trianglelefteq G/H$ & $(G/H)/(K/H) \cong G/K$.

---

④ Lattice iso. thm :- $A, B \leq G$

$N \leq A$, $N \leq B$, $N \trianglelefteq G$

(i) $A \leq B \Leftrightarrow \bar{A} \leq \bar{B}$ ... $\bar{A} \equiv A/N$, $\bar{B} \equiv B/N$

(ii) $A \leq B \Rightarrow |B : A| = |\bar{B} : \bar{A}|$

(iii) $\overline{\langle A, B \rangle} = \langle \bar{A}, \bar{B} \rangle$

(iv) $\overline{A \cap B} = \bar{A} \cap \bar{B}$

(v) $A \trianglelefteq G \Leftrightarrow \bar{A} \trianglelefteq \bar{G}$

---

# Cauchy's Thm for Abelian groups :-

$G \equiv$ finite Ab. group. $p \equiv$ prime s.t.

$p \mid |G| \dashv \exists\, x \in G$ s.t. $|x| = p$.

---

# Simple Groups :- $G$ simple if $|G| > 1$ & the only normal sub groups of $G$ are $\{1\}$ & $\{G\}$.

---

# Jordan-Hölder Alg. :-

$\{1\} = G_0 \trianglelefteq G_1 \dots \trianglelefteq G_s = \{G\}$

Solvable iff $G_{i+1}/G_i$ Abelian.

---

# if $N$ & $G/N$ solvable $\Rightarrow G$ is solvable.

---

# Alternating Group: $A_n$: $A_n \leq S_n$

s.t. $\sigma \in A_n \equiv$ even parity

- All $\sigma$'s $\in S_n$ can be written as a series of transpositions.

$\sigma = (123) = (13)(12)$

- sign(1 transposit$^n$) $= -1$ ← check notes/book.
- $\epsilon(\sigma) \equiv$ sign of $\sigma$. $\epsilon[(ij)] = -1$
- $\sigma \equiv$ even perm. if $\epsilon(\sigma) = +1$ ← even # of transposit$^n$s
  $\equiv$ odd perm — " — " $= -1$. ← odd — " —

---

# Group Act$^n$s:

$\sigma_g : A \to A$ def. by $\sigma_g : a \mapsto g \cdot a$

is a perm. of $A$. Associated homomorphism

$\varphi : G \to S_A$ def by $\varphi(g) = \sigma_g$

Perm. representat$^n$ associated w/ given act$^n$.

---

- If def$^n$ $\sim$ s.t. $a \sim b$ iff $a = g \cdot b$

$\rightarrow$ $\sim$ $\equiv$ equivalence rel$^n$

$\dashv$ partitions the set.

| # of elements in the equivalence class of a $= [G : G_a]$ | STABILIZER OF A $\{g \mid g a = a\}$

---

# Cycle Decompositions:

$\sigma \in S_n \rightarrow$ has a unique cycle decomposit$^n$

let $A = \{1, 2, \dots n\}$, $\sigma \in S_n$ & $G = \langle \sigma \rangle$

$\langle \sigma \rangle$ acts on $A \Rightarrow$ partit$^n$s $A$ in disjoint orbits

$O \equiv$ an orbit & $x \in O$

$d = |O| = |G : G_x|$ ← orbit-stabilizer result

$O \equiv \{x, \sigma(x), \sigma^2(x), \dots \sigma^{d-1}(x)\}$.

& so-on. ↳ d-cycle.

---

# Groups acting on themselves by left mult : Cayley's Thm :-

$G$ acting on itself → $g \cdot a = ga$; $g, a \in G$.

label elements of $G = \{g_1, g_2, \dots g_n\}$

$\sigma_g(i) = j$ iff $g g_i = g_j$

---

CAYLEY'S THM: If $|G| = n$ then $G \simeq H$

Where $H \leq S_n$.

Scanned by CamScanner

# Groups Acting on Themselves By Conjugat$^n$:

The Class Eq$^n$:-

$g \cdot a = gag^{-1}$

- $O_a \equiv$ conjugacy class of a
- $G_S = \{g \in G \mid gSg^{-1} = S\} = N_G(S)$ — normalizer of S.

stabilizer of S

- $N_G(\{s\}) = C_G(s)$

$|O_a| = |G : N_G(S)| = |G : C_G(s)|$.

