Abstract Algebra Notes

John Darges

May 2019

1 Group Theory

1.1 Groups

Definition of a Group A group is a set G paired with a binary operation $*$ that satisfies associativity, has an identity, and has inverses.

Properties

- $g_1h = g_2h$ implies $g_1 = g_2$
- Identity and inverses are unique
- $(gh)^{-1} = h^{-1}g^{-1}$
- $e^{-1} = e$

Example $S_n =$ the set of permutations of $\{1, ..., n\}$.

Definition of abelian group An abelian group is one with a commutative operation.

Example $D_n =$ symmetries of regular $n-$gon

Definition of Subgroup $H \subseteq G$ is a subgroup if it is closed under the operation $*$ and under inverses. Notation: $H < G$.

Properties

- $\{e\} < G$
- $G < G$
- $H_\alpha < G$ for all α implies that $\cap_\alpha H_\alpha < G$ item $H < G, K < H$ implies $K < G$

Proposition For any collection $\{x_\alpha\}_{\alpha\in A} \subseteq G$, there exists a subgroup $\langle\{x_\alpha\}\rangle < G$ satisfying

- $x_\alpha \in \langle\{x_\alpha\}\rangle$ for all α
- If $\{x_\alpha\}_{\alpha\in A} \subseteq H$, then $\langle\{x_\alpha\}\rangle < H$

Proof. Define $\langle\{x_\alpha\}\rangle = \cap_{H<G,\{x_\alpha\}_{\alpha\in A}\subseteq H} H$ □

Fact: If $g \in G$, then $\langle g\rangle = \{g^n | n \in \mathbb{Z}\}$.

Definition of cyclic A group G is cyclic if $G = \langle g\rangle$ for some $g \in G$. G is finitely generated if $G = \langle g_1, ..., g_n\rangle$.

Definition For $g \in G$, the order of G is $|\langle g\rangle|$ (the cardinality). The order of G is $|G|$.

Definition of homomorphism A map $\phi : G \to H$ is a homomorphism if $\phi(g_1 * g_2) = \phi(g_1) * \phi(g_2)$ for all $g_1, g_2 \in G$. If ϕ is bijective then it is an isomorphism.

Proposition Let $\phi : G \to H$ be a homomorphism

- $Ker(\phi) < G$
- $Im(\phi) < H$
- ϕ is injective $\iff$ $Ker(\phi) = \{e\}$
- ϕ is surjective $\iff$ $Im(\phi) = H$

Definition of automorphism group

$$Aut(G) = \{\phi : G \to G | \phi \text{ is an isomorphism }\}$$

1.2 Cosets

Definition of Coset Given $H < G$, for $g \in G$, $gH = \{gh | h \in H\}$ is a left coset, while Hg is a right coset.

We can use this to partition G into cosets. G/H is the set of equivalence classes of left cosets of H. The cardinality of G/H, $[G : H]$, is called the index of H in G.

Lagrange's Theorem If $H < G$, then $[G : H]|H| = |G|$. If $|G| < \infty$, then $|H|$ divides $|G|$.

More generally, if $K < H < G$, then $[G : K] = [G : H][H : K]$.

Proof. We will show a bijection $G/H \times H \to G$ □

1.3 Normal Subgroups

Definition of Normal Subgroup If $gH = Hg$ for all $g \in G$, then this is a normal subgroup. Notation: $H \triangleleft G$

Fact The following statements are equivalent

- $H \triangleleft G$
- $gHg^{-1} = H$ for all $g \in G$
- $gHg^{-1} \subseteq H$ for all $g \in G$

Proof. ((3) $\Rightarrow$ (2)) Suppose $gHg^{-1} \subseteq H$ for all $g \in G$. This implies that $H = g^{-1}(gHg^{-1})g \subseteq g^{-1}Hg$ for all $g \in G$. So $H \subseteq gHg^{-1}$. □

Lemma Let $\phi : G \to H$ be a homomorphism. Then $Ker(\phi) \triangleleft G$.

