I.
Group Theory

1.
Introduction to Groups

Groups

Group

Def'n 1.1. A ***group*** is an ordered pair $(G,\cdot)$ where

(a) G is a set; and

(b) $\cdot$ is an associative, unital binary operation on G such that every $g \in G$ is invertible.

G is ***abelian*** (or ***commutative***) if $\cdot$ is abelian. A group is ***finite*** if G is finite, and ***infinite*** if G is infinite. $|G|$ is called the ***order*** of G.

(1.1) Notations

Let $(G,\cdot)$ be a group.

(a) Usually we refer to $(G,\cdot)$ simply as G, where $\cdot$ is understood.

(b) Given any $g,h \in G$, we write gh to denote $g \cdot h$.

(c) The identity of G is denoted by e_G.

(d) For every $g \in G$, we write g^{-1} to denote the inverse of g. The function defined by $g \mapsto g^{-1}$ for every $g \in G$ is a unary operation on G. Moreover, this function is *bijective*.

Proof. Let $\varphi : G \to G$ be defined by

$$\varphi(g) = g^{-1}$$

for every $g \in G$. Then observe that

$$\varphi \circ \varphi = \mathrm{id}_G,$$

the identity function on G, since $\left(g^{-1}\right)^{-1} = g$. ∎

In fact, the above proof shows that φ is *idempotent* also.

(e) Given any $g \in G$, we write g^n to denote

$$\underbrace{gg\cdots g}_{n \text{ times}}$$

and g^{-n} to denote $(g^n)^{-1}$.

General Linear Group

Def'n 1.2. Let $\mathbb{K}$ be a field. Given $n \in \mathbb{N}$, we write $\mathrm{GL}_n(\mathbb{K})$ to denote the set of invertible $n \times n$ matrices with entries in $\mathbb{K}$. $\mathrm{GL}_n(\mathbb{K})$ under the usual matrix multiplication is called a ***general linear group***.

Proposition 1.1. *Let $n \in \mathbb{N}, n \geq 2$ and let $\mathbb{K}$ be a field. Then $\mathrm{GL}_n(\mathbb{K})$ is a group under the usual matrix multiplication.*

Proof. To see that $\mathrm{GL}_n(\mathbb{K})$ is a group, it suffices to observe that AB is invertible whenever $A,B \in \mathrm{GL}_n(\mathbb{K})$ are invertible, matrix multiplication is associative, and the identity matrix $I_n \in \mathrm{GL}_n(\mathbb{K})$ exists and is invertible. ∎

(1.2) Additive Notation

For groups like $(\mathbb{Z},+)$, it is confising to write mn instead of $m+n$, since mn already has another meaning in $\mathbb{Z}$. For abelian groups G, we often use *additive notation*, opposed to the *multiplicative notation* introduced in (1.1). In additive notation, given $g,h \in G$,

(a) we write the group operation as $g+h$;

(b) the identity of G is denoted as 0_G;

(c) the inverse of g is denoted by $-g$; and

(d) we write ng to denote

$$\underbrace{g+g+\cdots+g}_{n \text{ times}}$$

where $n \in \mathbb{N}$, and write $-ng$ to denote the inverse of ng.

Def'n 1.3. **Multiplication Table** of a Group

Let G be a group. The ***multiplication table***[a] of G is a table with rows and columns indexed by the elements of G. The cell for row g and column h contains the product gh.

[a] Although multiplication table is defined for any groups, it makes the most sense for finite (in particular small) groups.

(EX 1.3) Multiplication Table of $\mathbb{Z}/2\mathbb{Z}$

The multiplication table for $\mathbb{Z}/2\mathbb{Z}$ is

	0	1
0	0	1
1	1	0

.

Def'n 1.4. **Order** of an Element of a Group

Let G be a group and let $g \in G$. Then the ***order*** of g, denoted as $|g|$, is defined by

$$|g| = \min\left\{k \in \mathbb{N} : g^k = e_G\right\}$$

in case the set is nonempty. Otherwise, $|g| = \infty$.

(1.4) Properties of Order

Let $g \in G$.

(a) $|g| = 1$ if and only if $g = e_G$.

(b) If $g^n = e_G$, then $g^{n-1}g = gg^{n-1} = g^n = 1$, so $g^{n-1} = g^{-1}$. Thus, if $|g|$ is finite, then $g^{-1} = g^{|g|-1}$.

Proposition 1.2. *Let G be a group and let $g \in G$. Then $g^n = e$ if and only if $g^{-n} = e$.*

Proof. We have $g^{-n} = (g^n)^{-1}$. Since $\varphi : G \to G$ by $\varphi(h) = h^{-1}$ for all $h \in G$ is bijective,

$$g^n = e \iff (g^n)^{-1} = e^{-1} = e.$$

∎

Corollary 1.2.1. $|g| = \left|g^{-1}\right|$.

Dihedral Groups

Def'n 1.5. ***n*-gon**

Let $n \in \mathbb{N}, n \geq 3$. A regular polygon with n vertices, denoted as P_n, is called an ***n*-gon**.

(1.5) Fix $n \in \mathbb{N}, n \geq 3$ throughout this section. When we discuss about P_n, we imagine the complex plane, where we take

$$V = \left\{ v_i = e^{\frac{2\pi ik}{n}} : k \in \{0, \ldots, n-1\} \right\}$$

to be the set of the vertices, where we draw the edges by drawing the line segment from v_{k-1} to v_k for all $k \in \{1, \ldots, n\}$, where we define $v_n = v_0$.

Def'n 1.6. **Diheral Group**

A ***symmetry*** of P_n is $T \in \mathrm{GL}_2(\mathbb{R})$ such that $T(P_n) = P_n$. The set of symmetries of P_n, denoted as D_{2n}, is called a ***dihedral group***.

Proposition 1.3. *D_{2n} is a group under composition.*

The proof of Proposition 1.3 will be presented once we introduce subgroups.

Proposition 1.4.

(a) If $T \in D_{2n}$, then $T(v_0), T(v_1)$ are adjacent.[a]

(b) If $S, T \in D_{2n}$ and $S(v_i) = T(v_i)$ for every $i \in \{0, 1\}$, then $S = T$.

[a] Vertices of P_n are called ***adjacent*** if connected by a line segment.

Proof.

(a) It suffices to note that linear transformations map a line segment to a line segment. ◁

(b) Observe that v_0, v_1 are linearly independent. ■

Corollary 1.4.1. $|D_{2n}| \leq 2n$.

Proof. Let

$$A = \left\{ (v_i, v_j) : i, j \in \{0, \ldots, 4\}, |i - j| = 1 \right\},$$

the set of adjacent pairs, so $|A| = 2n$. Proposition 1.4 provides an injection from D_{2n} to A so $|D_{2n}| \leq |A| = 2n$. ■

(1.6) At the end of this section, we will prove that $|D_{2n}| = 2n$, that the injection provided by Proposition 1.4 is actually a bijection. Before this, let us discuss special elements of D_{2n}.

(a) Let $s \in D_{2n}$ be the *rotation* by $\frac{2\pi}{n}$, so $|s| = n$.

(b) Let $r \in D_{2n}$ be the *reflection* through the x-axis, so $|r| = 2$.