The Class Eq$^n$: $\boxed{|G| = |Z(G)| + \sum_{i=1}^{r} |G : C_G(g_i)|}$

$g_1, g_2, \ldots g_r \equiv$ representatives of distinct conj. classes not contained in center $Z(G)$

$Z(G) = \{x \in G \mid xg = gx\} \ \forall g \in G$.

- $p \equiv$ prime & $|P| = p^\alpha$ ← p-group, $\alpha \geq 1$

$\Rightarrow$ $P$ has a non-trivial center $Z(P) \neq \{1\}$

$\rightarrow$ $|P| = |Z(P)| + \underbrace{\sum_{i=1}^{r} |P : C_P(g_i)|}_{p \mid |P : C_P(g_i)|}$

$p \mid p^\alpha$

$\Downarrow$

$\boxed{p \mid |Z(P)|}$ ← QED.

# Conjugacy in $S_n$:

- $\sigma = (a_1 a_2 \ldots a_{k_1})(b_1 b_2 \ldots b_{k_2}) \ldots$

$\tau\sigma\tau^{-1} = (\tau(a_1)\tau(a_2) \ldots \tau(a_{k_1}))(\tau(b_1) \ldots \tau(b_{k_2})) \ldots$

- Two elements of $S_n$ conj. in $S_n$ iff they have same cycle-decomp.-type.

e.g. $\sigma_1 = (1)(35)(89)(2476)$

$\sigma_2 = (3)(47)(81)(5269)$

define $\tau(1) = 3$, $\tau(3) = 4$, $\tau(5) = 7$, etc.

$\tau = (13425769)(8)$

$\tau\sigma_1\tau^{-1} = \sigma_2$.

- 

| Partit$^n$ of 3 | representative of conj class |
|---|---|
| 1, 1, 1 | 1 |
| 1, 2 | (12) |
| 3 | (123 |

- $A_5$ is a simple group. | $A_{n \geq 5}$ is simple.

# Sylow's Theorem:

$G \equiv$ group $p \equiv$ prime.

(i) Group of order $p^\alpha$, $\alpha \geq 0$ → p-group.

$Q \leq G$, $|Q| = p^\alpha$ → $Q \equiv$ p-subgroup of G.

(ii) if $|G| = p^\alpha m$, $p \nmid m$, $P \leq G$ s.t. $|P| = p^\alpha$ → $P$ = Sylow-p subgroup of G.

(iii) $Syl_p(G) \equiv \{$set of $P$ s.t. $|P| = p^\alpha\}$.

Sylow Theorem:- $|G| = p^\alpha m$, $p \nmid m$,

(i) Sylow-p-subgroups of G exist.

(ii) $P \equiv$ Sylow-p subgroup

$Q \equiv$ p-subgroup

$\exists\ g \in G$ s.t. $Q \leq gPg^{-1}$

→ if $Q \equiv$ Sylow-p → $Q = gPg^{-1}$

Sylow-p sub. conjugate to each other.

(iii) $n_p \equiv |Syl_p(G)|$ ← # of Syl p subgroups in G

$n_p = 1 \pmod p$.

& $n_p = [G : N_G(P)] \Rightarrow n_p \mid m$.

- $n_p = 1 \Rightarrow$ unique normal subgroup. $N \trianglelefteq G$

# Direct Products & Abelian Groups:

Prop. 2:- $G_1, G_2, \ldots G_n \equiv$ groups.

$G = G_1 \times G_2 \times \ldots \times G_n \equiv$ direct prod.

(1) ~~If~~, fix i → put 1 @ $j \neq i$

$G_i \simeq \{(1, 1, 1, \ldots 1, g_i, 1, \ldots, 1) \mid g_i \in G_i\}$

& $G_i \trianglelefteq G$ & $G/G_i \simeq G_1 \times \ldots \times G_{i-1} \times G_{i+1} \times \ldots G_n$

Scanned by CamScanner

② for each fixed $i$ define $\pi_i : G \to G_i$ by $\pi_i((g_1, g_2, \cdots g_n)) = g_i$

$\pi_i$ is a surjective homomorphism.

$\ker \pi_i = \{(g_1, \cdots, g_{i-1}, 1, g_{i+1} \cdots g_n) \mid g_j \in G \ \forall j \neq i\}$
$\simeq G_1 \times G_2 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n.$

③ under identificat$^n$s of part ①
$x \in G_i$ & $y \in G_j \Rightarrow xy = yx$.