Proof. Let $h \in Ker(\phi)$. Fix $g \in G$ and consider $ghg^{-1} \in gKer(\phi)g^{-1}$. Then $\phi(ghginv) = \phi(g)\phi(h)\phi(h^{-1}) = \phi(g)\phi(g)^{-1} = e_H$. So $ghg^{-1} \in Ker(\phi)$. Then $gKer(\phi)g^{-1} \subseteq Ker(\phi)$. So $Ker(\phi) \triangleleft G$. □

Note: All subgroups of abelian groups are normal.

Proposition If $H < G$ is normal, then G/H admits a group structure given by $gH \cdot g'H = (g \cdot g')H$.

Proof. (Well-defined)

(Associativity)

(Identity)

(Inverse)

□

Fact

(1) Let $N \triangleleft G$. Define $\pi : G \to G/N$ such that $g \mapsto gN$.

Then π is a surjective homomorphism and $Ker(\pi) = \{g|gN = N\} = N$.

(2) If $N \triangleleft G$ and $H < G$, then $N \cap H \triangleleft H$

Corollary: If $N \triangleleft G$, $N < H < G$, then $N \triangleleft H$. In this case, $H/N = \{gN|g \in H\} < G/N$.

Induced Homomorphism Let $\phi : G \to H$ be a homomorphism. Choose $N \triangleleft G$ such that $N < Ker(\phi)$. Then ϕ induces $\bar{\phi} : G/N \to H$ defined by $\bar{\phi}(gN) = \phi(g)$.

Note

(1) $Im(\bar{\phi}) = Im(\phi)$

(2) $Ker(\bar{\phi}) = \{gN|\phi(g) = e\} = \{gN|g \in Ker(\phi)\} = Ker(\phi)/N$.

First Isomorphism Theorem Let $\phi : G \to H$ be a homomorphism. Then ϕ induces $\bar{\phi} : G/Ker(\phi) \to Im(\phi)$ which is an isomorphism.

Proof. □

Property Let $f : G \to H$ with $N \triangleleft G$ and $M \triangleleft H$. If $f(N) \subseteq M$, then f induces a homomorphism $\bar{f} : G/N \to G/M$ where $aN \mapsto f(a)M$.

Proof. (Well-defined)

(Homomorphism)

□

Second Isomorphism Theorem Let $K < G$, $N \triangleleft G$. Then $K/(N \cap K) \cong NK/N$ where $NK = \{nk|n \in N, k \in K\}$.

Third Isomorphism Theorem Let $K < H$ and $K, H \triangleleft G$. Then $H/K \triangleleft G/K$ and $(G/K)/(H/K) \cong G/H$.

Proof. Define $\phi : G/K \to G/H$ by $gK \mapsto gH$. □

Commutative Diagrams Let $\phi : G \to J$ be a homomorphism of groups. Then we saw there exists $\bar{\phi} : G/N \to J$ whenever $N \triangleleft G$ and $N \subseteq Ker(\phi)$.

By construction, $\bar{\phi} \circ \rho = \phi$ where $\rho : G \to G/N$ is the canonical projection. We illustrate this usinga commutative diagram.

Proposition $\bar{\phi}$ is unique in the sense that if there exists $\psi : G/N \to J$ such that $\phi = \psi \circ \rho$, then $\psi = \bar{\phi}$

Proof. This is a general principle about commutative diagrams. □

1.4 Symmetric Groups

Definition $\sigma \in S_n$ is a $k-$cycle if there exist $i_1, ..., i_k$ such that

- $\sigma(i_j) = i_{j+1}$ for $1 \leq j \leq k-1$
- $\sigma(i_k) = i_1$
- $\sigma(l) = l$ if $l \neq i_j$

We denote this by $(i_1 ... i_k)$.

If $\sigma = (i\ j)$, then σ is a transposition.

Proposition

(1) Every $\sigma \in S_n$ is a product of disjoint cycles.

(2) Every $\sigma \in S_n$ is a product of transpositions.