Now observe that, given any $j \in \{0, \ldots, n-1\}, k \in \{0,1\}$,

$$s^j(v_0) = v_i, s^j(v_1) = v_{i+1}$$

and

$$s^j r(v_0) = v_i, s^j r(v_1) = v_{i-1}.$$

Thus, we conclude the following.

Proposition 1.5. $D_{2n} = \left\{s^j r^k : j \in \{0, \ldots, n-1\}, k \in \{0,1\}\right\}$.

Corollary 1.5.1. $|D_{2n}| = 2n$.

It is also immediate that $rs = s^{-1}r$.

Permutatation Groups

(1.7) Let X be a set and let $\mathcal{F}(X,X)$ be the set of functions from X to X. We write S_X to denote

$$S_X = \{f \in \mathcal{F}(X,X) : f \text{ is bijective}\}.$$

Proposition 1.6. *Let X be a set. Then S_X is a group under the function composition.*

Def'n 1.7. **Symmetric Group**
Let $n \in \mathbb{N}$. A ***symmetric group*** S_n is the group S_X with $X = \{1, \ldots, n\}$. Elements of S_n are called ***permutations***.

(1.8) Permutations

Fix $n \in \mathbb{N}$ throughout. There are different ways to represent permutations. Suppose that $\sigma \in S_n$ is given.

(a) *two-line notation*:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 1 & 4 & 2 & 3 \end{pmatrix}.$$

(b) *one-line notation*: $\sigma = 651423$.

(c) *cycle notation*: $\sigma = (163)(25)(4) = (163)(25)$. Note that we typically omit cycles of length 1. [1]

Def'n 1.8. **Fixed Point, Support Set** of a Permutation
Let $\sigma \in S_n$ be a permutation.

(a) A ***fixed point*** of σ is $j \in \{1, \ldots, n\}$ such that $\sigma(j) = j$.

(b) The ***support set*** of σ, denoted as $\operatorname{supp}(\sigma)$, is defined as

$$\operatorname{supp}(\sigma) = \{1 \leq j \leq n : \sigma(j) \neq j\},$$

[1] Since identity is empty in cycle notation, we write e.

the set of points that are not fixed. If $\tau \in S_n$ is such that $\operatorname{supp}(\sigma) \cap \operatorname{supp}(\tau) = \varnothing$, then τ, σ are called ***disjoint***.

The numbers in $\operatorname{supp}(\sigma)$ are exactly the numbers that appear in the cycle notation of σ. Moreover, if $j \in \operatorname{supp}(\sigma)$, then $\sigma(j) \in \operatorname{supp}(\sigma)$.

Proposition 1.7. *If $\sigma, \tau \in S_n$ are disjoint, then σ, τ commute.*

Proof. Let $j \in \{1, \ldots, n\}$. We have three cases.

(a) If $j \in \operatorname{supp}(\sigma)$, then $\sigma(j) \in \operatorname{supp}(\sigma)$, so $j, \sigma(j) \notin \operatorname{supp}(\tau)$ since σ, τ are disjoint. It follows that

$$\sigma(\tau(j)) = \sigma(j) = \tau(\sigma(j)). \qquad \triangleleft$$

(b) If $j \in \operatorname{supp}(\tau)$, then we can repeat the argument in (a) to conclude that

$$\tau(\sigma(j)) = \tau(j) = \sigma(\tau(j)). \qquad \triangleleft$$

(c) If $j \notin \operatorname{supp}(\sigma) \cup \operatorname{supp}(\sigma)$, then

$$\sigma(\tau(j)) = j = \tau(\sigma(j)). \qquad \blacksquare$$

Def'n 1.9. *k*-**cycle** of a Symmetric Group

Given $k \in \mathbb{N}$, a ***k*-cycle** of S_n is an element of S_n with cycle notation $(a_1 \cdots a_k)$.

In fact, given any $\sigma \in S_n$ and the cycle notation

$$c_1 \cdots c_l$$

of σ, where $c_1, \ldots, c_l$ are the cycles of σ, the notation can be read as follows: multiply $c_1, \ldots, c_l$ as product in S_n. This means

$$\sigma^{-1} = (c_1 \cdots c_l)^{-1} = c_l^{-1} \cdots c_1^{-1} = c_1^{-1} \cdots c_l^{-1},$$

since c_j, c_k are disjoint for all $j, k \in \{1, \ldots, l\}, j \neq k$.

2. Subgroups and Homomorphisms

Subgroups

Subgroup of a Group

Def'n 2.1. Let G be a group. $H \subseteq G$ is called a ***subgroup*** if

(a) for all $g, h \in H, gh \in H$;

(b) $e_G \in H$; and

(c) for all $g \in H, g^{-1} \in H$.

We typically write $H \leq G$.

(EX 2.1) Consider D_{2n}, and let s be the rotation. Then

$$H = \left\{ s^k : k \in \{0, \dots, n-1\} \right\}$$

is a subgroup of D_{2n}. In fact, H is the smallest subgroup containing s, denoted as $H = \langle s \rangle$.

Trivial, Proper Subgroup

Def'n 2.2. Let G be a group.

(a) $\{e\}$ is called the ***trivial subgroup***.[a]

(b) A subgroup $H \leq G$ is called ***proper*** if $H \neq G$. We write $H < G$.

[a] It is very clear why $\{e\}$ is indeed a subgroup of G.

Proposition 2.1. *Let $(G, \cdot)$ be a group. Then $(H, \cdot|_{H \times H})$ is a group such that*

(a) $e_H = e_G$; and

(b) given any $g \in H$, the inverse of g in H is the same as the inverse of g in G.

Proof. It is clear that $\cdot|_{H \times H}$ is a binary operation on H by (a) of Def'n 2.1. For convenience, write $\star$ to denote $\cdot|_{H \times H}$. Since $\cdot$ is associative, $\star$ is associative. Also, it is clear that e_G is identity for $\star$. Moreover, if $g \in H$, then its inverse g^{-1} with respect to $\cdot$ is in H, where

$$g \star g^{-1} = g^{-1} \star g = e_G.$$

But we know that $e_G = e_H$, g^{-1} is the inverse of g with respect to $\star$. ∎

Operation Induced on a Subgroup

Def'n 2.3. Let $(G, \cdot)$ be a group and let $(H, \cdot|_{H \times H})$ be a subgroup of G. Then $\cdot|_{H \times H}$ is called the ***operation induced*** by $\cdot$ on H.

(2.2) Induced Operations

We usually refer to $\cdot|_{H \times H}$ as $\cdot$.

Proposition 2.2. Two-step Subgroup Test

Let G be a group. Then $H \subseteq G$ is a subgroup of G if and only if

(a) $H \neq \varnothing$; and

(b) for every $g, h \in H$, $gh^{-1} \in H$.

Proof.