---

# Elementary Abelian Group of order $p^n$:

$E_{p^n} = Z_p \times Z_p \times \cdots \times Z_p$ (n factors).

# of subgroups of order "p" in $E_{p^n}$

$$= \frac{p^n - 1}{p - 1}.$$

---

# Fundamental Thm. of Finitely Generated Abelian Groups:

① In terms of Elementary divisors

A = Finitely gen. Abelian group.

$$A \simeq \mathbb{Z}_{p_1^{a_1}} \oplus \mathbb{Z}_{p_2^{a_2}} \oplus \cdots \oplus \mathbb{Z}_{p_n^{a_n}}$$

$\{p_1^{a_1}, p_2^{a_2}, \ldots, p_n^{a_n}\}$ = elementary divisors.

② In terms of invariant factors

$$A \simeq \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_k}$$

$n_k \mid n_{k-1} \mid \cdots \mid n_2 \mid n_1$ $n_i$'s unique

$\{n_i\}$ = invariant factors.

useful result:

$m, n \in \mathbb{Z}^+$ s.t. $(m,n) = 1$

$\dashv$ $\mathbb{Z}_n \oplus \mathbb{Z}_m \cong \mathbb{Z}_{nm}$.

---

Ex.) Classify Abelian groups of order 200

$200 = 2^3 . 5^2$

$A \simeq P_2 \oplus P_5$ ← Sylow decomp.

$|P_2| = 2^3 = 8$ $|P_5| = 5^2 = 25$.

| $\pi(3) = 1,1,1;\ 1,2;\ 3$ | $\pi(2) = 1,1;\ 2$ |
|---|---|
| Possibilities for $P_2$ | Possibilities for $P_5$ |
| $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ | $\mathbb{Z}_5 \oplus \mathbb{Z}_5$ |
| $\mathbb{Z}_4 \oplus \mathbb{Z}_2$ | $\mathbb{Z}_{25}$ |
| $\mathbb{Z}_8$ | |

| Group | Elementary divisors |
|---|---|
| $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$ | 2, 2, 2, 5, 5. |
| $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{25}$ | 2, 2, 2, $5^2$ |
| $\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$ | $2^2$, 5, 5 |
| $\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{25}$ | $2^2$, 2, 25 |
| $\mathbb{Z}_8 \oplus \mathbb{Z}_{25}$ | $2^3$, 25 |

$\simeq \mathbb{Z}_{200}$ $\because$ $(8, 25) = 200$

---

Elementary divisor form to invariant factors form:-

Take e.g. $\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{25} = G$

elementary divisors = $\{2^2, 2, 5^2\}$

combine max powers of all primes.

$n_1 = 2^2 . 5^2 = 100$

$n_2 = 2$

$\Rightarrow \boxed{G \simeq \mathbb{Z}_{100} \times \mathbb{Z}_2}$

invariant factors form

# RING THEORY FACTOIDS:

**Defn:** ① $R \equiv$ ring → a set with 2 binary op. $+$ & $\times$ s.t. (i) $(R,+)$ is an Abelian group
(ii) $\times$ is associative: $(a\times b)\times c = a\times(b\times c)$
(iii) distributive laws hold in $R$ $\forall a,b,c \in R$
$(a+b)\times c = (a\times c)+(b\times c)$ & $a\times(b+c) = (a\times b)+(a\times c)$

② $R \equiv$ commutative ring if $a\times b = b\times a$ $\forall a,b \in R$

③ $R$ has identity if $\exists$ an element $1 \in R$ with $1\times a = a\times 1 = a$ $\forall a \in R$.

---

**Division Ring:** $R \equiv$ ring with $1 \neq 0$ if every nonzero $a \in R$ has mult inv., i.e, $\exists$ $b \in R$ s.t. $ab = ba = 1$.

---

A comm. division ring $\equiv$ field

- $a \in R$ is called zero divisor if $\exists$ $b \neq 0$ $(\in R)$ s.t. $ab = 0$
- $u \in R$ (with $1 \neq 0$) $\equiv$ unit if $\exists$ $v$ ($\neq 0$), s.t. $uv = 1$.
  Set of units $\equiv R^\times$

---

- a zero divisor cannot be a unit
  Pf:- $a \equiv$ unit in $R$ & let $ab = 0$ for some $b \neq 0$ then $va = 1$ for some $v \in R$.
  $b = 1b = (va)b = v0 = 0$ → contradiction
  Sim if $ba = 0$ for some $b \neq 0$ then $a$ cannot be unit.
  ∴ in particular → fields contain no zero divisors.

