Group Theory

Definitions

- [Equivalence Relation] An equivalence relation $\sim$ on X satisfies:
  - Reflexivity: $x \sim x$
  - Symmetry: $x \sim y \Rightarrow y \sim x$
  - Transitivity: $x \sim y, y \sim z \Rightarrow x \sim z$
- [Group] A group G is a set with a binary operation $\cdot: G \times G \to G$ which obeys:
  - Associativity: $\forall g_1, g_2, g_3 \in G$, $g_1(g_2g_3) = (g_1g_2)g_3$
  - Identity: $\exists e \in G$ s.t. $ge = g = g$
  - Inverse: $\forall g \in G$, $\exists g^{-1} \in G$ s.t. $gg^{-1} = g^{-1}g = e$.
- [Subgroup] Say H is a subgroup of G if $H \subseteq G$ and H is a group given the operation inherited from G. Notation: $H \leq G$.
- [Cyclic Group] Say a group G is cyclic if it is generated by a single element $g \in G$ i.e. $G = \langle g \rangle$.
- [Subgroup Generated by S] Let $S \subset G$. Then the subgroup generated by S, denoted as $\langle S \rangle$, is the intersection of all subgroups H containing S i.e. $\langle S \rangle = \bigcap_{\substack{H \leq G \\ S \subset H}} H$.
- [Centralizer] Let G be a group and $a \in G$. The centralizer of a in G is the set of all elements in G that commutes with a i.e. $C(a) = \{g \in G | ag = ga\}$. It is a subgroup of G.
- [Center] Let G be a group. Then the center of G is the set of elements that commutes with all element in G i.e. $Z(G) = \{z \in G | zg = gz\ \forall g \in G\}$. It is a subgroup of G.
- [Left Coset] Let $H \leq G$, then a left coset of H is $gH = \{gh | h \in H\}$ where $g \in G$. The set of left cosets of H in G is $S = \{gH | g \in G\}$
- [Right Coset] Let $H \leq G$, then a right coset of H is $Hg = \{hg | h \in H\}$ where $g \in G$. The set of right cosets of H in G is $S = \{Hg | g \in G\}$
- [Set of Cosets] Denote by G/H the set of cosets of H in G.
- [Index] The index of H in G is $|G/H|$.
- [Representative of Coset] Any element of gH is a representative of coset gH. If g_1 and g_2 are representatives of the same coset, then $g_1H = g_2H$.
- [Simple] Say a group G is simple if it is a non-trivial group and its normal subgroups are only $\{e\}$ and G itself.
- [Normal] Say a subgroup N of G is a normal subgroup of G if $\forall g \in G$, $\forall n \in N$, $gng^{-1} \in N$.
  - N is a normal subgroup of G if and only if $gNg^{-1} = N\ \forall g \in G$.
  - N is a normal subgroup of G if and only if $\forall g \in G, n \in N$, $gng^{-1} \in N$
  - N is a normal subgroup of G if and only if $gNg^{-1} \subseteq N\ \forall g \in G$.
  - N is a normal subgroup of G if and only if $\forall g \in G$, $gN = Ng$.
  - N is a normal subgroup of G if and only if the product of any two right cosets of N is still a right coset of N, specifically $(Nx)(Ny) = Nxy$.
- [Homomorphism] Let G, H be groups. A function $\phi: G \to H$ is a homomorphism if $\forall g_1, g_2 \in G$, $\phi(g_1g_2) = \phi(g_1)\phi(g_2)$
- [Isomorphism] Say a homomorphism $\phi: G \to H$ is an isomorphism if ϕ is both injective and surjective.
- [Automorphism] An automorphism is an isomorphism of G onto itself.
- [Commutator] If $g, h \in G$, the commutator of g and h is $[g, h] = ghg^{-1}h^{-1} \in G$. If g, h commutes, $[g, h] = e$.
- [Commutator Subgroups] The commutator subgroup of G is $[G, G] = \langle [g, h] | g, h \in G \rangle$ i.e. the subgroup generated by all the commutators in G.
- [Endomorphism] An endomorphism is a homomorphism from an object to itself. The set of endomorphisms of M is denoted as $\mathrm{End}(M) = \{\phi: M \to M\}$ where ϕ is a group homomorphism.