- ($\Longrightarrow$) If H is a subgroup of G, then $e_G \in H$, so $H \neq \varnothing$. Also, if $g, h \in H$, then $h^{-1} \in H$, so $gh^{-1} \in H$. ◁
- By (a), there exists $h \in H$, and by (b), $hh^{-1} = e_G \in H$. So by (b) again, $e_G g^{-1} = g^{-1} \in H$ for every $g \in H$. Lastly, if $g, h \in H$, then $h^{-1} \in H$, so $gh = g\left(h^{-1}\right)^{-1} \in H$. ∎

Proposition 2.3. Finite Subgroup Test

Let G be a group and let $H \subseteq G$ be finite. Then H is a subgroup of G if and only if

(a) $H \neq \varnothing$; and

(b) for every $g, h \in H$, $gh \in H$.

Proof. The forward direction is clear. Suppose $g \in H$. Since H is finite, there must exist $j, k \in \mathbb{N}$, $j < k$ such that

$$g^j = g^k.$$

Let $n = k - j$. Then observe that $g^n = e_G$ so $e_G \in H$ and

$$g^{n-1} = g^{-1} \in H.$$

∎

Subgroups Generated by a Set

Proposition 2.4. Intersection of Subgroups Is a Subgroup

Let G be a group and let $\mathcal{F}$ be a nonempty collection of subgroups of G. Then

$$\bigcap_{H \in \mathcal{F}} H$$

is a subgroup of G.

Proof. For convenience denote the intersection by K. Since every $H \in \mathcal{F}$ is a subgroup of G, so $e_G \in H$ for every $H \in \mathcal{F}$. It follows that $e_G \in K$, so $k \neq \varnothing$. Now suppose that $g, h \in K$. Then

$$\begin{aligned} \forall H \in \mathcal{F}\,[g, h \in H] &\Longrightarrow \forall H \in \mathcal{F}\left[h^{-1} \in H\right] \\ &\Longrightarrow \forall H \in \mathcal{F}\left[gh^{-1} \in H\right] \\ &\Longrightarrow gh^{-1} \in K. \end{aligned}$$

Thus K is a subgroup of G by the subgroup test. ∎

Subgroup Generated by a Subset

Def'n 2.4. Let G be a group and let $S \subseteq G$. The ***subgroup generated by*** S in G, denoted as $\langle S\rangle$, is

$$\langle S\rangle = \bigcap_{S\subseteq H\leq G} H,$$

the intersection of every subgroup of G containing S.[a]

[a] Note that $\langle S\rangle$ is a subgroup by Proposition 2.4.

(2.3) $\langle S\rangle$ Observe that $\langle S\rangle$ is the smallest subgroup containing S, since any subgroup $H \subseteq G$ that contains S appears in the intersection. When we write out the elements of S, we often write

$$\langle s_1,\ldots,s_k\rangle,$$

where $S = \{s_1,\ldots,s_k\}$, instead of $\langle\{s_1,\ldots,s_k\}\rangle$ for convenience.

(2.4) Previously we said that

$$\langle s\rangle = \left\{s^k : k\in\{0,\ldots,n-1\}\right\} \leq D_{2n}.$$

First, $K = \left\{s^k : k\in\{0,\ldots,n-1\}\right\}$ is a subgroup of D_{2n} by the subgroup test, since $s\in K$ so $K\neq\varnothing$ and for every $g,h\in K, gh^{-1} = s^l$ for some $l\in\mathbb{Z}$, but

$$K = \left\{s^k : k\in\mathbb{Z}\right\}$$

since $s^n = e_{D_{2n}}$. But clearly any subgroup $H\leq D_{2n}$ that has s must contain K, so $K = \langle s\rangle$. Now we ask the following question: can we generalize this example to other cases? The answer is yes, and to see this, let us introduce the following notation: given any $S\subseteq G$, write S^{-1} to dentoe

$$S^{-1} = \left\{s^{-1} : s\in S\right\}.$$

Proposition 2.5. *Let G be a group and let $S\subseteq G$. Let*

$$K = \left\{\prod_{j=1}^{k} s_j : k\in\mathbb{N}\cup\{0\}, s_1,\ldots,s_k\in S\cup S^{-1}\right\}.$$

Then $\langle S\rangle = K$.[a]

[a] Observe that we are using the convention that the empty product is the identity.

Proof. We have two claims.

- *Claim 1*: $S\subseteq K\subseteq\langle S\rangle$.

  Proof. We know that the empty product $e_G\in\langle S\rangle$. The rest follows by induction. ◁

- *Claim 2*: *K is a subgroup.*

  Proof. Again, we know that the empty product $e_G\in\langle S\rangle$. Suppose $g,h\in K$, where

  $$g = s_1\cdots s_k, h = t_1\cdots t_l$$

  for some $k,l\in\mathbb{N}\cup\{0\}, s_1,\ldots,s_k,t_1,\ldots,t_l\in S\cup S^{-1}$. Then

  $$gh = s_1\cdots s_k t_1\cdots t_l\in K$$

by definition. Finally, $g^{-1} = s_k^{-1} \cdots s_1^{-1} \in K$ since $s_k^{-1}, \ldots, s_1^{-1} \in S \cup S^{-1}$, since $S \cup S^{-1}$ is closed under taking inverses. Thus K is a subgroup.[1] ◁

It is immediate from Claim 2 that $\langle S \rangle \subseteq K$. Thus $K = \langle S \rangle$, as desired. ∎

(2.5) Lattice of Subgroups

Let G be a group. Subgroups of G are ordered by set inclusion $\subseteq$. If $H_1, H_2 \leq G$ and $H_1 \subseteq H_2$, then $H_1 \leq H_2$, so we also write this order as $\leq$. The collection of subgroups of G together with (partial) order $\leq$ is called the ***lattice of subgroups*** of G. Given any $H_1, H_2 \leq G$, the ***subgroup below*** H_1, H_2 in the lattice is $H_1 \cap H_2$. The ***subgroup above*** H_1, H_2 is $\langle H_1 \cup H_2 \rangle$.

Cyclic Groups

Def'n 2.5. **Generator** of a Subgroup

Let G be a group and let $H \leq G$. $S \subseteq G$ is called a ***generator*** of H if $\langle S \rangle = H$. A group G is ***cyclic*** if $G = \langle g \rangle$ for some $g \in G$.

Proposition 2.6.

Let G be a group and let $g \in G$.

(a) $\langle g \rangle = \{g^j : j \in \mathbb{Z}\}$.

(b) If $|g| = n \in \mathbb{N}$, *then* $\langle g \rangle = \{g^j : j \in \{0, \ldots, n-1\}\}$.

Proposition 2.7.

Let G be a group and let $g \in G$. Then

$$|\langle g \rangle| = |g|.$$

Proof. Denote $H = \langle g \rangle$ for convenience. We already know that $|H| \leq |g|$ from Proposition 2.6. Suppose that $|G| = n \in \mathbb{N}$ without loss of generality. This means

$$a^0, \ldots, a^n$$

must have repetition: there are $j, k \in \{0, \ldots, n\}$ with $a^j = a^k$. This means $a^{k-j} = e_G$, so $|g| \leq n$, implying $|g| \leq |G|$. Thus $|g| = |G|$, as desired. ∎

Proposition 2.8.

Let G be a group and let $S \subseteq G$ be such that $\langle S \rangle = G$. Then, given any $T \subseteq G$,

$$G = \langle T \rangle$$

if and only if $S \subseteq \langle T \rangle$.

