GROUPS

for $(G, \times) \to$ group law is map $G \times G \to G$ s.t. $(g,h) \mapsto g \times h$.

- $f: G \to H$ homomorphism if $\forall a,b \in G$ $f(ab) = f(a) \cdot f(b)$
  $\hookrightarrow$ $f(e_G) = e_H$ and $f(g)^{-1} = f(g^{-1})$.

- f ISOMORPHISM if homomorphism + bijection.
  (isomorphic groups indistinguishable) e.g. $\mathbb{Z}/n\mathbb{Z} \cong C_n$.
  (recall: $C_n = \{a^0, a^1, \dots, a^{n-1}\}$)

- isomorphism $f: G \to G$ is AUTOMORPHISM.
  $\hookrightarrow$ $\mathrm{Aut}(G)$ = group of all automorphisms of G.

e.g. $\mathrm{Aut}(\mathbb{Z}) \to$ isomorphism must map generator to generator.
$\hookrightarrow$ $f(n) = n \cdot f(1)$. If $f(1) = m$, then $f(n) = n \cdot f(1) = nm$
$\Rightarrow \mathrm{Im}(f) = m\mathbb{Z}$ so for f to be surjection $m = 1$ or -1.
$\Rightarrow f(n) = n$ or $f(n) = -n$ so $|\mathrm{Aut}(\mathbb{Z})| = 2$.

- $f: G \to G$ CONJUGATION by g if $x \mapsto gxg^{-1}$. $\in \mathrm{Aut}(G)$

N/B: f INJECTIVE iff $\mathrm{Ker}(f) = \{e_G\}$.

$\mathrm{Im}(f)$ and $\mathrm{Ker}(f)$ (normal) subgroups of H and G for $f: G \to H$.

- subgroup $S \subset G$ is NORMAL if all $s \in S$ stable under conjugation by any element of G. $\Rightarrow$ if $s \in S$, then $gsg^{-1} \in S$ $\forall g \in G$.

- G SIMPLE if only normal subgroups are G and $\{e\}$.

- for subgroup $H \subset G$, if cosets: $gH = Hg$ $\forall g \in G$, then H is normal subgroup of G.

- if N normal subgroup of G then G/N is quotient group of G modulo N.

for N normal subgroup of G, $f: G \to G/N$ given by $g \mapsto g \cdot N$ is surjective homomorphism with $\underline{\text{Ker}(f) = N}$.

<u>ISOMORPHISM THM</u>: $f: G \to H$ be homomorphism. Then, the map $g \cdot \text{Ker}(f) \mapsto f(g)$ is isomorphism; $G/\text{Ker}(f) \cong f(G)$

$\text{Im}(f)$

↳ check homomorphism; clearly surjective; show kernel is just trivial coset $= \text{Ker}(f)$.

<u>NOTE</u>: Image of group <u>NOT</u> normal subgroup. <u>BUT</u> for a surjective homomorphism, image of a <u>normal subgroup</u> is <u>normal</u>.

↳ if $N \trianglelefteq G$ and $f: G \to G/N$ s.t. $g \mapsto gN$ (and f surjective) and $S \subset G$ subgroup containing N, then N also a normal subgroup of S and $f(S) = S/N$ subgroup of G/N.

<u>CENTRE</u>: $Z(G) = \{g \in G : gx = xg \ \forall x \in G\}$ i.e. set of elements of G that commute with everything in G.

- <u>$\text{Inn}(G)$</u> $\to$ group of inner automorphisms of G form subgroup of $\text{Aut}(G)$ and they are <u>set of conjugations</u> by all elements of G.

  NOTE: $\underline{G/Z(G) \cong \text{Inn}(G)}$ by isomorphism thm.

<u>COMMUTATOR</u>: $[a,b] = aba^{-1}b^{-1}$, and $[G,G]$ is smallest subgroup of G containing all possible commutators, $[a,b] \ \forall a,b \in G$.

$[G,G]$ is normal subgroup of G and $G/[G,G]$ abelian.

↳ if $G/[G,G]$ abelian $\forall x,y \in G$, $x[G,G] \cdot y[G,G] = \underline{xy[G,G] = yx[G,G]}$
$\Leftrightarrow x^{-1}y^{-1}xy \in [G,G]$.

for $N \trianglelefteq G$, G/N abelian <u>iff</u> N contains $[G,G]$.

↳ a group abelian if its commutator is $\{e_G\}$. For G/N, group abelian iff $[a,b] \in N$ for any $a,b \in G$.
$\Rightarrow [G,G] \subset N$. $\square$

- for $a, b \in G$, order of ab divides $\text{lcm}(n, m)$ where n is order of a and m is order of b.