Properties

- $(\mathbb{Z}/n\mathbb{Z}, +)$ is a cyclic group $\forall n$

- If $\{H_i\}_i$ is a collection of subgroups of G, then the intersection $\bigcap_i H_i$ is also a subgroup of G
- Function composition is associative.
- All cyclic groups are either $\mathbb{Z}$ or $\mathbb{Z}/m\mathbb{Z}$ with addition for some $m \in \mathbb{Z}$.
- [Properties of Group Homomorphism] Let $\phi: G \to H$ be a homomorphism:
  - $\phi(e_G) = e_H$
  - $\phi(g^{-1}) = \phi(g)^{-1}$
  - $\text{image}(\phi) \leq H$
  - $\ker \phi$ is a normal subgroup in G
- Group isomorphism is an equivalence relation i.e.:
  - $G \approx G$
  - $G \approx H \Rightarrow H \approx G$
  - $G_1 \approx G_2, G_2 \approx G_3 \Rightarrow G_1 \approx G_3$
- Let $\mathcal{g}(G)$ denote the group of inner automorphisms of G, then $\mathcal{g}(G) \approx G/Z_G$.
- Let ϕ be an automorphism of group G. If $a \in G$ s.t. $o(a) > 0$, then $o\big(\phi(a)\big) = o(a)$.
- $N(a) \leq G$
- Each coset gH has H elements.
- Action of G on cosets of $H \leq G$: $a(g, xH) = (gx)H$.
- [Factor Groups] If N is a normal subgroup of G, then G/N is a group.
- $[G, G]$ is a normal subgroup of G
- If N is a normal subgroup of G, then G/N is abelian if and only if $[G, G] \subset N$.
- $G/[G, G]$ is the largest abelian quotient of G.
- For an abelian group M, $\text{End}(M)$ is a ring with addition as pointwise addition (group operation) and multiplication as function composition.

Actions and Orbits

- [Action] An <u>action</u> of group G on set X is a homomorphism $\phi: G \to \text{Sym}(X)$
  - It can also be characterized by action map
  - [Left Action Map] A left action map $a: G \times X \to X$ of an action ϕ corresponds to $a(g, x) = \phi(g)(x)$. It must satisfy:
    - $a(e, x) = x$
    - $a\big(g, a(h, x)\big) = a(gh, x)\ \forall g, h \in G, x \in X$
  - [Right Action Map] A right action map $a: X \times G \to X$ satisfies:
    - $a(x, e) = x$
    - $a(a(x, g), h) = a(x, gh)\ \forall g, h \in G, x \in X$
  - $a(g, x) = xg^{-1}$ is a left action where $a: G \times G \to G$
  - $a(x, g) = xg$ is a right action where $a: G \times G \to G$
- [Orbits] Let G act on X. The <u>orbit</u> of $x \in X$ is $Gx = \{gx | g \in G\}$. Denote $[x] = \{y | y \in X, y \sim x\} = Gx$ the orbits of the group actions. Note that gx here means g acting on x, not multiplication.
  - Orbits form an equivalence relation i.e. $x \sim y$ if $y \in Gx$
  - Orbits of the action of $\langle g \rangle \leq \text{Sym}_n$ on $\{1,2, \dots, n\}$ are the same as the cycles of g i.e. if $g = (1\ 2)(3\ 4\ 5)$, then the action has one orbit of length 2 ($\{1,2\}$) and one orbit of length 3 ($\{3,4,5\}$)
  - $\sigma, \tau \in \text{Sym}_n$ are conjugated if and only if their orbits have the same length
  - If $f \in \text{Sym}_n$ is of order p prime, then the orbits of any element under f has either 1 or p elements.
- [Action of Group on Itself] $a: G \times G \to G$
- [Conjugate] Let G be a group and $a, b \in G$. Say b is the <u>conjugate</u> of a in G if $\exists c \in G$ s.t. $b = c^{-1}ac$.
- [Conjugation] Conjugation is the action of G on itself given by $a(g, x) = gxg^{-1}$
  - $a(g, \cdot)$ is a bijection in addition to being a homomorphism.
  - If g is abelian, then conjugation is just the identity action.