Proof. □

Remark σ cannot be uniquely written as a product of disjoint cycles.

However, the set of disjoint cycles is unique.

Definition A representation of a group G is a homomorphism $\rho : G \to GL_n(\mathbb{R})$ for some n. We define a homomorphism $\rho : S_n \to GL_n(\mathbb{R})$ by $\sigma \mapsto A_\sigma$ where A_σ is the permutation of the identity matrix by σ. ρ is an injective homomorphism.

Since every σ is the product of transpositions, each A_σ is the product of elementary permutation matrices that switch two columns.

Theorem σ can be expressed as a product of and odd number of cycles or an even number, but not both.

Proof. □

1.5 Free Groups

Let $X \subseteq G$. $\langle\langle X \rangle\rangle$ is the normal subgroup generated by X.

Definition Let G_α be a collection of groups. A simplified word is a finite sequence $g_{\alpha_1} ... g_{\alpha_n}$ where $g_{\alpha_i} \in G_{\alpha_i}$.

The collection of all simplified words, $*_{\alpha \in A} G_\alpha$ has a group structure. This is the free product on the G_{α_i}s.

Definition of free group A free group is one of the form $*_{\alpha \in A} \mathbb{Z}$.

Definition Consider $F(A)$ on letters g_α for $\alpha \in A$. Let $\{r_\beta\}_{\beta\in B}$ be a collection of words in the g_α.

The group presentation $\langle\{g_\alpha\}|\ \{r_\beta\}\rangle$ represents $F(A)/\langle\langle\{r_\beta\}\rangle\rangle$.

Key observation Consider the free group $*_{\alpha\in A}\mathbb{Z}$ and let H be any group.

Any assignment $f : \mathbb{Z} \to H$ $g_\alpha \mapsto f(g_\alpha) \in H$ extends to a function $\bar{f} : *_{\alpha\in A}\mathbb{Z} \to H$ by $\bar{f}(*_{i=1}^n g_{\alpha_i}^{p_i}) = *_{i=1}^n \bar{f}(g_{\alpha_i})^{p_i}$.

This function is a homomorphism regardless of where f sends the generators g_α.

More generally, given $f_\alpha : G_\alpha \to H$ for all α, there exists a unique homomorphism $f : *_\alpha G_\alpha \to H$ such that $f \circ \iota_\alpha = f_\alpha$ where ι_α is the inclusion map $G_\alpha \to *_\alpha G_\alpha$.

If $f(r_\beta) = e$ for all $\beta \in B$, then f induces $\bar{f} : \langle g_\alpha|\ r_\beta\rangle \to G$.

Theorem

(1) Every group is isomorphic to a quotient of a free group.

(2) Every group admits a presentation.

Proof. □

Remark: Not all groups admit a finite presentation

Theorem A subgroup of a free group is free (Proof in topology sequence).

Here are some other constructions of groups.

Definition Let $\{G_n\}_{n=1}^k$ be a sequence of groups. The direct product $\Pi_{n=1}^k G_n$ consists of all sequences $(g_n)_{n=1}^k$ where $g_n \in G_n$. This is a group under multiplication $(g_n)_{n=1}^k \cdot (h_n)_{n=1}^k = (g_n \cdot h_n)_{n=1}^k$.

The direct sum $\oplus_{n=1}^k G_n$ is the subgroup consisting of sequences for which at most finitely many elements are non-trivial.

Note: if $k < \infty$ then the direct product and direct sum are the same. We can define many homomorphisms through inclusion and projection maps.

Theorem Given a collection of homomorphisms and groups $\phi_n : H \to G_n$,

(1) There exists a unique $\phi : H \to \Pi_{n=1}^\infty G_n$ such that $\pi_n \circ \phi = \phi_n$ for all n.

(2) If K is any other group with homomorphisms $\pi_n' : K \to G_n$ satisfying (1), then $K \cong \Pi_{n=1}^\infty G_n$.