- G_{tors} = <u>TORSION SUBGROUP</u> of G = set of elements of G of finite order. (NOTE: G abelian)

($\hookrightarrow$ if $G = G_{tors}$ then G is torsion abelian group.)

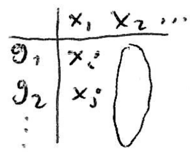
- For <u>prime p</u>, set of elements $g \in G$ of order p^k for $k \in \mathbb{N}$ forms the <u>p-primary subgroup</u> of G, <u>$G\{p\}$</u>.

$$\boxed{\begin{array}{l}\text{For } n = p_1^{\alpha_1} \cdots p_m^{\alpha_m} \ (p_1, \dots, p_m \text{ prime}), \text{ then;} \\ \qquad C_n \cong C_{p_1^{\alpha_1}} \times \dots \times C_{p_m^{\alpha_m}}\end{array}}$$

- for group G and set $S \subset G$, intersection of all subgroups of G containing S is <u>SUBGROUP of G GENERATED by S</u>, and if G is only subgroup of G containing S, then "elements of S generate G".

<u>GROUP ACTION</u>: let G be group, X be set. $S(X)$ is group of bijections (permutations) $X \to X$. An <u>action of G on X</u> is homomorphism <u>$G \to S(X)$</u>.

$\hookrightarrow$ (or $G \times X \to X$, $(g, x) \mapsto g \cdot (x)$).

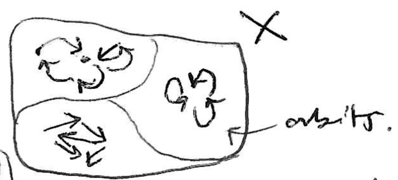


- group action <u>FAITHFUL</u> if it is <u>injective</u>.

<u>ORBIT</u>: $G(x) = \{g(x) : g \in G\} \subset X$ (call $g \in G$ acting on x)
("image")

<u>STABILISER</u>: $St_G(x) = \{g \in G : g \cdot (x) = x\} \underset{\text{(subgroup)}}{\leq} G$
("kernel")

$\boxed{X \text{ is a } \underline{\text{disjoint}} \text{ union of } G\text{-orbits}}$



$\boxed{\text{for action } G \times X \to X, \ \boxed{St(g(x)) = g \cdot St(x) \cdot g^{-1}}}$ $\to$ so St normal in G.

if $h(x) = x$ ($n \in h$), then $(ghg^{-1})\, g(x) = (ghg^{-1}g)(x) = (gh)(x)$
$= g(h(x)) = g(x)$

$\Rightarrow g St(x) g^{-1} \subset St(g(x))$ etc.

ORBIT-STABILISER THM: for an action $G \times X \to X$, for any $x \in X$, map $g \cdot St(x) \mapsto g \cdot (x)$ gives bijection $G/St(x) \to G(x)$ and $|G(x)| = |G| / |St(x)|$.

orbit of x

CAYLEY'S THM: G a finite group of order n. then, S_n contains a subgroup isomorphic to G.

↳ action of G on itself $G \times G \to G$ by $(a,b) \mapsto ab$. injective since $ge = e \Rightarrow g = e$. And $G \to S(G)$, image is subgroup of S_n so it isomorphic to $G/St(g) = G/\{e\} = G$. □

CAUCHY'S THM: G a finite group of order n and p is a prime factor of n. Then G contains an element of order p.

- if X can be represented by just one G-orbit, i.e. $X = G(x)$ for some $x \in X$, then G acts TRANSITIVELY on X.
- FIXED POINT: $x \in X$ is fixed point of $g \in G$ if $g(x) = x$.
  ↳ $Fix(g) \subset X$ = all points in X which are "fixed" under g.

JORDAN'S THM: let $G \times X \to X$ act transitively on X, and G and X finite, then $\sum_{g \in G} |Fix(g)| = |G|$

↳ AND $\exists g \in G$ s.t. $Fix(g) = \emptyset$

↳ coroll: for $G \times X \to X$, the number of G-orbits in X is $|G|^{-1} \cdot \sum_{g \in G} |Fix(g)|$

$\Rightarrow X = \bigcup_{i=1}^{n} X_i$ then the number of fixed points of $g \in G$ in X is the sum of the number of fixed points of g in X_i.
then applying Jordan's thm for each orbit, the above formula gives 1 each time $\Rightarrow$ summing to n.

FREE ABELIAN GROUP of RANK n : $\mathbb{Z}^n = \{(a_1, \dots, a_n) : a_i \in \mathbb{Z}\}$

← n copies of $\mathbb{Z}$.

(addition = group law) ← (finitely generated abelian groups).