- [Conjugacy Class] The conjugacy class of $x \in G$ is the set $C(x) = \{g \in G | g \sim x\} = \{g^{-1}xg | g \in G\}$. It is just the orbit of x under conjugation.
- [Transitive] Say an action is transitive if there is only one orbit for the action of G on X.
- [Stabilizer] The stabilizer of $x \in X$ is $\mathrm{stab}_G(x) = \{g \in G | gx = x\}$ i.e. $a(g, x) = x$.
  - $\mathrm{stab}_G(x) \leq G$
- [Orbit Stabilizer Relation] If G acts on set X and $x \in X$, then $|G| = |Gx||\mathrm{stab}_G(x)|$.
- [Conjugacy Class Equation] Let G be a finite group.
  - For any $x \in G$, the elements in the conjugacy class $C(x)$ are in one-to-one correspondence with the cosets of the centralizer $C_G(x)$.
  - $|C(x)| = [G/C_G(x)]$
  - $|G| = |Z(G)| + \sum_i [G/C_G(x_i)]$ where the sum is over a representative element from each conjugacy class that is not in the center.

Theorems

- [Subgroup Criterion] A **nonempty** subset $H \subseteq G$ is a subgroup of G if and only if $x, y \in H \Rightarrow xy^{-1} \in H$.
- If $H \leq G$ and S is the set of right cosets of H in G, then there is a homomorphism $\theta: G \to \mathrm{Sym}(S)$ with $\ker\theta$ being the largest normal subgroup of G contained in H.
- If G is a finite group and $H \leq G$ with $H \neq G$ such that $o(G) \nmid i(H)!$, then H must contain a nontrivial normal subgroup of G. In particular, G cannot be simple.
- If G is a finite group, then $|C(a)| = \frac{|G|}{|N(a)|}$
- [Lagrange's Theorem] If $H \leq G$, then $|H|||G|$.
  - A group G with prime order is cyclic.
  - If G is finite and $a \in G$, then $o(a)||G|$
  - If G is finite, then $a^{|G|} = e \; \forall a \in G$
- [Cauchy's Theorem] If G is a finite group and p prime s.t. $p||G|$, then G contains a subgroup that is cyclic with p elements.
- [Burnside Lemma] Let G be a finite group that acts on set X. Denote by X^g the set of elements of X fixed by g i.e. $g \cdot x = x$. Then $|X/G| = \frac{1}{|G|}\sum_{g\in G}|X^g| = \frac{1}{|G|}\sum_{x \in X}|\mathrm{stab}_G(x)|$ i.e. the number of orbits is equal to the average number of points fixed by an element of G.
- [First Homomorphism Theorem] If $\phi: G \to H$ is a homomorphism, then $G/\ker\phi \cong \mathrm{im}(\phi)$
  - The isomorphism can be written as $\psi: G/\ker\phi \to \mathrm{im}(\phi)$ via $\psi(a\ker\phi) = \phi(a)$
  - If N is a normal subgroup of G, then one can define a homomorphism $\phi: G \to G/N$ with $\phi(g) = [g] = gN$ with $\ker\phi = N$.
- [Correspondence Theorem] Let $\phi: G \to H$ be a homomorphism with kernel K. If $H' \leq \mathrm{im}(\phi)$ and $H = \{a \in G | \phi(a) \in H'\}$, then $H \leq G$, $\ker\phi \subset H$ and $H/K \cong H'$. If H' is a normal subgroup of $\mathrm{im}(\phi)$, then H is also a normal subgroup of G.
- [Second Homomorphism Theorem] Let $H \leq G$ and $N \trianglelefteq G$, then $H/(H \cap N) \cong HN/N$.
  - $H \cap N \trianglelefteq H$
  - $HN \leq G$
  - $N \trianglelefteq HN$
  - $\psi: H \to HN/N$ such that $\psi(h) = hN$
- [Third Homomorphism Theorem] Let $\phi: G \to H$ be a homomorphism with $\ker\phi = K$. If $N' \trianglelefteq \mathrm{im}(G)$ and $N = \{g \in G | \phi(g) \in N'\}$, then $(G/K)/(N/K) \cong G/N$.
  - $G/K \cong \mathrm{im}(G)$
  - $N/K \cong N'$
  - $\psi: G/K \to G/N$ such that $\psi(gK) = gN$
- [Jordan Hölder Theorem] Any two composition series of the same group have the same length and the same composition factors (up to permutation).