Question Given a group G, is $G \cong G_1 \oplus G_2$ with G_i nontrivial.

If $G \cong G_1 \oplus G_2$ then

(1) $\iota_1\pi_1(x) + \iota_2\pi_2(x) = x$ for all $x \in G$

(2) $\pi_i\iota_i(x) = x$ for $i = 1, 2$

(3) $\pi_i\iota_j(x) = 0$ for $i \neq j$

Theorem Suppose G is abelian, and there exists homomorphisms $\iota_i : G_i \to G$ and $\pi_i : G \to G_i$ satisfying (1) and (3). Then $G \cong G_1 \oplus G_2$

(A similar result applies to non-abelian groups)

Theorem Let N_1, N_2 be normal subgroups of G such that $G = \langle N_1 \cup N_2 \rangle$. If $N_1 \cap N_2 = \{e\}$, then $G \cong N_1 \times N_2$.

1.6 Category Theory

A category $\mathcal{C}$ is

- a collection of objections $Ob(\mathcal{C})$
- Sets $Mor(X, Y)$ called set of morphisms for objects X, Y. Composition functions $\circ : Mor(X, Y) \times M(Y, Z) \to Mor(X, Z)$ with the properties that
  - For all objects X there exists a morphism $1_X \in Mor(X, X)$ such that $f \circ 1_X = f = 1_Y \circ f$ for any $f \in Mor(X, Y)$.
  - composition is associative.

Definition We say $A, B \in Ob(\mathcal{C})$ are equivalent if there exist morphisms $f : A \to B, g : B \to A$ such that $f \circ g = 1_B$ and $g \circ f = 1_A$.

Examples

(1) In *Groups*, equivalence is isomorphisms

(2) In $Vect$, V is equivalent to W if and only if $dimV = dimW$

Definition Let $\{X_\alpha | \ \alpha \in A\}$ be a collection of objects in $\mathcal{C}$. A product in $\mathcal{C}$ of $\{X_\alpha\}$ is an object $\Pi_\alpha X_\alpha$ and morphisms $\pi_\alpha : \Pi_\alpha X_\alpha \to X_\alpha$ for all α such that if there exists $\phi_\alpha : B \to X_\alpha$ for all α then there exists a unique $\phi : B \to \Pi_\alpha X_\alpha$ such that $\pi_\alpha \circ \phi = \phi_\alpha$ for all α.

Theorem In any category, the product is unique up to equivalence.

Definition Let $\{X_\alpha | \ \alpha \in A\}$ be objects in $\mathcal{C}$. We say that S is a coproduct if there exist morphisms $\iota_\alpha : X_\alpha \to S$ such that, given $\rho_\alpha : X_\alpha \to H$, there exists a unique morphism $\rho : X \to H$ such that $\rho \circ \iota_\alpha = \rho_\alpha$.

Note: we can often think of objects living in different categories (a group is also a set). These constructions heavily depend on the category we are viewing our object in.

Let $\rho_\alpha : G_\alpha \to H$ be homomorphisms with G_α, H abelian groups. Then define $\rho : \oplus_\alpha G_\alpha \to H$ by $\rho(g) = \sum_\alpha \rho_\alpha \pi_\alpha(g)$.

Note that ρ is the only homomorphism that could satisfy $\rho \circ \iota_\alpha = \rho_\alpha$ since $\oplus_\alpha G_\alpha$ is generated by $Im(\iota_\alpha)$'s. This implies $\oplus_\alpha G_\alpha$ is the coproduct in the category of abelian groups.

2 Structures of Groups

2.1 Structures of Abelian Groups

Definition A free abelian group is a direct sum of copies of $\mathbb{Z}$.

Note: A homomorphism $f : \mathbb{Z} \to H$ is simply governed by a choice of element in H. $f(1)$ determines the homomorphism.

Corollary Every abelian group is the quotient of a free abelian group. Thus, they admit abelian group presentations. The proof is the same as for regular group presentations.