If $\mathbb{Z}^n \cong \mathbb{Z}^m \Rightarrow n = m$, ($\Rightarrow$ well-defined).

$\boxed{\text{• any subgroup of } \mathbb{Z}^n \text{ is isomorphic to } \mathbb{Z}^m \text{ for some } m \leq n.}$

N/B: all subgroups of abelian groups are normal.

$\boxed{\text{Every finitely generated abelian group isomorphic to product of finitely many cyclic groups.}}$

↳ Any finite generated abelian group isomorphic to a product of its p-primary torsion subgroups. → set of elements of G of order power of p.

(use: $C_n \cong C_{p_1^{a_1}} \times \dots \times C_{p_m^{a_m}}$ where $n = p_1^{a_1} \cdot \dots \cdot p_m^{a_m}$)

RINGS

- set R with $+$ and $\times$ s.t.; $(R, +)$ is abelian group.
- $(ab)c = a(bc)$ $\forall a,b,c \in R$ (multiplication ASSOCIATIVE).
- Multiplicative identity $= 1$ exists $(x \cdot 1 = 1 \cdot x = x)$
- Distributivity: $a(b+c) = ab + ac$ and $(a+b)c = ac + bc$ $\forall a,b,c \in R$.

SUBRING TEST: $S \subseteq R$ s.t. $1 \in S$, $\forall a, b \in S$, $a+b \in S$ and $ab \in S$ and $-a \in S$.

DIVISION RING $\rightarrow$ every non-zero element is invertible.

FIELD: commutative division ring.

HOMOMORPHISM: $f: R \rightarrow S$ if, $f: (R, +) \rightarrow (S, +)$ hom. of abelian groups.

$f(xy) = f(x) \cdot f(y)$, $f(1_R) = 1_S$.

KERNEL: $\mathrm{Ker}(f)$ is subgroup of $(R, +)$ s.t. $\forall x \in \mathrm{Ker}(f)$ and all $r \in R$, then $xr \in \mathrm{Ker}(f)$, $rx \in \mathrm{Ker}(f)$.

IDEAL: $I \subset R$ if subgroup of $(R, +)$ and $\forall x \in I$, $r \in R$, $rx \in I$ and $xr \in I$.

QUOTIENT RING: $I \subset R$ proper ideal, then $R/I = \{r + I : r \in R\}$

PRINCIPAL IDEAL: for $a \in R$, the set $aR = \{ax : x \in R\}$. (generator a).

$$\boxed{\text{ISOMORPHISM THM: } f: R \rightarrow S, \text{ then } \underbrace{R/\mathrm{Ker}(f) \cong f(R)} \subset S}$$

$\hookrightarrow$ $x + \mathrm{Ker}(f) \mapsto f(x)$ is isomorphism of groups under $+$. The map respects multiplication and sends 1 to 1 $\Rightarrow$ ring hom.

ZERO DIVISORS: if $a, b \in R$ non-zero and $ab = 0$ then a, b zero divisors.

$$\boxed{\begin{array}{l}\text{INTEGRAL DOMAIN: commutative ring without zero-divisors.} \\ \text{i.e. } ab = 0 \Rightarrow a = 0 \text{ or } b = 0.\end{array}}$$

$\boxed{aR = bR \iff a = br \text{ where } r \in R^\times \text{ (unit.)}}$

↳ if $a = 0$ clear so $a \neq 0$. $a = a \cdot 1 \in aR = bR$
$\Rightarrow a = bc$ for $c \in R$, also $b = ad$ for $d \in R$
$\Rightarrow a = acd \Rightarrow cd = 1 \Rightarrow c \in R^\times$.

$\boxed{\text{Every field is an integral domain.}}$

$\boxed{\text{Every finite integral domain is a field.}}$

↳ let $R = \{r_1, \dots, r_n\}$, take $r \in R$ and consider
$\{r_1 \cdot r, \dots, r_n \cdot r\}$. If $r_i \cdot r = r_j \cdot r \Rightarrow r_i = r_j$
$\Rightarrow \{r_1 r, \dots, r_n r\}$ distinct so $\{r_1 r, \dots, r_n r\} = R = \{r_1, \dots, r_n\}$
$\Rightarrow$ any $r_i = r_j r$, specifically $1 = r_j r \Rightarrow r_j = r^{-1}$. □

- $\mathbb{F}_p$ denoted by $\mathbb{Z}/p\mathbb{Z}$.