---

- Comm ring with id $1 \neq 0$ is called integral domain – (ID). if it has no zero divisors.

---

- Any finite ID is a field → proof? text.

---

*** Ring homomorphisms:** let $R, S \equiv$ rings.

(1) A ring homomorphism is a map $\varphi: R \to S$ s.t. (i) $\varphi(a+b) = \varphi(a)+\varphi(b)$ $\forall a,b \in R$
(ii) $\varphi(ab) = \varphi(a)\varphi(b)$ $\forall a,b \in R$

(2) $\ker\varphi = \{a \in R \mid \varphi(a) = 0_S\}$

(3) bij ring homom → isomorphism

---

**Prop #1:** (1) $\operatorname{im}\varphi \equiv$ subring of $S$
(2) $\ker\varphi \equiv$ ideal of $R$, i.e.
$\ker\varphi \equiv$ subring & if $\alpha \in \ker\varphi$, $r\alpha \in \ker\varphi$, $\alpha r \in \ker\varphi$

---

*** Ideals:-** $R \equiv$ ring $I \subset R$ & $I$ is additive subgroup of $R$. i.e. $(I,+) < (R,+)$

- $I$ → left ideal if $\forall x \in R$, $a \in I \Rightarrow xa \in I$
- $I$ → right –"– ——"—— –| $ax \in I$
- $I$ → two sided –"– if $I$ is left & right ideal

---

*** Quotient Rings:** $R \equiv$ ring $I \subset R$: 2-sided ideal

$R/I$ is a quotient group. To make it a ring, need closure under $\times$ as well.

$x+I$ → typical element of $I$

$(x+I)+(y+I) = (x+y)+I$ ✓ abelian group

define $(x+I)\times(y+I) = xy+I$

well defined? let $x+I = x'+I$, $y+I = y'+I$ } repr. by diff representatives.

need $xy+I = x'y'+I \Rightarrow xy - x'y' \in I$

$x+I = x'+I \Rightarrow x - x' \in I$
$y+I = y'+I \Rightarrow y - y' \in I$ } does this $\Rightarrow xy - x'y' \in$?

$$xy - x'y' = xy - x'y + x'y - x'y'$$
$$= \underbrace{(x-x')y}_{\in I} + \underbrace{x'(y-y')}_{\in I} \in I \checkmark$$

defn of "×" ok.

---

*** Isomorphism Theorems for Rings:**

① $\varphi: R \to S$ a ring homomorphism
then
- $\ker\varphi$ is an ideal of $R$
- $R/\ker\varphi \simeq \varphi(R)$ as rings.

② $R \equiv$ ring $S \subset R$, a subring, $I \equiv$ ideal of $R$

$$\begin{tikzcd}[row sep=small, column sep=small]
 & R \arrow[d, dash] & \\
 & S+I \arrow[dl, dash] \arrow[dr, equal] & \\
S \arrow[dr, equal] & & I \arrow[dl, dash] \\
 & S\cap I &
\end{tikzcd}$$

- $S\cap I$ is an ideal in $S$
- $I$ –"– —— in $S+I$
- $S+I/I \simeq S/S\cap I$ as rings

③ $R \equiv$ ring, $I, J \equiv$ ideals in $R$ s.t. $I \subseteq J$ then
- $J/I$ is an ideal of $R/I$
- $(R/I)/(J/I) \simeq R/J$ as rings

④ $I \equiv$ ideal of $R$, $A \equiv \{$set of subrings containing $I\}$
corr $A \leftrightarrow A/I$ inclusion preserving
$\{$Subrings of $R$ containing $I\}$ → $\{$subrings of $R/I\}$
- $A$ ideal of $R$ $\Leftrightarrow$ $A/I$ ideal of $R/I$.