(2.6) Generators of $\mathbb{Z}/n\mathbb{Z}$

Let $n \in \mathbb{N}$ for the rest of this section, and consider the group $\mathbb{Z}/n\mathbb{Z}$. We know that $\mathbb{Z}/n\mathbb{Z} = \langle [1] \rangle$, so by Proposition 2.8, $\langle [a] \rangle = \mathbb{Z}/n\mathbb{Z}$ if and only if $[1] \in \langle [a] \rangle$, given any $a \in \mathbb{Z}$. But

$$[1] \in \langle [a] \rangle \iff \gcd(a, n) = 1,$$

so $\langle [a] \rangle = \mathbb{Z}/n\mathbb{Z}$ if and only if $\gcd(a, n) = 1$ (i.e. a is coprime to n).

[1] Note that we are directly using the definition of subgroup instead of the subgroup test here.

Proposition 2.9. *Let G be a group and let $g \in G$ be such that $g^n = e_G$. Then $|g| | n$.*

Proposition 2.10. *Suppose $a|n$, where $a \in \mathbb{N}$. Then $|[a]| = \frac{n}{a}$.*

Proof. Let $k \in \mathbb{N}$ be such that $n = ka$. Then $l[a] \neq 0$ for all $l \in \{1, \dots, k-1\}$. But

$$k[a] = [ka] = 0$$

so the order of $[a]$ is k. ∎

Proposition 2.11. *Let $a \in \mathbb{Z}$ and let $b = \gcd(a,n)$. Then $\langle [a] \rangle = \langle [b] \rangle$.*

Proof. Since $b|a$, there exists $k \in \mathbb{Z}$ such that $a = kb$. This means $[a] \in \langle [b] \rangle$, implying $\langle [a] \rangle \subseteq \langle [b] \rangle$. But by Bezout's lemma, there exist $x, y \in \mathbb{Z}$ such that

$$xa + yn = b.$$

So $[b] = x[a]$, implying $\langle [b] \rangle \subseteq \langle [a] \rangle$. Thus the result is established. ∎

Proposition 2.12. *Suppose $a \in \mathbb{Z}$. Then*

$$|[a]| = \frac{n}{\gcd(a,n)}.$$

Proof. Let $b = \gcd(a,n)$. Then $\langle [a] \rangle = \langle [b] \rangle$, so

$$|[a]| = |[b]| = \frac{n}{b} = \frac{n}{\gcd(a,n)}.$$

∎,

Corollary 2.12.1. *Let $n \in \mathbb{N}$.*

(a) The order of any cyclic subgroup of $\mathbb{Z}/n\mathbb{Z}$ divides n.

(b) For every $d \in \mathbb{N}$ that divides n, there exists a unique cyclic subgroup of $\mathbb{Z}/n\mathbb{Z}$ of order d, generated by $\left[\frac{n}{d}\right]$.

Proof.

(a) This follows immediately from Proposition 2.12. ◁

(b) For the existence part, first note that $\left|\left[\frac{n}{d}\right]\right| = d$ by Proposition 2.10. So $\left\langle \left[\frac{n}{d}\right] \right\rangle$ is a cyclic subgroup of $\mathbb{Z}/n\mathbb{Z}$ of order d. Moreover, given any $a \in \mathbb{Z}$ such that $\langle [a] \rangle = d$, by Proposition 2.12,

$$\gcd(a,n) = \frac{n}{d},$$

so by Proposition 2.11 $\langle [a] \rangle = \left\langle \left[\frac{n}{d}\right] \right\rangle$. ∎

Homomorphisms

Def'n 2.6. **Homomorphism** between Groups

Let G, H be groups. A function $\varphi : G \to H$ such that

$$\varphi(gh) = \varphi(g)\varphi(h)$$

for all $g, h \in G$ is called a (group) ***homomorphism***.

(2.7) Intuitively speaking, group homomorphisms are functions that *preserve the group structure*.

Proposition 2.13. Properties of Homomorphisms

Let G, H be groups and let $\varphi : G \to H$ be a homomorphism.

(a) $\varphi(e_G) = e_H$.

(b) $\varphi(g^n) = \varphi(g)^n$ for all $g \in G, n \in \mathbb{Z}$.

(c) $|\varphi(g)| \mid |g|$ for all $g \in G$.[a]

[a] We are following the convention that $n|\infty$ for all $n \in \mathbb{N}$.

Proof.

(a) Observe that

$$\varphi(e_G) = \varphi(e_G e_G) = \varphi(e_G)\varphi(e_G)$$

so $\varphi(e_G) = e_H$. ◁

(b) The result is clear for $n \in \mathbb{N}$ by induction. The case $n = 0$ follows from (a). So it suffices to show that

$$\varphi\left(g^{-1}\right) = \varphi(g)^{-1}.$$

But note that

$$\varphi\left(g^{-1}\right)\varphi(g) = \varphi\left(g^{-1}g\right) = \varphi(e_G) = e_H,$$

so it follows that $\varphi\left(g^{-1}\right) = \varphi(g)^{-1}$. ◁

(c) Without loss of generality assume that g has a finite order, say $|g| = n \in \mathbb{N}$. Then

$$\varphi(g)^n = \varphi(g^n) = \varphi(e_G) = e_H$$

by (a), (b), so it follows that $|\varphi(g)|$ is at most g. But if $|\varphi(g)|$ does not divide n, then $\varphi(g)^n = \varphi(g)^r$ for some $r < |\varphi(g)|$, implying that $\varphi(g)^n \neq e_H$, which is a contradiction. Thus $|\varphi(g)|$ divides n. ∎

Proposition 2.14.

Let G be a group and let $K \leq G$ with the induced operation from G. Then $\eta : K \to G$ by

$$\eta(g) = g$$

for every $g \in K$ is a homomorphism.

Proof. Observe that

$$\varphi(gh) = gh = \varphi(g)\varphi(h)$$

for every $g, h \in H$. ∎

Proposition 2.15. Composition of Homomorphisms

Let G, H, K be groups and let $\varphi : G \to H, \psi : H \to K$ be homomorphisms. Then $\psi \circ \varphi : G \to K$ is a homomorphism.

Proof. Let $g, h \in G$. Then

$$\psi(\varphi(gh)) = \psi(\varphi(g)\varphi(h)) = \psi(\varphi(g))\psi(\varphi(h)).$$ ∎

Corollary 2.15.1.

Let G, H be groups and let $K \leq G$. Let $\varphi : G \to H$ be a homomorphism. Then $\varphi|_K : K \to H$ is a homomorphism.

Proof. Let $g, h \in K$. Then

$$\varphi|_K(gh) = \varphi(gh) = \varphi(g)\varphi(h) = \varphi|_K(g)\varphi|_K(h).$$

Alternatively, observe that $\varphi|_K = \varphi \circ \eta$, where η is the homomorphism discussed in Proposition 2.14. ∎

Def'n 2.7. **Restriction** of a Homomorphism to a Subgroup

Consider the setting of Corollary 2.15.1. $\varphi|_K$ is called the ***restriction*** (homomorphism) of φ to K.

Proposition 2.16.