Definition Let G be a group. $g \in G$ is torsion if it has finite order. If G is abelian, $\{g \in G | \ g \text{ is torsion}\}$ forms a subgroup of G called the torsion subgroup.

Theorem Let G be a finitely generated abelian group. Then

(1) $G \cong \mathbb{Z}^b \oplus (\mathbb{Z}_{p_1}^{n_1} \oplus ... \oplus (\mathbb{Z}_{p_k})^{n_k}$

(2) This decomposition is unique up to reordering.

Example

(1) Find all abelian groups of order 18, up to isomorphism.

(2) Prove $\mathbb{Q}/\mathbb{Z}$ is not finitely generated.

Definition A group G is decomposable if $G \cong G_1 \times G_2$ where both groups are nontrivial.

Question If $G \cong H_1 \times H_2$ and $G \cong K_1 \times K_2$, with H_i, K_i's indecomposable, can we say that H_i, K_i's must be isomorphic? Not true for infinite case, but true for finite groups. Under what conditions is this true for any group?

Definition

- G satisfies the ascending chain condition (ACC) if $H_1 < H_2 < ... < G$ implies $H_i = H_{i+1}$ for all $i \geq n$ for some n.
- G satisfies the descending chain condition (DCC) if $G > H_1 > ...$ implies $H_i = H_{i+1}$ for all $i \geq n$ for some n.

Krull-Schmidt Theorem Let G satisfy the ACC and DCC for normal subgroups. If $G \cong G_1 \times \cdots \times G_k \cong H_1 \times \cdots \times H_l$ with G_i, H_j's indecomposable, then $k = l$ and $G_i \cong H_i$ after reordering.

Theorem If G is nontrivial and satisfies ACC or DCC for normal subgroups, then $G \cong H_1, \times ... \times H_n$ where each $H_i < G$ is decomposable.

Proof. Suppose □

Proposition If $G = \langle N_1, N_2 \rangle$ with $N_1, N_2 \triangleleft G$ and $N_1 \cap N_2 = \{e\}$, then $G \cong N_1 \times N_2$.

Proof. Define $\phi : N_1 \times N_2 \to G$ by $(n_1, n_2) \to n_1 * n_2$. □

Definition of normal homomorphism $f : G \to G$ is normal if $af(b)a^{-1} = f(aba^{-1})$ for all $a, b \in G$.

Lemma If $f : G \to G$ is normal and G satisfies ACC and DCC on normal subgroups, then $G \cong Ker(f^n) \times Im(f^n)$ for some n.

Proof. □

Corollary If G satisfies the ACC and DCC, is indecomposable, and $f : G \to G$ is normal, then f is an isomorphism or is nilpotent.

Idea of Krull-Schmidt proof For simplicity, let $G = G_1 \times G_2 = H_1 \times H_2$ with G abelian. We'll show $G_1 \cong H_1$ or H_2.

Proof. Let $\pi_1 : G \to G_1$ be a projection. □

2.2 Group Actions

Definition Let G be a group, X be a set. An action of G on X is a function $G \times X \to X$, $(g, x) \mapsto gx$, satisfying

(1) $e * x = x$

(2) $(g_1 * g_2) * x = g_1(g_2 * x)$

Definition Let $G \curvearrowright X$ and fix $x \in X$

(1) The stabilizer of x is $G_x = \{g \in G | \ gx = x\}$

(2) The orbit of x is $\mathcal{O}_x = \{gx \in X | \ g \in G\}$

We say that G acts

- freely on X if $gx = hx$ implies $g = h$
- transitively if for all $x, y \in X$ there exists g such that $gx = y$ (i.e., there is exactly one orbit)
- faithfully if for all $g \in G$, there exists $x \in X$ such that $gx \neq x$

$Fix(G) = \{x | \ gx = x \text{ for all } g \in G\}$ Called fixed points.

Remark Let X be a set, $Perm(X)$ the group of bijections $f : X \to X$. An action of G on X is the same as a homomorphism from G to $Perm(X)$.