Scanned by CamScanner

**Defn:-** let $I, J$ = ideals of $R$

- sum of $I$ & $J \to I+J = \{a+b \mid a \in I, b \in J\}$
- prod. of —"— $\to IJ = \{ab \mid a \in I, b \in J\}$
- $n^{th}$ power of $I \to I^n = \{\sum_{i=0}^{m} z \mid m < \infty, z = a_1 a_2 \ldots a_n$, $a_i \in I$, finite sums$\}$

**ex:** $R = \mathbb{Z}$, $I = 6\mathbb{Z}$, $J = 10\mathbb{Z}$.

- $I+J = \{6x + 10y \mid x, y \in \mathbb{Z}\} =$
  $\because 2 \mid 6x+10y \Rightarrow I+J \subseteq 2\mathbb{Z}$
  but $2 = 6(2) + 10(-1) \to 2\mathbb{Z} \subseteq I+J$ $\Big\} \; 6\mathbb{Z} + 10\mathbb{Z} = 2\mathbb{Z}$
  $6\mathbb{Z} + 10\mathbb{Z} = \gcd(6,10)\mathbb{Z}$
- $IJ = \{60xy \mid x, y \in \mathbb{Z}\} = 60\mathbb{Z}$
- $I \cap J = 6\mathbb{Z} \cap 10\mathbb{Z} = \text{lcm}(6,10)\mathbb{Z} = 30\mathbb{Z}$.

## * Properties of Ideals: $R$ = ring with $1 \neq 0$

**Defn:** • ideal gen. by $A = (A)$ = smallest ideal of $R$ containing $A$

- $RA$ = finite sums of elements of the form $ra$
  $RA = \{r_1 a_1 + r_2 a_2 + \ldots + r_n a_n \mid r_i \in R, a_i \in A, n \in \mathbb{Z}^+\}$
- $AR = \{a_1 r_1 + \ldots + a_n r_n \mid$ —"— $\}$
- $RAR = \{r_1 a_1 r_1' + \ldots + r_n a_n r_n' \mid r_i, r_i' \in R,$ —"— $\}$
- if $R$ = comm. $\Rightarrow RA = AR = RAR = (A)$
- Principal ideal: ideal gen. by a single element, i.e., if $A = \{a\} \Rightarrow (A) = (a)$

**Proposition.** $I$ = ideal of $R$

① $I = R \Leftrightarrow I$ contains a unit.

Pf: ($\Rightarrow$) obvious $\because 1 \in R, I = R \Rightarrow 1 \in I$.
($\Leftarrow$) $I$ has unit $u \Rightarrow uv = 1$ for some $v$
$r \in R$ s.t. $r \notin I \Rightarrow r = r \cdot 1 = r(vu) = (rv)\underbrace{u}_{\in I} \in I$
$\Rightarrow r \in I$ QED

② Assume $R$ = commutative.
then $R$ = field $\Leftrightarrow \{0\}, \{R\}$ are its only ideals.

$\to$ • $R$ = field $\Rightarrow$ every $r \neq 0 \in R$ is a unit.
By ①, $\{0\}, \{R\}$ only ideals
• if $\{0\}, \{R\}$ only ideals of $R$, let $u (\neq 0) \in R \Rightarrow (u) = R \Rightarrow 1 \in (u)$
$\Rightarrow \exists\, v \in (u)$ s.t. $vu = 1$
$\Rightarrow$ every $u \neq 0$ of $R$ is unit $\Rightarrow R$ field. ∎

• Maximal Ideal: $M$ is maximal ideal of $R$ if $M \neq R$ & only ideals containing $M$ are $M$ & $R$.

$\boxed{\text{\# Assume } R = \text{comm. Then ideal } M \text{ is maximal} \Leftrightarrow R/M \text{ is a field.}}$

Pf:- $M$ maximal $\Rightarrow$ ideals of $R$ containing $M$ = $M$ & $R$
Lattice iso. thm for rings $\Rightarrow$
$\left\{\begin{array}{l}\text{ideals of } R \text{ containing} \\ M, \text{ i.e., } M, R\end{array}\right\} \xleftrightarrow{\text{bijectn}} \{\text{ideals of } R/M\}$
$\{M, R\} \longleftrightarrow$ ideals of $R/M$
$\Rightarrow \{0\}, \{R/M\}$ only ideals of $R/M$.
By ② above, $R/M$ field. QED

• Prime Ideal: Assume $R$ = comm.
$P$ = prime ideal if $P \neq R$ & whenever for $a, b \in R$, if $ab \in P \Leftrightarrow a \in P$ or $b \in P$.
e.g. if $R = \mathbb{Z}$, prime ideals are $p\mathbb{Z}$ with $p$ = prime.