Let G, H be groups and let $\varphi : G \to H$ be a homomorphism. Let $K \leq G$. Then

$$\varphi(K) \leq H.$$

Proof. Since $K \neq \varnothing$, $\varphi(K) \neq \varnothing$. Moreover, given any $x, y \in \varphi(K)$, there are $g, h \in K$ such that

$$x = \varphi(g), y = \varphi(h).$$

So $xy^{-1} = \varphi(g)\varphi(h)^{-1} = \varphi\left(gh^{-1}\right) \in \varphi(K)$. Thus by the subgroup test the result follows. ∎

Def'n 2.8. **Image** of a Homomorphism

Let G, H be groups and let $\varphi : G \to H$ be a homomorphism. Then the ***image*** of φ, often denoted as $\text{image}(\varphi)$, is the subgroup $\varphi(G)$ of H.

Proposition 2.17.

Let G, H be groups and let $\varphi : G \to H$ be a homomorphism such that $\varphi(G) \leq K$ for some $K \leq H$. Then $\tilde{\varphi} : G \to K$ defined by

$$\tilde{\varphi}(g) = \varphi(g)$$

is also a homomorphism with $\tilde{\varphi}(G) = \varphi(G)$.

Proof. Observe that, given any $g, h \in G$,

$$\tilde{\varphi}(gh) = \varphi(gh) = \varphi(g)\varphi(h) = \tilde{\varphi}(g)\tilde{\varphi}(h).$$

Moreover, it is by definition that $\tilde{\varphi}(G) = \varphi(G)$. ∎

Corollary 2.17.1. *Let G,H be groups. Then any homomorphism $\varphi : G \to H$ induces a surjective homomorphism $\tilde{\varphi} : G \to K$, where $K = \varphi(G)$.*[a]

[a] We usually refer this surjective homomorphism $\tilde{\varphi}$ as φ for convenience.

Proposition 2.18. *Let G,H be groups and let $\varphi : G \to H$ be a homomorphism. Then*

$$\varphi(\langle S\rangle) = \langle \varphi(S)\rangle$$

for every $S \subseteq G$.

Proof. Observe that

$$\varphi\left(S^{-1}\right) = \left\{\varphi\left(s^{-1}\right) : s \in S\right\} = \left\{\varphi(s)^{-1} : s \in S\right\} = \varphi(S)^{-1}.$$

So

$$\begin{aligned}\varphi(\langle S\rangle) &= \varphi\left(\left\{\prod_{j=0}^{k} s_j : k \in \mathbb{N}\cup\{0\}, s_1, \ldots, s_k \in S \cup S^{-1}\right\}\right)\\ &= \left\{\prod_{j=0}^{k} \varphi(s_j) : k \in \mathbb{N}\cup\{0\}, s_1, \ldots, s_k \in S \cup S^{-1}\right\}\\ &= \left\{\prod_{j=0}^{k} t_j : k \in \mathbb{N}\cup\{0\}, t_1, \ldots, t_k \in \varphi(S) \cup \varphi(S)^{-1}\right\}\\ &= \langle \varphi(S)\rangle.\end{aligned}$$

■

Proposition 2.19. Preimage of a Subgroup under a Homomorphism Is a Subgroup

Let G,H be groups and let $\varphi : G \to H$ be a homomorphism. Then for every $K \leq H$,

$$\varphi^{-1}(K) \leq G.$$

Proof. Observe that $\varphi(e_G) = e_H \in K$, so $e_G \in \varphi^{-1}(K)$. Moreover, given any $g,h \in \varphi^{-1}(K)$, $\varphi(g), \varphi(h) \in K$, so

$$\varphi\left(gh^{-1}\right) = \varphi(g)\varphi(h)^{-1} \in K.$$

Thus $gh^{-1} \in \varphi^{-1}(K)$. ■

Def'n 2.9. **Kernel** of a Homomorphism

Let G,H be groups and let $\varphi : G \to H$ be a homomorphism. Then the ***kernel*** of φ, denoted as $\ker(\varphi)$, is the subgroup

$$\ker(\varphi) = \varphi^{-1}(\{e_H\}) \leq G.$$

Proposition 2.20. Characterization of Injectivity of a Homomorphism

Let G,H be groups and let $\varphi : G \to H$ be a homomorphism. Then φ is injective if and only if $\ker(\varphi) = \{e_H\}$.

Proof.

- ($\implies$) Since φ is a homomorphism, $\varphi(e_G) = e_H$, so if φ is injective, given any $g \in G$, $\varphi(g) = e_H$ if and only if $g = e_G$. Thus $\ker(\varphi) = \{e_G\}$. ◁

- Suppose that $\ker(\varphi) = \{e_G\}$, and let $g, h \in G$ be such that
$$\varphi(g) = \varphi(h),$$
where it suffices to show $g = h$. Then
$$\varphi\left(gh^{-1}\right) = \varphi(g)\varphi(h)^{-1} = e_H,$$
so $gh^{-1} \in \ker(\varphi)$. This means $gh^{-1} = e_G$, so $g = h$ as desired. ∎

Proposition 2.21.
Any Subgroup of a Cyclic Group Is Cyclic

Let G be a cyclic. Then for any $H \leq G$, H is cyclic.

Proof. We have the following three claims.

- *Claim 1*: *All subgroups of $\mathbb{Z}$ are of the form $m\mathbb{Z} = \langle m \rangle$, hence cyclic.*
- *Claim 2*: *Given any group K, K is cyclic if and only if there is a surjective homomorphism $\mathbb{Z} \to K$.*
- *Claim 3*: *If X, Y are sets, $f : X \to Y$ is a surjection, and $S \subseteq Y$, then $f\left(f^{-1}(S)\right) = S$.*

Since G is cyclic, there is a surjective homomorphism $\varphi : \mathbb{Z} \to G$ by Claim 2. Since all subgroups of $\mathbb{Z}$ are cyclic by Claim 1, there is $m \in \mathbb{Z}$ such that $\varphi^{-1}(H) = \langle m \rangle$. Let $\psi : \mathbb{Z} \to \mathbb{Z}$ be defined by
$$\varphi(k) = mk$$
for every $k \in \mathbb{Z}$, which is a homomorphism. Then $\varphi \circ \psi : \mathbb{Z} \to G$ is a surjective homomorphism with
$$\varphi(\psi(\mathbb{Z})) = \varphi(m\mathbb{Z}) = \varphi\left(\varphi^{-1}(H)\right) = H$$
by Claim 3. Therefore, by restricting the codomain of $\varphi \circ \psi$ to get a surjective homomorphism from $\mathbb{Z}$ to H. Thus by Claim 2 H is cyclic. ∎

Isomorphisms

Def'n 2.10.

Isomorphism between Groups

Let G, H be groups and let $\varphi : G \to H$ be a homomorphism. If φ is bijective, then we say φ is an ***isomorphism***.

Proposition 2.22.
Inverse of an Isomorphism Is an Isomorphism

Let G, H be groups and let $\varphi : G \to H$ be an isomorphism. Then $\varphi^{-1} : H \to G$ is also an isomorphism.