Examples

(A) Left translation: $(g, x) \mapsto gx$. This action is free and transitive.

(B) Conjugation: $(g, x) \mapsto gxg^{-1}$.

Proposition If $|G| < \infty$, then G is isomorphic to a subgroup of $S_{|G|}$.

Proof. Let G act on itself by left translation. This gives a homomorphism from G to $Perm(G) \cong S_{|G|}$. □

Note $G_x = \{g \in G | \ gx = xg\}$ This is called the centralizer of $x : C_G(x)$.

Proposition Fix $x \in X$. $[G : G_x] = |\mathcal{O}_x|$.

Proof. Define a function $\phi : G/G_x \to \mathcal{O}_x$ by $gG_x \mapsto g \cdot x$ □

Example If $G \curvearrowright G$ by conjugation, then $|\mathcal{O}_g| = 1 \iff g \in Z(G)$. This implies $|G| = |Z(G)| + \sum_{|\mathcal{O}_{x_\alpha} \geq 2} [G : C_G(x_\alpha)]$ (Class Equation)

Corollary If $|G| = p^n$ for p prime, then $Z(G)$ is nontrivial.

Proof. Note that if $[G : C_G(x_\alpha)] > 1$, then □

If $|G| = p^n$ and $G \curvearrowright X$, then $|X| = |Fix(X)| mod_p$

Corollary If $|X| \neq 0 mod_p$, then there exists a fixed point (so action is not free).

Theorem If $|G| = p^2$ with p prime. Then G is abelian. ($G \cong \mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \oplus \mathbb{Z}_p$)

Proof. $Z(G)$ is nontrivial. Therefore $|Z(G)| = p$ or p^2 by Lagrange's Theorem. □

2.3 Sylow Theorems

Goal is to study finite subgroups with order p^k with p prime. For finite groups, this will help us to classify. Throughout, p denotes a prime.

Definition A $p-$subgroup is a group such that every element has order of a power of p.

Cauchy's Theorem Let G be a finite group. If p divides $|G|$ with p prime, then there exists an element of order p.

Proof. (Case 1) Suppose G is abelian.

(Case 2) Suppose G is not abelian.

□

Definition A Sylow $p-$subgroup of order p^n where $|G| = p^n m$ with $gcd(p, m) = 1$.

First Sylow Theorem Let $|G| = p^n m$ with $gcd(p, m) = 1$. Fix $1 \leq i \leq n$. Then there exists a subgroup $H < G$ such that

(1) $|H| = p^i$

(2) If $i < n$, then H is normal in a subgroup of order p^{i+1}.

In particular, Sylow subgroups exist.

Proof. This proof assumes the case where $|G| = p^n$. We proceed by induction.

($i = 1$)

(General)

□

Second Sylow Theorem If $H < G$ with $|H| = p^k$ and P is a Sylow $p-$subgroup, then $H < xPx^{-1}$ for some $x \in G$. (Any two Sylow $p-$subgroups are conjugate).

Proof. Let $S = G/P$ (not considered as a group, just set of cosets). $H \curvearrowright S$ by left multiplication. □

Corollary If H is a normal Sylow $p-$subgroup, then it is the unique Sylow $p-$subgroup.

Third Sylow Theorem If $|G| < \infty$, then the number of Sylow $p-$subgroup divides $|G|$ and is of the form $kp + 1$.

Proof. Let $s =$ number of Sylow subgroups. $\square$

2.4 Solvability and Subnormal Series

Definition Let G be a group. A subnormal series is a sequence $G_n < G_{n-1} < ... < G_0 = G$ where $G_{i+1} \triangleleft G_i$ for $0 \leq i \leq n$.

A composition series is one of the form $\{e\} = G_n < ... < G_0 = G$ where G_i/G_{i+1}.

Proposition Any finite group admits a composition series.

Proof. If G is simple, then we are done. If not, choose $G_1 \triangleleft G$.

$\square$

Jordan-Holder Theorem Suppose G has a composition. Any other composition series has the same set of nontrivial factors up to isomorphism. (Order of factors need not be preserved.)