$\boxed{\text{\# Assume } R = \text{comm. Then } P \text{ is prime ideal in } R \Leftrightarrow R/P \text{ is an integral domain (ID)}}$

Pf: $ab \in P \Rightarrow a \in P$ or $b \in P$.
$\bar{r} = r + P \in R/P$ $\quad r \in P \Leftrightarrow \bar{r} = \bar{0}$ in $R/P$
$\Rightarrow$ in quotient $\to P$ = prime iff $\bar{R} \neq \bar{0}$
& if $ab \in P \Rightarrow \overline{ab} = \bar{0} \Rightarrow \bar{a} = \bar{0}$ or $\bar{b} = \bar{0}$
but that's the defn of ID. $\Rightarrow R/P$ ID.

## * Rings of Fractions: Idea: how one constructs $\mathbb{Q}$ from $\mathbb{Z}$.

$\frac{a}{b} \in \mathbb{Q}$, $a, b \in \mathbb{Z}, b \neq 0$; $\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc$

think:- $\mathbb{Q} = \{\frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0\}/\sim$
where $\frac{a}{b} \sim \frac{c}{d} \Leftrightarrow ad = bc$.

let $R$ = comm. ring. $D \subset R$ s.t.
① $0 \notin D$, ② $D$ has no zero divisors
③ $D$ closed under "$\times$"
fractns from $R$ = $\mathcal{F} = \{(a,b) \mid a \in R, b \in D\}/\sim$
where $(a,b) \sim (c,d)$ iff $ad = bc$

Scanned by CamScanner

# RING THEORY FACTOIDS: Cntd

## * Rings of fract$^{ns}$: cntd.

- $F = \{(a,b) \mid a \in R, b \in D\}/\sim$; where $(a,b)\sim(c,d)$ if $ad = bc$
- $Q$ = set of eq. classes of $\sim$
- NOTATION: $\frac{a}{b}$ for the eq. class of $(a,b)$.
- "+" & "×" on $Q$: $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ w $bd \in D$ ∵ $D$ closed "×"

"+" well def? → if $(a,b)\sim(a',b')$, $(c,d)\sim(c',d') \Leftrightarrow \frac{a'}{b'}+\frac{c'}{d'} = \frac{a}{b}+\frac{c}{d}$?

must p.t. $\frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'}$, i.e., $(ad+bc)(b'd') = (a'd'+b'c')(bd)$

lhs $= ab'dd' + cd'bb'$ … $R$ = comm.

but $\frac{a}{b} = \frac{a'}{b'}$ & $\frac{c}{d} = \frac{c'}{d'}$ ∵ $(a,b)\sim(a',b')$, $(c,d)\sim(c',d')$

⇒ $= a'bdd' + c'dbb'$ = rhs ⇒ "+" well-def.

"×": $\frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}$.

---

- $(Q,+)$ Abelian group. $(Q,+,\times)$ → comm. ring with id

where id $= \frac{d}{d}$ ∀ $d \in D$.

$\boxed{Q \equiv \text{ring of fract}^{ns}\text{ of } R \text{ by } D.}$

---

- If $R \equiv ID$ & $D = R - \{0\}$ → $Q$ is a field

$\frac{r}{d} \times (\#) = 1 \Rightarrow \# = \frac{d}{r}$ // QED

Field of fract$^{ns}$ or quotient field

---

## * The Chinese Remainder Theorem (CRT):

- To solve systems of simultaneous congruences.
- $R$ = comm ring with $1 \neq 0$; $A_1, A_2, \dots, A_n$ = ideals of $R$
- map $f: R \longrightarrow R/A_1 \times R/A_2 \times \dots \times R/A_n$

$r \longmapsto (r+A_1, r+A_2, \dots, r+A_n)$

$f$ = ring homomorphism

$\operatorname{Ker} f$: $A_1 \cap A_2 \cap \dots \cap A_n$

- In addit$^n$, if $\{A_i\}$'s pairwise comaximal, i.e., $(A_i + A_j = R \quad i \neq j)$ then $f$ is surjective

& $A_1 \cap A_2 \cap \dots \cap A_n = A_1 A_2 A_3 \cdots A_n$

1st iso. thm ⇒ $R/A_1A_2\cdots A_n \simeq R/A_1 \times R/A_2 \times \dots \times R/A_n$

## * Euclidean Domains (ED's):

$R$ = ring $N$ = norm ($N: R \to \mathbb{Z}^+ \cup \{0\}$, $N(0)=0$)

$a, b \in R$, $b \neq 0$ → $\exists\, q, r$ s.t.