Proof. Since φ^{-1} is bijective, it suffices to show that φ^{-1} is a homomorphism. Let $g, h \in H$. Then
$$\varphi\left(\varphi^{-1}(g)\varphi^{-1}(h)\right) = \varphi\left(\varphi^{-1}(g)\right)\varphi\left(\varphi^{-1}(h)\right) = gh,$$
which means
$$\varphi^{-1}(g)\varphi^{-1}(h) = \varphi^{-1}(gh),$$
so φ^{-1} is homomorphic. ∎

Corollary 2.22.1. *Let G,H be groups and let $\varphi : G \to H$ be a homomorphism. Then φ is an isomorphism if and only if there exists a homomorphism $\psi : H \to G$ such that*

(a) $\psi \circ \varphi = e_G$; and

(b) $\varphi \circ \varphi = e_H$.

Def'n 2.11. **Isomorphic** Groups

Let G,H be groups. If there exists an isomorphism between G,H, then we say G,H are ***isomorphic***, denoted as $G \cong H$.

(2.8) $\cong$ is an equivalence relation. That is, given groups G,H,K,

(a) $G \cong H \implies H \cong G$;

(b) $G \cong H, H \cong K \implies G \cong K$; and

(c) $G \cong G$.

Proposition 2.23. *Let G,H be isomorphic groups. Then*

(a) $|G| = |H|$;

(b) G is abelian if and only if H is abelian;

(c) $|g| = |\varphi(g)|$ for all $g \in G$; and

(d) $K \subseteq G$ is a subgroup of G if and only if $\varphi(K)$ is a subgroup of H.

Proposition 2.24. Characterization of Isomorphic Cyclic Groups

Let G,H be cyclic groups. Then $G \cong H$ if and only if $|G| = |H|$.

Proof. Let $g \in G, h \in H$ be such that $G = \langle g \rangle, H = \langle h \rangle$.

- ($\implies$) This direction is clear. ◁
- ($\impliedby$) Suppose that $|G| = |H|$. Define $\varphi : G \to H$ so that

$$\varphi\left(g^j\right) = b^j$$

for every $j \in \mathbb{Z}$. Note that this φ is well-defined, since if $g^j = g^k$ for some $j,k \in \mathbb{Z}$, then $|g|\,|k-j$, so $|h|\,|k-j$, since we assumed $|G| = |H|$ so $|g| = |h|$. But this means $h^j = h^k$. To show that φ is homomorphic, let $j,k \in \mathbb{Z}$. Then

$$\varphi\left(g^j g^k\right) = \varphi\left(g^{j+k}\right) = h^{j+k} = h^j h^k = \varphi\left(g^j\right)\varphi\left(g^k\right).$$

To show that φ is invertible, observe that we can define $\psi : H \to G$ such that

$$\psi\left(h^j\right) = g^j$$

for every $j \in \mathbb{Z}$, where this ψ is a well-defined homomorphism via similar arguments, and it is clear that ψ is the inverse of φ. ∎

Corollary 2.24.1. Identification of Cyclic Groups

Let G be a cyclic group.

(a) If $|G| = \infty$, then $G \cong \mathbb{Z}$.

(b) If $|G| = n \in \mathbb{N}$, then $G \cong \mathbb{Z}/n\mathbb{Z}$.

Corollary 2.24.2. *Every cyclic group is abelian.*

Def'n 2.12. C_n

Let a be a formal indeterminate. We define

(a) $C_\infty = \left\{a^k : k \in \mathbb{Z}\right\}$, where $a^j a^k = a^{j+k}$ for every $j, k \in \mathbb{Z}$; and

(b) $C_n = \left\{a^k : k \in \mathbb{Z}/n\mathbb{Z}\right\}$, where $a^j a^k = a^{j+k}$ for every $j, k \in \mathbb{Z}/n\mathbb{Z}$.

(2.9) It is immediate that C_n's are groups under the given operations. C_n's are useful when we want to use multiplicative notation for cyclic groups. Note that

$$C_\infty \cong \mathbb{Z}, C_n \cong \mathbb{Z}/n\mathbb{Z}$$

for every $n \in \mathbb{N}$.

3.
Cosets and Product Groups

Cosets and Lagrange's Theorem

(3.1) Let G be a group and let $S \subseteq G$. Given any $g \in G$, we write gS to denote

$$gS = \{gh : h \in S\}$$

and Sg to denote

$$Sg = \{hg : h \in S\}.$$

In terms of additive notation, we write $g+S$ instead of gS and $S+g$ instead of Sg.

Def'n 3.1. **Left Coset, Right Coset** of a Subgroup

Let G be a group and let $H \leq G$. Given any $g \in G$, gH is called a ***left coset*** of H in G and Hg is called a ***right coset*** of H in G. If $gH = Hg$, we call gH a ***coset*** of H in G.[a]

[a] For abliean groups, left cosets are always right cosets and vice versa.

When $H \leq G$, we write G/H to denote

$$G/H = \{gH : g \in G\} \tag{3.1}$$

the *collection of left cosets* of H in G, and $H \setminus G$ to denote

$$H \setminus G = \{Hg : g \in G\},$$

the *collection of right cosets* of H in G.

(3.2) $\mathbb{Z}/n\mathbb{Z}$ So far we are writing $\mathbb{Z}/n\mathbb{Z}$ to denote the group whose elements are the equivalence classes under modulo n. It is worth pointing out that using the notation in [3.1] agrees with our previous usage of $\mathbb{Z}/n\mathbb{Z}$. That is, by using the notation in [3.1],

$$\mathbb{Z}n\mathbb{Z} = \{a+n\mathbb{Z} : a \in \mathbb{Z}\} = \{a+n\mathbb{Z} : 0 \leq a < n\} = \{[a] : 0 \leq a < n\},$$

so we again get the equivalence classes as the elements of $\mathbb{Z}/n\mathbb{Z}$. This motivates us the following question: *given a group G, for which $H \leq G$ is G/H a group?* We have to wait until the next chapter to answer this question.

Proposition 3.1. *Let G, K be groups and let $\varphi : G \to K$ be a homomorphism. Let $H = \ker(\varphi)$ and let $x_0 \in G, b \in K$ be such that $\varphi(x_0) = b$. Then*

$$\varphi^{-1}(\{b\}) = x_0H = Hx_0,$$

which is the solution set of the equation $\varphi(x) = b$.[a]

[a] We are taking x here to be a formal indeterminate.

Proof. We verify the result for the left cost x_0H; essentially same argument works for Hx_0. Suppose $\varphi(x) = b$ for some $x \in G$. Then

$$\varphi\left(x_0^{-1}x_1\right) = \varphi(x_0)^{-1}\varphi(x_1) = b^{-1}b = e_K.$$

So $x_0^{-1}x \in H$, which implies $x = x_0\left(x_0^{-1}x\right) \in x_0H$. Conversely, if $x = x_0h$ for some $h \in H$, then $\varphi(x) = \varphi(x_0)\varphi(h) = be_K = b$, so every element of x_0H is a solution. Thus $\varphi^{-1}(\{b\}) = x_0H$. ∎

Proposition 3.2. *Let G, K be groups and let $\varphi : G \to K$ be a homomorphism. Then there exists a bijection between $G/\ker(\varphi)$ and $\varphi(G)$.*

Proof. Suppose that $g\ker(\varphi) \in G/\ker(\varphi)$ is given. Then by Proposition 3.1, $g\ker(\varphi)$ is the set of solutions to $\varphi(x) = b$, where $b = \varphi(g)$. Therefore, $\varphi(g \cdot \ker(\varphi)) = \{b\}$, so $g\ker(\varphi)$ corresponds to b. Conversely, given any $b \in \varphi(G)$, b corresponds to $\varphi^{-1}(b)$. ∎

Def'n 3.2. Index of a Subgroup

Let G be a group and let $H \leq G$. The ***index*** of H in G, denoted as $[G : H]$, is

$$[G:H] = \begin{cases} |G/H| & \text{if } G/H \text{ is finite} \\ \infty & \text{otherwise} \end{cases}.$$

(3.3) First, let us consider the following question: *why do we use left cosets, not right cosets, for defining index?* It turns out to be a matter of choice (i.e. it does not matter if we used $H \setminus G$ instead of G/H in Def'n 3.2), as the following proposition shows.