Definition A solvable series is a subnormal series $G = G_0 > ... > G_n = \{e\}$ such that G_i/G_{i+1} is abelian. A group is solvable if it has a solvable series.

Proposition If $H < G$ and G is solvable, so is H.

Proof. Let $\square$

Proposition Any finite group is solvable if and only if there exists a composition series whose factors are cyclic groups.

Proof. Let $G = G_0 > ... > G_n$ be a solvable series. $\square$

Proposition If G is solvable, $G > [G, G] = G' > [G', G'] = G'' > ... > \{e\}$ gives a solvable series.

3 Rings

3.1 Intro to Rings

Definition A ring is an abelian group R (group operation is addition) together with a binary operation $\cdot : R \times R \to R$ satisfying

- $r(st) = (rs)t$
- $r(s+t) = rs + rt$ and $(s+t)r = sr + tr$

Definition $a \in R$ is a left (or right) zero divisor if $a \neq 0$ and there exists some $b \neq 0 \in R$ such that $ab = 0$ (or $ba = 0$). A zero divisor is a left and right zero divisor.

Proposition If R has no left zero divisors then $a \neq 0$ and $ab = ac$ implies $b = c$.

Definition $\phi : R \to S$ is a homomorphism if $\phi(r+s) = \phi(r) + \phi(s)$ and $\phi(rs) = \phi(r)\phi(s)$.

Definition Let R have mult. identity.

(1) If R has no zero divisors and is commutative, then it is a domain.

(2) If every nonzero element of a ring R is a unit, then R is a division ring.

(3) If a division ring R is commutative, then R is a field.

Proposition A division ring has no zero divisors.

Definition A subring of R is a subgroup that is closed under multiplication.
Every ring is isomorphic to a subring of a ring with identity.

Definition R has characteristic n if n is the minimum positive integer such that $nr = 0$ for all $r \in R$. If no such n exists, then R has characteristic 0.

3.2 Ideals

Let $I \subseteq R$. I is a left (or right) ideal if

(1) $I < R$

(2) $x \in R$ and $s \in I$ implies $xs \in I$.

If R is commutative, then every ideal is two-sided.

Note An ideal is a subring, but not all subrings are ideals.

Proposition We can generate ideals. Let $\{I_\alpha\}_{\alpha \in A}$ be a collection of ideals in R. Then $\cap_{\alpha \in A} I_\alpha$ is an ideal.

Definition Let X be a subset of a ring R. $\langle X \rangle$ is the intersection of all ideals containing X, (i.e., the ideal generated by X).

Definition An ideal in R is principal if it is generated by one element.

Definition An ideal I is prime if for ideals A, B such that $A, B \subset I$, then either $A \subseteq I$ or $B \subseteq I$ and $I \neq R$.

Proposition Let $I \subset R$ be an ideal and $a, b \in R$. If $ab \in I$ implies $a \in I$ or $b \in I$, then I is prime.

Conversely, if R is commutative and I is prime, then $ab \in I$ implies $a \in I$ or $b \in I$.

3.3 Quotient Rings

Proposition Let $I \subseteq R$ be an ideal. Then R/I is a ring with addition coming from the quotient group and multiplication given by $(a + I)(b + I) = ab + I$.

Exercise

- Prove $\mathbb{Z}[x]/\langle x^2 \rangle$ is not ring isomorphic to $\mathbb{Z} \oplus \mathbb{Z}$.
- Consider the ring $\mathbb{Z}[x]/\langle x^2 - 1 \rangle$. Is there a zero divisor in this ring? Is there a unit other than $+/-1$?
- Consider the ring $\mathbb{Z}[x, y]$. Show $\mathbb{Z}[x, y]/\langle x - y \rangle \cong \mathbb{Z}[x]$.

Note The kernel of a ring homomorphism is an ideal. If I is an ideal containing $Ker(\phi)$ then $\psi : R/I \to S \; r + I \mapsto \phi(r)$ is a well defined homomorphism. $Im(\phi)$ is not always an ideal, though it is always a subring.