Symmetric and Alternating Groups

- The symmetric group on set X, denoted as $\mathrm{Sym}(X)$, is the group of bijections from $X \to X$ with function composition.
- If $f: X \to Y$ is a bijection, then $\phi: \mathrm{Sym}(X) \to \mathrm{Sym}(Y)$ is an isomorphism, where $\phi(g) = f \circ g \circ f^{-1}$.
- Cycles with disjoint entries commute i.e. if $A = (a_1, \dots, a_n)$ and $B = (b_1, \dots, b_m)$ with $\{a_1, \dots, a_n\} \cap \{b_1, \dots, b_m\} = \phi$, then $AB = BA$.
- A transposition is a two-cycle e.g. $(2\ 4) = (4\ 2)$
- A l-cycle can be written as the product of $l - 1$ transpositions.
- Transpositions generate Sym_n
- An element $\sigma \in \mathrm{Sym}_n$ is even if it can be written as a product of an even number of transpositions and odd otherwise.
    - A l-cycle is even if and only if l is odd.
- A permutation matrix is a $n \times n$ matrix M such that $M_{ij} = 0$ for all i, j except for one entry in each row and column where $M_{ij} = 1$.
    - Bijection $M_{ij} = \begin{cases} 1, & i = \sigma(j) \\ 0, & i \neq \sigma(j) \end{cases}$
- Two elements are conjugate in Sym_n if and only if they consist of the same number of disjoint cycles of the same length
- For conjugation in symmetric groups, $g\big((a\ b)(c\ d)\big)g^{-1} = \Big(\big(g(a)\ g(b)\big)\big(g(c)\ g(d)\big)\Big)$
- $\epsilon: \mathrm{Sym}_n \to \{1, -1\}$ is a sign homomorphism.
    - ϵ: $\mathrm{Sym}_n \cong \{M_{ij}\} \xrightarrow{\det} \{\pm 1\}$
    - $\epsilon(g) = -1$ if and only if g has an odd number of transpositions
    - $\ker \epsilon = A_n$
- A_n is the subgroup of Sym_n consisting of even permutations
- $|A_n| = \begin{cases} 1, & n = 1 \\ \frac{n!}{2}, & n \geq 2 \end{cases}$
- A_n is generated by 3-cycles.
- [Cayley's Theorem] Any group G is isomorphic to a subgroup of $\mathrm{Sym}(G)$.

Examples

- $GL_n(\mathbb{C})$: general linear group i.e. invertible $n \times n$ matrices with components in $\mathbb{C}$
- [Dihedral Group] The dihedral group D_n is the group of symmetries of a regular n-gon.
    - $|D_n| = 2n$
    - $D_n = \{e, r, r^2, \dots, r^{n-1}, z, rz, r^2z, \dots, r^{n-1}z\} = \langle\{r, z\}\rangle$
    - $rzr = z^{-1}$
- K_4: Klein-4 group; product of two non-identity elements maps to the third element.
- C_n: cyclic group of order $n = \{e, g, g^2, \dots, g^{n-1}\}$
- Sym_n: symmetric group; the set of bijections from $[n]$ to $[n]$ with function composition
    - $\{e, (1\ 2)\}$ is a subgroup, but not a normal subgroup, in Sym_3
    - Sym_3 is not abelian
- A_n: alternating group; group of even permutations of a finite set.
    - A_n is abelian if and only if $n \leq 3$
    - A_n is simple if and only if $n = 3$ or $n \geq 5$
    - A_5 is the smallest non-abelian simple group, with order 60
    - K_4 is a proper normal subgroup of A_4

