

Group Set G and binary operation \cdot .

- Closure $a \cdot b \in G$
- Associativity $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- Identity $e \cdot a = a \cdot e = a$
- Inverse $a \cdot a^{-1} = a^{-1} \cdot a = e$

Identity is unique

Order $|x| = \min k$ s.t. $(x^k = e)$

Direct product Set: $A \times B$ Operation: $(a_1, b_1)(a_2, b_2) = (a_1a_2, b_1b_2)$

Subgroup $H \leq G$, $hk \in H$ and $h^{-1} \in H$

Normal $H \trianglelefteq G$, if $gHg^{-1} = H$ for all $g \in G$

Coset left: gH right: Hg with representative g

Congruate of $n \in N$ by g . $gn g^{-1}$

Abelian Group $a \cdot b = b \cdot a$

Cyclic Group is generated by a single element

Homomorphism $\varphi: G \rightarrow H$ such that $\varphi(xy) = \varphi(x)\varphi(y)$

- Kernel: $\varphi^{-1}(e_H)$
- Isomorphism $G \cong H$, a bijective homomorphism
- Automorphism: an isomorphism from $G \rightarrow G$

Mod $G/H := \{\sigma H \mid \sigma \in G\}$, set of equivalence classes of G under the equivalence relation defined by φ . Is a group iff H is normal

Field $(F, +)$ and $(F - \{0\}, \cdot)$ are abelian groups and

- $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$

Group Action on set A is map $G \times A \rightarrow A$

- $g_1 \cdot (g_2 \cdot a) = (g_1g_2) \cdot a$
- $1 \cdot a = a$

Stabilizer G acts on $A, \{g \in G \mid ga = a\}$

Examples of Groups:

- Symmetric $S_n = \zeta_n$ bijections of $\{1, 2, \dots, n\}$
- Dihedral D_{2n}
- Quaterion Q_8
- General Linear Group of degree n $GL_n(F)$, $\{A \mid A \text{ is an } n \times n \text{ matrix whose entries come from } F \text{ and}$
- Integers Modulo n $\mathbb{Z}/n\mathbb{Z}$
- Special Unitary Group $SU(1, 1) = \left\{ \begin{pmatrix} \alpha & \beta \\ \bar{\beta} & \bar{\alpha} \end{pmatrix} \mid \alpha, \beta \in \mathbb{C}, |\alpha|^2 - |\beta|^2 = 1 \right\}$
- Projective Special Unitary Group $PSU(1, 1) = SU(1, 1) / \left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$

Ring a set with binary operations $+$, \times

- $(R, +)$ is an abelian group
- \times is associative: $(a \times b) \times c = a \times (b \times c)$
- distribution of multiplication over addition:
 - $(a + b) \times c = (a \times c) + (b \times c)$
 - $a \times (b + c) = (a \times b) + (a \times c)$
- usually, contains identity: $1 \times a = a \times 1 = a$ for all $a \in R$
- called commutative if multiplication commutes
- If $R/\{0\}$ is a group under \times , R is a field

Subring a subgroup closed under multiplication

Ideal $I \trianglelefteq R$

- I is an abelian subgroup of R under addition
- $r \times a \in I$ for all $r \in R$ and $a \in I$
- every ideal is the kernel of a homomorphism

1st isomorphism thm

Quotient Ring $R/I = \{r + I | r \in R\}$ equivalence classes

Prime Ideal whenever $ab \in P$ either $a \in P$ or $b \in P$

- P is prime iff R/P is an integral domain

Prime Element $p|ab \rightarrow p|a$ or $p|b$ also $ab \in (p) \rightarrow a \in (p)$ or $b \in (p)$

Irreducible Element $p = ab \rightarrow a$ is a unit or b is a unit

Zero divisor a is a zero divisor if there exists a nonzero b such that $ab = 0$

Integral Domain a commutative ring with no zero divisors

Maximal Ideal $M \trianglelefteq R$ is maximal whenever $I \trianglelefteq R$ and $I \supseteq M$ then $I = M$ or $I = R$

- M is maximal iff R/M is a field

Field has multiplicative inverses: for any $a \neq 0$, $\exists b \in R$ s.t. $ab = ba = 1$

Norm function $N : R \rightarrow \mathbb{Z}_{\geq 0}$ and $N(0) = 0$

Euclidean Domain a ring where the division algorithm holds

- given $a, b \in R$, $b \neq 0$ then $\exists q, r \in R$ s.t. $a = bq + r$ where $N(r) < N(b)$

Principil Ideal Domain every ideal $I \trianglelefteq R$ is principle, ie $\exists a \in R$ s.t. $I = (a)$

Unit u is a unit if $\exists v \in R$ s.t. $uv = vu = 1$

Module if R a ring and M a set, M is a left R-module if

1. $(M, +)$ is an abelian group
2. Scalar multiplication $\cdot : R \times M \rightarrow M$, for all $r, s \in R$, $n, m \in M$
 - (a) $(r + s)m = rm + sm$
 - (b) $(rs)m = r(sm)$
 - (c) $r(m + n) = rm + rn$
 - (d) $1m = m$ if $1 \in R$

Submodule $N \subseteq M$ a submodule if N a subgroup and closed under multiplication

Classes Commutative rings \supset integral domains \supset integrally closed domains \supset unique factorization domains \supset principal ideal domains \supset Euclidean domains \supset fields