First Isom Theorem for Rings Let $\phi : R \to S$ be a ring homomorphism and $Ker(\phi) \subseteq I \subseteq R$, then $\psi : R/I \to S$ is an isomorphism onto $Im(\phi)$.

Proof. We know $\psi : R/I \to Im(\phi)$ is a surjective ring homomorphism. $\square$

Proposition Let R be a commutative ring with $1_R \neq 0$. R/I is a domain if and only if I is prime.

Proof. ($\Longleftarrow$) Let $a+I, b+I$ be such that $(a+I)(b+I)=0$.

($\Longrightarrow$)

□

3.4 Maximal Ideals

Definition An ideal I is maximal if, for $I \subseteq J \subseteq R$, with J ideal, then $J = I$ or $J = R$.

Proposition Let R be commutative. If $I \subset R$ is maximal, then I is prime.

Proof. □

Theorem Let R be commutative with mult. identity. $I \subset R$ is maximal if and only if R/I is a field.

Proof. ($\Longleftarrow$)

($\Longrightarrow$)

□

Example In $\mathbb{Z}$ every ideal is of the form $k\mathbb{Z}$. $k\mathbb{Z}$ is prime if and only if k is zero or prime. $k\mathbb{Z}$ is maximal if and only if $k\mathbb{Z}$ is prime.

Definition A principal ideal domain (PID) is a domain such that every ideal is principal (generated by a single element).

Proposition Maximal ideals always exist in rings with 1_R.

Proof. Requires Zorn's Lemma. If X is a partially ordered set such that every totally ordered subset an upper bounded, then there exists a maximal element. Let P be the set of proper ideals of R. A maximal element is necessarily a maximal ideal. □

Chinese Remainder Theorem Let R be a ring with mult. identity. Let $I_1, ..., I_n$ be ideals in R such that $I_i + I_j = R$ for all $i \neq j$. If $r_1, ..., r_n \in R$, then there exists $r \in R$ such that

- $r + I_i = r_i + I_i$ for all i
- r is unique up to adding by elements in $I_1 \cap ... \cap I_n$

Proof. $(n = 2)$ Let $I_1 + I_2 = R$. □

Corollary If $I_1 + I_2 = R$, where R has mult. identity, then $R/(I_1 \cap I_2) \cong R/I_1 \times R/I_2$. (More generally, $R/(I_1 \cap ... \cap I_n) \cong R/I_1 \times ... \times R/I_n$)

Proof. Define ϕ : □

3.5 Divisibility in Rings

Assume all rings are commutative with mult. identity. It is important to note that in this setting, $\langle a \rangle = \{ra | r \in R\}$.

Definition Let $a, b \in R$ and suppose $a \neq 0$. We say $a|b$ if there exists $r \in R$ such that $ar = b$.

Proposition $a|b$ if and only if $(b) \subseteq (a)$.

Proof. □

Proposition

(1) $u|r$ for all $r \in R$ if and only if u is a unit.

(2) If $a = ub$ with u a unit, then $b|a$.

(3) Let R be a domain. If $a|b$ and $b|a$, then $ar = b$ implies r is a unit.

Definition

- An irreducible element of R is a nonzero nonunit $x \in R$ such that $x = ab$ implies a or b is a unit.
- $x \in R$ is prime if x is a nonzero nonunit such that $p|ab$ implies $p|a$ or $p|b$.

Theorem Let R be a domain and $x \in R$ nonzero.

- x is prime implies (x) is a prime ideal.
- x is irreducible if and only if (x) is maximal among principal proper ideals
- x is prime implies x is irreducible (the converse holds if R is a PID).

Definition A unique factorization domain (UFD) is a domain satisfying

- If r is a nonzero nonunit element, then there exist $r_1, ..., r_k$ irreducible such that $r = r_1 \cdot ... \cdot r_k$
- This factorization is unique up to mult. by units.