Ring Theory

Definitions

- [Ring] A <u>ring</u> is a set R with two operations addition $+: R \times R \to R$ and multiplication $\cdot : R \times R \to R$ such that
  - $(R, +)$ is an abelian group: associative, has an identity, closed under inverse, commutative
  - Associativity of multiplication: $(ab)c = a(bc)$
  - Distributivity: $a(b+c) = ab + ac$, $(a+b)c = ac + bc$ $\forall a, b, c \in R$
  - Identity 1 for multiplication exists (and belong to the ring)
- [Commutative Ring] Say a ring R is <u>commutative</u> if its multiplication is commutative.
- [Polynomial] Let R be a ring. Then $R[x]$ is the set of polynomials with coefficients in R.
  - $R[x]$ is a ring
  - $(f+g)(n) = f(n) + g(n)$
  - $(fg)(n) = \sum_{i=0}^{n} f(i)g(n-i)$
- [Matrices] Let R be a ring. Then $\mathrm{Mat}_n(R)$ is the set of $n \times n$ matrices with entries in R.
  - $\mathrm{Mat}_n(R)$ is a ring.
- [Zero Divisor] A <u>zero-divisor</u> in a commutative ring R is a nonzero element $a \in R$ s.t. $ab = 0$ for some nonzero $b \in R$
- [Integral Domain] An <u>integral domain</u> is a commutative ring with no zero divisors.
  - If $ab = ac$, then either $a = 0$ or $b = c$
- [Subring] Say S is a <u>subring</u> of R if:
  - $(S, +)$ is a subgroup of $(R, +)$
  - Multiplication is associative in S (inherited from R)
  - Distributivity (inherited from R)
  - $1_R \in S$ and 1_R must be the multiplicative identity in S
  - S is closed under multiplication
- [Ring Homomorphism] Let R and S be rings. Say $\phi: R \to S$ is a <u>ring homomorphism</u> if:
  - $\phi(r_1 + r_2) = \phi(r_1) + \phi(r_2)$ (group homomorphism)
  - $\phi(r_1 r_2) = \phi(r_1)\phi(r_2)$
  - $\phi(1_R) = 1_S$
- [Kernel] Let $\phi: R \to S$ be a ring homomorphism, then the <u>kernel</u> of ϕ is $\ker \phi = \{r \in R | \phi(r) = 0\}$.
- [Ideal] Let R be a ring and I a subset of R s.t. $(I, +) \leq (R, +)$
  - Say I is a <u>left ideal</u> if $\forall r \in R, \forall x \in I$, $rx \in I$
  - Say I is a <u>right ideal</u> if $\forall r \in R, \forall x \in I$, $xr \in I$
  - Say I is a <u>two-sided ideal</u> if it is both a left ideal and a right ideal.
- [Principal Ideal] Let R be a ring, then the <u>principal ideal generated by $a \in R$</u> is $Ra = \{ra | r \in R\}$.
- [Ideal Generated] Let $(r_i)_i$ be a family of elements of R (i.e. $r_i \in R$ $\forall i$), then the ideal generated by r_i is $\bigcap_{r_i \in J, J \text{ an ideal of } R} J$.
- [Quotient] Let R be a ring and I be an ideal of R. Then, define the <u>quotient group</u> as $R/I = \{r + I | r \in R\}$. R/I is also a ring in addition to being an abelian group.
- [Prime Ideal] An ideal P of a ring R <u>prime</u> if $P \neq R$ and $\forall a, b \in R$, $ab \in P \Rightarrow a \in P$ or $b \in P$.
- [Maximal Ideal] An ideal $I \neq R$ in ring R is <u>maximal</u> if for any ideal J such that $I \subseteq J \subseteq R$, either $J = I$ or $J = R$.
- [Principal Ideal Domain] A <u>principal ideal domain</u> is an integral domain in which every ideal is principal i.e. of the form $\{ra | r \in R\}$ for some $a \in R$.
- [Divides] Let R be an integral domain and $a, b \in R$. Say a <u>divides</u> b if $\exists d \in R$ s.t. $da = b$.
- [Unit] Say a nonzero element $a \in R$ is a unit if $\exists$ nonzero element $b \in R$ s.t. $ab = 1$.
- [Group of Units] Denote by $R^\times = \{a | \exists b \text{ s.t.} ab = 1\}$ the group of units. It forms a group under multiplication.