Proposition 3.3. *Let G be a group and let $H \leq G$. Then $\varphi : G/H \to H \setminus G$ defined by*

$$\varphi(S) = S^{-1}$$

for every $S \in G/H$ is a bijection.

Theorem 3.4. Lagrange's Theorem

Let G be a group. For any $H \leq G$,

$$|G| = [G:H]\,|H|.$$

(3.4) We are going to discuss a proof of Lagrange's theorem shortly. Before that, let us look at some of the consequences of Lagrange's theorem.

Corollary 3.4.1. *If $x \in G$, then $|x|$ divides $|G|$.*

Proof. Observe that $|x| = |\langle x \rangle|$, which divides $|G|$. ∎

Corollary 3.4.2. *If $|G|$ is prime, then G is cyclic.*

Proof. Let $x \in G \setminus \{e_G\}$. Then $|x| \neq 1$, and $|x|$ divides $|G|$, so $|x| = |G|$ since $|G|$ is prime. Since $|\langle x \rangle| = |x| = |G|$, $G = \langle x \rangle$. ∎

Corollary 3.4.3. *Let K be a group and let $\varphi : G \to K$ be a homomorphism. Then $|\varphi(G)| = [G : \ker(\varphi)]$ and hence divides $|G|$.*

Proof. This is a direct consequence of Proposition 3.2, Theorem 3.4. ∎

Corollary 3.4.4. *Let K be a group such that G,K have coprime order. Then the only homomorphism from G to K is the trivial homomorphism.*[a]

[a] A homomorphism is called ***trivial*** if its image is the trivial subgroup.

Proposition 3.5. *Let G be a group and let $H \leq G$. Let $g,k \in G$. Then the following are equivalent.*

(a) $g^{-1}k \in H$.

(b) $k \in gH$.

(c) $gH = kH$.

(d) $gH \cap kH \neq \varnothing$.

Proof.

- (a) $\implies$ (b) If $g^{-1}k = h$ for some $h \in H$, then $k = gh \in gH$. ◁
- (b) $\implies$ (c) Suppose $k = gh$ for some $h \in H$. Then given any $h' \in H$, $kh' = g(hh') \in gH$, since $hh' \in H$. So $kH \subseteq gH$. Also, $g = kh^{-1} \in kH$, so $gH \subseteq kH$. ◁
- (c) $\implies$ (d) This is clear since $H \neq \varnothing$ so $gH \neq \varnothing$. ◁
- (d) $\implies$ (a) Let $x \in gH \cap kH$. Then $x = gh_1 = kh_2$ for some $h_1, h_2 \in H$, so $g^{-1}k = h_1 h_2^{-1} \in H$. ∎

Corollary 3.5.1. *G/H is a partition of G.*

Proof. Given any $g \in gH$, $g \in gH$. Consequently,

$$\bigcup G/H = G.$$

Now let $S,T \in G/H$, where we may assume $S \neq T$ without loss of generality. If $S \cap T \neq \varnothing$, then $S = T$ by (c), (d) of Proposition 3.5. So $S \cap T = \varnothing$. Thus G/H is a partition of G. ∎

Proposition 3.6. *Let G be a group and let $S \subseteq G$. Given any $g \in G$, $\varphi : S \to gS$ by*

$$\varphi(s) = gs$$

for every $s \in S$ is a bijection.

Proof. Observe that $\psi : gS \to S$ by

$$\psi(h) = g^{-1}h$$

for every $h \in gS$ is the inverse of φ. ∎

Proof of Lagrange's Theorem. If $|H| = \infty$ or $[G:H] = \infty$, then $|G| = \infty$, so assume $|H|, [G:H]$ are finite. By Proposition 3.6,

$$|gH| = |H|$$

for every $g \in G$. Since G/H is a partition of G by Corollary 3.5.1, G is a disjoint union of $[G:H]$ subsets, all of size $|H|$. Thus

$$|G| = [G:H]\,|H|,$$

as desired. ∎

Normal Subgroups

(3.5) By symmetry, we have the following proposition from Proposition 3.5.

Proposition 3.7. *Let G be a group and let $H \leq G$. Then given any $g,k \in G$, the following are equivalent.*

(a) $kg^{-1} \in H$.

(b) $k \in Hg$.

(c) $Hg = Hk$.

(d) $Hg \cap Hk \neq \varnothing$.

Proposition 3.8. *Let G be a group and let $H \leq G$. If $Hg = hH$ for some $g,h \in G$, then $gH = Hg$.*

Proof. Observe that

$$g \in Hg = hH,$$

so $gH = hH$. ∎

Def'n 3.3. **Normal** Subgroup
Let G be a group. A subgroup $N \subseteq G$ is called ***normal***, denoted as $N \trianglelefteq G$, if $gN = Ng$ for every $g \in G$.

Def'n 3.4. **Conjugate**
Let G be a group and let $g,h \in G$. Then the ***conjugate*** of h by g is ghg^{-1}.

Proposition 3.9. Characterizations of Normal Subgroups

Let G be a group and let $N \leq G$. Then the following are equivalent.

(a) $N \trianglelefteq G$.

(b) $gNg^{-1} = N$ *for all* $g \in G$.

(c) $gNg^{-1} \subseteq N$ *for all* $g \in G$.

(d) $G/N = N\backslash G$.

(e) $G/N \subseteq N\backslash G$.

(f) $N\backslash G \subseteq G/N$.

Proof.

- (1) $\Longleftrightarrow$ (2) Clearly (1) holds if and only if (2) holds. ◁

- (2) $\Longleftrightarrow$ (3) The forward direction is clear. To see the reverse direction, observe that if (c) is true, then given any $g \in G$,
$$N = g^{-1}\left(gNg^{-1}\right)g \subseteq g^{-1}Ng.$$ ◁

- (1) $\iff$ (4) Clearly (1) holds if and only if (4) holds. $\triangleleft$
- (4) $\implies$ (5), (6) Clearly (4) implies (5), (6). $\triangleleft$
- (5) $\implies$ (1) Suppose $G/N \subseteq N\setminus G$. Then for any $g \in G$, $gN = Hh$ for some $h \in G$, so $gN = Ng$ by Proposition 3.8. $\triangleleft$
- (6) $\implies$ (1) This can be proved similarly to (5) $\implies$ (1).