$a = qb + r$ with $r = 0$ or $N(r) < N(b)$

---

$\boxed{\#\ \text{Every ideal in a ED is principal}}$

- if $I \neq \{0\}$ in the ED, $R$ then $I = (d)$ where $d \neq 0$ of $I$ of minimum norm.

Pf: if $d = 0$ nothing to prove. If $d \neq 0$ & $d$ has min norm in $I$ → ∵ $R$ is ED, for every $a \in I$

$a = qd + r$, $r = 0$ or $N(r) < N(d)$

$N(r) < N(d)$ → contradict$^n$ ∵ $N(d)$ = min

⇒ $N(r) = 0$ ⇒ $a = qd$ ⇒ $I = (d)$ QED

---

- Above can be used to p.t. some ID's are NOT ED's

---

- $R$ = ring $a, b \in R$ $d = \gcd(a,b)$ if

(i) $d|a$ & $d|b$ (ii) if $d'|a$ & $d'|b$ then $d'|d$

- If $I = (a,b)$ then $d = \gcd(a,b)$ if

(i) $I \subset (d)$ (ii) $(d')$ contains $I$, $(d) \subseteq (d')$

---

## * Principal Ideal Domains (PID's):

- PID ≡ an ID where every ideal is principal

$\boxed{\#\ \text{Every non-zero prime ideal in a PID is a maximal ideal}}$

Pf: let $(p)$ = prime ideal in a PID $R$. Let $I = (m)$ s.t. $(p) \subseteq I$. Must show $I = (p)$ or $I = R$.

∵ $p \in (m)$, $p = rm$ for some $r \in R$. ∵ $(p)$ = prime ideal $rm \in (p)$ ⇒ $r \in (p)$ or $m \in (p)$. If $m \in (p)$, then $(m) = (p) = I$. If $r \in (p)$, write $r = ps$. Here, $p = rm = psm$ ⇒ $sm = 1$ & $m$ = unit ⇒ $I = R$ ∎

---

$\boxed{\#\ R = \text{any comm. ring s.t. } R[x] = PID \Rightarrow R \text{ is necessarily a field}}$

Pf:- $R[x]$ = PID ∵ $R \subseteq R[x]$ a subring → $R$ = ID ($R[x]$ has 1 ⇔ $R$ has 1) ∵ $R[x]/(x) \simeq R$

& $R$ = ID ⇒ $(x)$ = prime ideal in $R[x]$

By previous prop. ∵ $R[x]$ = PID prime ideal is maximal

⇒ $(x)$ = maximal iff $R[x]/(x)$ is field

⇒ $R$ is a field QED.

Scanned by CamScanner

## * Unique Factorizatⁿ Domains (UFDs):

Defⁿ: let $R$ = ID.

(1) $r \in R$, $r \neq 0$, $r$ not a unit. $r$ is irreducible in $R$ if whenever $r = ab$ with $a, b \in R$, at least one of $a$ or $b$ must be a unit in $R$. Otw $r$ is reducible.

(2) $p \neq 0$, $p \in R$ = prime if $(p)$ is a prime ideal in $R$.

(3) associates: $a, b$ associates if $a = ub$, $u$ = unit.

# In an ID a prime element is always irreducible

Pf:- $(p)$ = prime ideal & $p \in (p) \Rightarrow$ if $p = ab$, $a \in (p)$ or $b \in (p)$. Let $a = pr$ for some $r \in R$. $\Rightarrow p = ab = prb \Rightarrow rb = 1 \Rightarrow b$ = unit. $\Rightarrow p$ is irreducible. QED.

# In a PID $p$ is prime $\Leftrightarrow$ $p$ is irreducible

Pf:. prime $\Rightarrow$ irred. as above. ($\Leftarrow$) Let $p$ be irred. Must show $(p)$ is a prime ideal if $p$ is irred. If $(p) \subseteq M$ ~ some ideal; since we're in PID, $M = (m)$. $\Rightarrow (p) \subseteq (m)$ $\because p \in (m)$, $p = rm$ for some $r$. But $p$ = irred. $\Rightarrow r$ is unit or $m$ is unit. $m$ unit $\Rightarrow (m) = (1) = R \Rightarrow (p)$ maximal. But in PID maximal $\Leftrightarrow$ prime $\Rightarrow (p)$ prime ✓. If $r$ unit, then $(p) = (m)$. $\Rightarrow$ only ideals containing $(p)$ are $(1)$ & $(p)$. $\Rightarrow (p)$ is prime ✓.