- [Associates] Say $a, b \in R$ are associates if any (and therefore all) of the following holds:
  - $a = ub$ for some $u \in R^\times$ (i.e. multiplicative inverse of u exists)
  - $a|b$ and $b|a$
  - $Ra = Rb$
- [Group of Units] Let R be a ring, then the group of units of R is $R^\times = \{r \in R | \exists s \in R: rs = sr = 1\}$ (i.e. the set of elements in R with multiplicative inverses)
- [Greatest Common Divisor] Let R be a principle ideal domain. The greatest common divisor of $a, b \in R$ is any $d \in R$ s.t. $Rd = Ra + Rb$ (d is defined up to associates).
- [Prime] Let $a \in R$ be a nonzero, non-unit element. Say $a \in R$ is prime if $\forall b, c \in R$, $a|bc \implies a|b$ or $a|c$
- [Irreducible] Let $a \in R$ be a nonzero, non-unit element. Say $a \in R$ is irreducible if $\forall b, c \in R$ $a = bc \implies$ either a, b are associates or a, c are associates (the other one must be a unit).
- [Unique Factorization Domain] An integral domain R is a unique factorization domain if any nonzero element can be written as $u \cdot x_1 \cdot x_2 \cdot \ldots \cdot x_n$ with $u \in R^\times$ and x_i irreducible. Given two such factorizations, we have $m = n$ and x_i,y_i are associates (up to ordering).
- [Noetherian] A commutative ring R is Noetherian if for any nested sequence of ideals $I_1 \subseteq I_2 \subseteq \cdots$, there exists $N \in \mathbb{N}$ s.t. $I_n = I_N$ $\forall n \geq N$ i.e. there is no infinite strictly increasing chain of ideals.
- [Nilradical] The nilradical of a ring R is the ideal containing nilpotent elements i.e. $N = \{r \in R | \exists n \in \mathbb{Z}^+ \text{ s.t. } r^n = 0\}$

Properties

- [Properties of Ring] $\forall a \in R$
  - $a0 = 0a = 0$
  - $-a = (-1)a$
  - $-(-a) = a$
  - $(-a)b = -(ab) = a(-b)$
  - $(-a)(-b) = ab$
- [Subring Criterion]
  - $a, b \in S \Rightarrow a - b \in S$
  - $a, b \in S \Rightarrow ab \in S$
  - $1_R \in S$
- Let $\phi: R \to S$ be a ring homomorphism, then $\mathrm{im}(\phi)$ is a subring of S.
- Let $\phi: R \to S$ be a ring homomorphism, then $\ker \phi$ is a two-sided ideal of R.
- Let I be an ideal inside ring R. If $1_R \in I$, then $I = R$.
- The sum of two ideals $I_1 + I_2 = \{x_1 + x_2 | x_1 \in I_1, x_2 \in I_2\}$ is an ideal.
- In a commutative ring, for any element $a \in R$, Ra is an ideal. (!!!)
- Let $(I_n)_n$ be a family of left/right/two-sided ideals of ring R. Then $\bigcap_n I_n$ is also a left/right/two-sided ideal of R.
- $a|b \Leftrightarrow Rb \subseteq Ra$ i.e. the smaller element generate the larger ideal.
- Let R be an integral domain. Then if $a \in R$ is prime, then a is also irreducible.

Theorems and Lemmas

- [Fundamental Homomorphism Theorem] If $\phi: R \to S$ is a ring homomorphism, then $R/\ker\phi \cong \mathrm{im}(\phi)$ and $R/\ker\phi$ and $\mathrm{im}(\phi)$ are both rings.
  - Use $\psi: R/\ker\phi \to \mathrm{im}(\phi)$ with $\psi(r + \ker\phi) = \phi(r)$
- A subring of an integral domain is still an integral domain
- Let R be a commutative ring and $I \neq R$ be an ideal. Then I is prime if and only if R/I is an integral domain.
- Let R be a commutative ring and I be an ideal. Then I is a maximal ideal if and only if R/I is a field.
- Any maximal ideal of a commutative ring is also a prime ideal.
- A commutative ring R is a field if and only if the only ideals of R are $\{0\}$ and R.