$\boxed{\begin{array}{l} K \subseteq F \text{ is \underline{subfield} of } F \text{ if } K \text{ is field with same } + \text{ and } \times \\ \hookrightarrow F \text{ is \underline{FIELD EXTENSION} of } K. \end{array}}$

$\boxed{\text{for any ring } R, \exists \text{ unique homomorphism } \mathbb{Z} \to R.}$

↳ if R integral domain, kernel of this hom. is either $\{0\}$ zero ideal or principal ideal $p\mathbb{Z}$ for prime p.

- N/B: the zero ideal $\{0\}$ of R is <u>PRIME</u>.

<u>CHARACTERISTIC</u>: of an int. dom. is non-negative unique generator of the kernel of a hom. $\mathbb{Z} \to R$ so it's 0 or prime #.

$\boxed{\text{A field extension } F \text{ of field } K \text{ is a vector space over } K.}$

~~For field K with char$(K) = 0$, then $\exists$ unique subfield of~~

For field k, with $char(k) = 0$, k contains a unique subfield isomorphic to $\mathbb{Q}$ $\Rightarrow$ k vector space over $\mathbb{Q}$.

if $char(k) = p$ prime, then k contains unique subfield isomorphic to $\mathbb{F}_p$ $\Rightarrow$ k vector space over $\mathbb{F}_p$.

- every finite field has p^n elements.

commutative ring is field iff any proper ideal is $\{0\}$.

$f: R \to S$ hom. and let $J \subset S$ be ideal. Then $f^{-1}(J)$ ideal.

↳ note → $f^{-1}(J)$ subgroup of $(R, +)$. (inverse image of subgroup is subgroup).

PRIME IDEAL: proper ideal $I \subset R$ of commutative ring s.t. R/I is integral domain.

↳ $I \subset R$ prime iff $\forall x, y \in R$ s.t. $xy \in I \Rightarrow x \in I$ or $y \in I$.

MAXIMAL IDEAL: proper ideal $I \subset R$ of commutative ring s.t. R/I is a field. all maximal ideals prime.

↳ $I \subset R$ maximal iff $\forall J$ with $I \subseteq J$, then $J = I$ or $J = R$.

- in integral domain, $\deg(p(t) \cdot q(t)) = \deg(p(t)) + \deg(q(t))$.

For field k, $a(t), b(t) \in k[t]$ then:

$a(t) = b(t) \cdot q(t) + r(t)$ $\quad (\deg(r) < \deg(b)$ or $r = 0)$

EUCLIDEAN DOMAIN: integral domain R with $\phi: R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ s.t. $\phi(xy) \geq \phi(x)$ $\forall x, y \in R \setminus \{0\}$.

$\forall a, b \in R$, $\exists q, r \in R$ s.t. $a = qb + r$ $\quad (r = 0$ or $\phi(r) < \phi(b))$

e.g. $\mathbb{Z}$ w/ $\phi(n) = |n|$ or $k[t]$ with degree.

PRINCIPAL IDEAL DOMAIN : integral domain where every ideal principal.

$\boxed{\text{Every Euclidean Domain is a PID.}}$

IRREDUCIBLE : integral domain R, let non-zero $x \in R \setminus R^\times$

is irreducible if x NOT a product of 2 elements of $R \setminus R^\times$.

↳ irreducibles non-invertible.

if x irred and $a \in R^\times \Rightarrow ax$ also irred.

UNIQUE FACTORISATION DOMAIN: integral domain where every element of $R \setminus R^\times$ can be written as product of finitely many irreducibles (up to reordering and multiplying by $R^\times$).

for $a, b \in R$ integral domain and $r \in R^\times$ then if;

$b = ra \Rightarrow a$ and b are ASSOCIATES.

e.g. NON-UFD $\rightarrow R = \{a_0 + a_1 x + \dots + a_n x^n \mid a_0 \in \mathbb{Z}, a_i \in \mathbb{Q}\}$.

UFD but NOT PID $\rightarrow k[x, y]$ - polynomial ring in x AND y, with coeffs in field k.

↳ or $\mathbb{Z}[x]$

$\boxed{\text{Every PID is a UFD.}}$

$\boxed{\text{for PID } R, \ aR \text{ maximal iff } a \text{ irreducible.}}$

$\boxed{\text{if } R \text{ PID, } a \in R \text{ irreducible, THEN } R/aR \text{ field.}}$

let k be field s.t. $\text{char}(k) = p$, $\Rightarrow \forall x, y \in k$,

$$(x + y)^{p^m} = x^{p^m} + y^{p^m}.$$

$\boxed{R[x] \text{ poly ring is PID iff } R \text{ is field.}}$

↳ if f unit, then $\exists g \in R[x]$ s.t. $1 = g \cdot f \in (f) = fR[x]$

$\Rightarrow 1 \in (f) \Rightarrow (f) = (1)$ or $fR[x] = R[x]$.