- UFD is an ID $R$ in which $r \neq 0$, unit has 2 prop
  - (i) $r = p_1 p_2 \cdots p_n$ where $p_i$'s = irreducibles.
  - (ii) (i) is unique up to associates.

# In a UFD, $p \neq 0$ is prime $\Leftrightarrow$ $p$ is irred.

($\Rightarrow$) proved. ($\Leftarrow$) let $p$ = irred. let $p \mid ab$. Must show $p \mid a$ or $p \mid b$. Since it's a UFD $\rightarrow a = p_1 p_2 \cdots p_n$, $b = q_1 q_2 \cdots q_n$. $p \mid ab \Rightarrow ab = pc$ $\Rightarrow p \sim$ one of $p_i$'s or $q_i$'s. let $p_1 = up$. w/o loss of generality. $p_i$'s, $q_i$'s irred.

$\Rightarrow a = (up) p_2 \cdots p_n \Rightarrow \underbrace{a = pd}_{\Downarrow\ p \mid a}$ where $d = u p_2 \cdots p_n$

QED.

# $a, b \in$ UFD $a = u p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}$ $b = v p_1^{f_1} p_2^{f_2} \cdots p_n^{f_n}$

$u, v$ = units; $p_i$'s distinct; $e_i, f_i \geq 0$

$d = p_1^{\min(e_1, f_1)} \cdots p_n^{\min(e_n, f_n)}$ = gcd$(a,b)$ in the UFD.

# Every PID is a UFD. In part, every ED is UFD

Pf. text.

# $\mathbb{Z}$ is a UFD

## * Factorizatⁿ in the Gaussian Integers:

Gaussian int. = $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$.

$\alpha = a + bi \Rightarrow N(\alpha) = a^2 + b^2$; $N$·

if $\alpha = \beta\gamma$ $N(\alpha) = N(\beta)N(\gamma)$ under this norm

$u$ = unit $\Leftrightarrow N(u) = \pm 1 \Rightarrow$ units in $\mathbb{Z}[i] = \{\pm 1, \pm i\}$.

# The prime $p \in \mathbb{Z}$ divides an int. of form $n^2 + 1 \Leftrightarrow p = 2$ or $p \equiv 1 \pmod 4$

Pf:- text.

# Fermat's Thm. on Sums of Squares:

(1) $p$ = prime $\in \mathbb{Z}$ $p = a^2 + b^2$, $a, b \in \mathbb{Z}$

$\Leftrightarrow p = 2$ or $p \equiv 1 \pmod 4$

(except interchanging $a, b$ or changing signs, representatⁿ of $p$ is unique)

(2) Irreducibles in $\mathbb{Z}[i]$

(a) $(1+i)$ (with norm 2).

(b) the primes $p \equiv 3 \pmod 4$ ... norm$(p) = p^2$

(c) $a+bi$, $a-bi$ → distinct irred. factors of $p = a^2 + b^2 = (a+bi)(a-bi)$ for $p \in \mathbb{Z}$ with $p \equiv 1 \pmod 4$ (both $N(a \pm bi) = p$).

# Let $n \in \mathbb{Z}^+$ & $n = 2^k p_1^{a_1} \cdots p_r^{a_r} q_1^{b_1} q_2^{b_2} \cdots q_s^{b_s}$

$p_i$'s = distinct primes $\equiv 1 \pmod 4$

$q_i$'s = — " — $\equiv 3 \pmod 4$

then $n$ can be expressed as $n = A^2 + B^2$, $A, B \in \mathbb{Z}$ $\Leftrightarrow$ each $b_i$ is even.

Further, if all $b_i$'s even,

# of repres. of $n$ as sum of 2 squares $= 4(a_1+1)(a_2+1)\cdots(a_r+1)$.

$\boxed{\text{Fields} \subset \text{EDs} \subset \text{PIDs} \subset \text{UFDs} \subset \text{IDs}}$

## * Polynomial Rings: Gauss's lemma, Eisenstein, etc.

: text