- Let R be an integral domain. Then $\phi: R \to \mathrm{Frac}(R)$ given by $\phi(r) = \frac{r}{1}$ is a ring homomorphism.
  - If R is a field, then ϕ is an isomorphism i.e. $R \cong \mathrm{Frac}(R)$.
- R is an integral domain $\Leftrightarrow$ $R[x]$ is an integral domain
- If $\mathbb{F}$ is a field, then $\mathbb{F}[x]$ is a principal ideal domain i.e. every ideal in $\mathbb{F}[x]$ is principal.
- Let R be an integral domain and $a, b \in R$, then the following are equivalent:
  - $a = ub$ for some $u \in R^\times$ (i.e. $\exists u^{-1}$)
  - $a|b$ and $b|a$
  - $Ra = Rb$
- In a principal ideal domain R, Ra is a maximal ideal if and only if a is irreducible.
- In a principal ideal domain, irreducible elements are prime.
- Principal ideal domains are Noetherian.
- Principal ideal domains are unique factorization domains.
  - If $\mathbb{F}$ is a field, then $\mathbb{F}[x]$ is a unique factorization domain.
- Let R be an integral domain. If R is also a unique factorization domain, then so is $R[x]$
- Let R be a principal ideal domain.
  - If $a \in R$ is not zero nor unit, then a is divisible by an irreducible element.
  - If a is a nonzero element, we may write it as $a = u \cdot x_1 \cdot \ldots \cdot x_n$ where $u \in R^\times$ is a unit and x_i irreducible.

Examples

- $\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}$ is a ring
- $\mathbb{Z}, \mathbb{Q}[x]$ are integral domains
- $\mathbb{Z}, \mathbb{Q}[x], \mathbb{R}[x], \mathbb{C}[x]$ is a principle ideal domain and hence a unique factorization domain

Field Theory

Definitions

- [Field] A field is a commutative ring in which every non-zero element has a multiplicative inverse.
- [Field of Fractions] Let R be an integral domain. The field of fractions of R is $\text{Frac}(R) = \{(a,b) \in R \times (R\{0\})\}/\sim$ where $(a,b) \sim (c,d)$ if $ad = bc$.
  - $\text{Frac}(\mathbb{Z}) = \mathbb{Q}$
  - $\text{Frac}(R)$ is a field
- [Field Extension] Let K, L be fields with $K \subseteq L$, then say L is a field extension of K and write as L/K.
- [Degree] Let L/K be a field extension, then its degree is the dimension of L as a vector space over K.
- [Algebraic] Let L/K be a field extension and $t \in L$. If any (and therefore all) of the following conditions holds, say t is algebraic over K.
  - Powers of t span a finite dimensional subspace of L (over K)
  - t obeys a nontrivial polynomial equation with coefficients in K
  - $\ker \phi_t$ is nontrivial (i.e. contains a nonzero element of $K[x]$)
- [Transcendental] Say t is transcendental over K if it is not algebraic over K.
- [Algebraic Extension] Let L/K be a field extension. Say L/K is an algebraic extension if every element of L is algebraic over K.
- [Algebraically Closed] Say a field K is algebraically closed if every polynomial $P(x)$ of degree ≥ 1 in $K[x]$ has a zero in K (i.e. $P(t) = 0$ for some $t \in K$)
- [Minimal Polynomial] Let L/K be a field extension and $t \in L$. Define $\phi_t: K[x] \to L$ as the evaluation at t. Then the minimal polynomial of t is the element of $K[x]$ that generates the ideal $\ker(\phi_t)$, usually taken to be monic.
- [$\mathbb{Q}[\alpha_1, \dots, \alpha_r]$] Let $\alpha_1, \dots, \alpha_r \in \mathbb{C}$, then $\mathbb{Q}[\alpha_1, \dots, \alpha_r]$ is the smallest subring of $\mathbb{C}$ containing $\mathbb{Q}$ and $\alpha_1, \dots, \alpha_r$.
- [$\mathbb{Q}(\alpha_1, \dots, \alpha_r)$] Let $\alpha_1, \dots, \alpha_r \in \mathbb{C}$, then $\mathbb{Q}(\alpha_1, \dots, \alpha_r)$ is the smallest subfield of $\mathbb{C}$ containing $\mathbb{Q}$ and $\alpha_1, \dots, \alpha_r$.
  - $\mathbb{Q}(\alpha_1, \dots, \alpha_r) = \text{Frac}(\mathbb{Q}[\alpha_1, \dots, \alpha_r])$
- [Characteristic] The characteristic of a ring R is the unique nonnegative integer m such that $\ker \psi = m\mathbb{Z}$ where $\psi: \mathbb{Z} \to R$ is the unique homomorphism for R.
- [Prime Subfield] The prime subfield of a field K is: (equivalent conditions)
  - The subfield generated by 1
  - The smallest subfield of K
  - The intersection of all subfields of K

Properties

- A field is an integral domain i.e. it has no zero divisors.
- A commutative ring R is a field if and only if its only ideals are $\{0\}$ and R.
- Let K, L be fields and $\phi: K \to L$ be a ring homomorphism, then ϕ is injective.
- If $\deg L/K$ is finite i.e. L is finite dimensional over K, then L is algebraic over K. For any $t \in L$, $\text{span}(\{1, t, t^2, \dots\})$ is finite dimensional.
- Minimal polynomials are irreducible.
- If K is an algebraically closed field and L/K is an algebraic extension, then $L = K$.
- A commutative ring R is a field if and only if its only ideals are $\{0\}$ and R.
- Let K be a field, then $K[x]$ is a principal ideal domain.

Theorems

- [Wedderburn's Little Theorem] Every finite integral domain is a field.
- Let L/K be a field extension and $t \in L$. Let $\phi_t: K[x] \to L$ be evaluation at t. The following are equivalent:
  - Powers of t span a finite dimensional subspace of L (over K)

- t obeys a nontrivial polynomial equation with coefficients in K
- $\ker \phi_t$ is nontrivial (i.e. contains a nonzero element of $K[x]$)

- If $\deg(L/K)$ finite i.e. L finite dimensional over K, then L is algebraic over K. For any $t \in L$, $\operatorname{Span}\{1, t, t^2, \dots\}$ is a subspace of L and hence finite dimensional.
- Let K be a field and $p(x) \in K[x]$ be an irreducible polynomial.
  - $K[x]p(x) = \big(p(x)\big)$ is a maximal ideal
  - $K[x]/(p(x))$ is a field
  - $\deg\big((K[x]/p(x))/K\big) = \deg(p)$

Characteristics

- Let R be a ring, then there is a unique homomorphism $\psi: \mathbb{Z} \to R$.
- The characteristic of a field is either 0 or a prime number.
- There are no homomorphisms between fields of different characteristics.
- If $\mathbb{F}$ is a finite field, then $\operatorname{char}(\mathbb{F}) > 0$ i.e. all finite fields have positive characteristic.
- If $\operatorname{char}(K) > 0$, then $\ker \psi = p\mathbb{Z}$ for some prime p and $\operatorname{im}(\psi) \cong \mathbb{Z}/\operatorname{char}(K)\mathbb{Z}$
- If $\operatorname{char}(K) > 0$, then its prime subfield is $\mathbb{Z}/\operatorname{char}(K)\mathbb{Z}$ and it is a field extension of $\mathbb{Z}/\operatorname{char}(K)\mathbb{Z}$. If $\operatorname{char}(K) = 0$, then its prime subfield is $\mathbb{Q}$.
- If K is a finite field, its prime subfield is $\mathbb{Z}/\operatorname{char}(K)\mathbb{Z}$ and it is a field extension of $\mathbb{Z}/\operatorname{char}(K)\mathbb{Z}$.
- If $\mathbb{F}$ is a finite field of characteristic p, then the size of $\mathbb{F}$ is a power of p.

Examples

- $\mathbb{Z}/p\mathbb{Z}$ is a field for prime p.
- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields.
- $\mathbb{C}$ is algebraically closed.
- $\mathbb{Q}\big(\sqrt{2}\big)/\mathbb{Q}$, $\mathbb{C}/\mathbb{R}$ are algebraic field extension