(3.6) Here are some remarks about normal subgroups.

(a) Let G be a group. If G is abelian, then every subgroup of G is normal.

(b) Let G, K be groups and let $\varphi : G \to K$ be a homomorphism. Then $\ker(\varphi)$ is normal.[1] We utilize (b) of Proposition 3.9 to prove this.

Proof. Given any $x \in \ker(\varphi)$ and $g \in G$, we have

$$\varphi\left(gxg^{-1}\right) = \varphi(g)\varphi(x)\varphi(g)^{-1} = \varphi(g)\varphi(g)^{-1} = e_K,$$

so $gxg^{-1} \in \ker(\varphi)$. Thus $g(\ker(\varphi))g^{-1} \subseteq \ker(\varphi)$ for all $g \in G$, so $N \trianglelefteq G$ by Proposition 3.9. $\triangleleft$

(c) $\trianglelefteq$ is not transitive. For instance, $H = \left\langle r, s^2 \right\rangle \trianglelefteq D_8$, and since H is abelian, $\langle r \rangle \trianglelefteq H$. But $\langle r \rangle$ is not a normal subgroup of D_8.

Normalizer of a Subset

Def'n 3.5. Let G be a group and let $S \subseteq G$. Then the ***normalizer*** of S in G, denoted as $N_G(S)$, is defined as

$$N_G(S) = \left\{g \in G : gSg^{-1} = S\right\}.$$

Proposition 3.10. *Let G be a group and let $S \subseteq G$. Then*

$$N_G(S) \leq G.$$

Proof. Since $e_G S e_G = S$, so $e_G \in N_G(S)$. Given any $g, h \in N_G(S)$,

$$ghS(gh)^{-1} = g\left(hSh^{-1}\right)g^{-1} = gSg^{-1} = S,$$

so $gh \in N_G(S)$. Moreover,

$$g^{-1}Sg = g^{-1}\left(gSg^{-1}\right)g = e_G S e_G = S,$$

so $g^{-1} \in N_G(S)$. ∎

Proposition 3.11. *Let G be a group and let $H \leq G$. Then $H \trianglelefteq G$ if and only if $N_G(H) = G$.*

[1] Note that this is a direct consequence of Proposition 3.1.

Corollary 3.11.1. *If $G = \langle S \rangle$, then given any $H \leq G$, $H \trianglelefteq G$ if and only if $gHg^{-1} = H$ for every $g \in S$.*

Proposition 3.12. *Let G be a group and let $H \leq G$. Then for any $g \in G$ of finite order, if $gHg^{-1} \subseteq H$, $g \in N_G(H)$.*

Proof. By induction $g^j H g^{-j} \subseteq H$ for every $j \in \mathbb{N} \cup \{0\}$. Denote $n = |g|$, so that $g^{-1}Hg = g^{n-1}Hg^{-(n-1)} \subseteq H$. This means $H \subseteq gHg^{-1}$, so $gHg^{-1} = H$. Thus $g \in N_G(S)$. ∎

Corollary 3.12.1. *Suppose G is finite and let $S \subseteq G$ be such that $G = \langle S \rangle$. Let $H \leq G$. If $gHg^{-1} \subseteq H$ for all $g \in S$, then $H \trianglelefteq G$.*

Def'n 3.6. **Center** of a Group

Let G be a group. The ***center*** of G, denoted as $Z(G)$, is defined as

$$Z(G) = \{g \in G : \forall h \in G[gh = hg]\}.$$

Proposition 3.13. *Let G be a group. Then*

$$Z(G) \trianglelefteq G.$$

Product Groups

Proposition 3.14. *Let $(G_1, \cdot_1), (G_2, \cdot_2)$ be groups. Then $G_1 \times G_2$ is a group under operation $\cdot$ defined as $(g_1, g_2) \cdot (h_1, h_2) = (g_1 \cdot_1 h_1, g_2 \cdot_2 h_2)$ for every $(g_1, g_2), (h_1, h_2) \in G_1 \times G_2$.*

Def'n 3.7. **Product** of Groups

Let G_1, G_2 be groups. Then the group $G_1 \times G_2$ with the operation described in Proposition 3.14 is called the ***product*** of G_1, G_2.

Proposition 3.15. *Let H, K be groups and let $G = H \times K$. Let*

$$\tilde{H} = \{(h, e_K) : h \in G\}, \tilde{K} = \{(e_H, k) : k \in K\}.$$

(a) $\tilde{H}, \tilde{K} \leq G$.

(b) $\varphi : H \to \tilde{H}, \psi : K \to \tilde{K}$ defined by

$$\varphi(h) = (h, e), \psi(k) = (e, k)$$

for every $h \in H, k \in K$ are isomorphisms.

(3.7) What Proposition 3.15 means we can think H, K as subgroups of $H \times K$.

Proposition 3.16. *Consider the setting of Proposition 3.16. For every $h \in \tilde{H}, k \in \tilde{K}$, $hk = kh$.*

Corollary 3.16.1. *If $\varphi : H \times K \to G$ is a homomorphism, then*

$$\varphi(h)\varphi(k) = \varphi(k)\varphi(h)$$

for all $h \in \tilde{H}, k \in \tilde{K}$.

Proposition 3.17. *Let G, H, K be groups and let $\alpha : H \to G, \beta : K \to G$ be homomorphisms. If*

$$\alpha(h)\beta(k) = \beta(k)\alpha(h)$$

for all $h \in H, k \in K$, then $\gamma : H \times K \to G$ defined by

$$\gamma((h,k)) = \alpha(h)\beta(k)$$

is a homomorphism.

Proof. Observe that, for all $h_1, h_2 \in H, k_1, k_2 \in K$,

$$\begin{aligned}\gamma((h_1,k_1)(h_2,k_2)) &= \gamma((h_1h_2, k_1k_2)) = \alpha(h_1h_2)\beta(k_1k_2)\\ &\alpha(h_1)\alpha(h_2)\beta(k_1)\beta(k_2) = \alpha(h_1)\beta(k_1)\alpha(k_2)\beta(k_2) = \gamma(h_1,k_1)\gamma(h_2,k_2).\end{aligned}$$ ∎

Corollary 3.17.1. *Let H, H', K, K' be groups and let $\alpha : H \to H', \beta : K \to K'$ be homomorphisms. Then $\gamma : H \times K \to H' \times K'$ by*

$$\gamma((h,k)) = (\alpha(h), \beta(k))$$

for all $(h,k) \in H \times K$ is a homomorphism.[a] *Moreover, if α, β are isomorphisms, then γ is an isomorphism.*

[a] We denote γ by $\alpha \times \beta$.

Corollary 3.17.2. *Let G be a group and let H be a trivial group. Then $\varphi : G \to G \times H$ by*

$$\varphi(g) = (g, e_H)$$

for all $g \in G$ is an isomorphism.

Proposition 3.18. *Let $p \in \mathbb{N}$ be prime. If G is a group of order p^2, then one of the following holds.*

(a) *G is cyclic.*

(b) $G \cong (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$.

Proposition 3.19. *Let G be a group and let $S,T \subseteq G$. Then $G = ST$ if and only if for every $g \in G$ there exist $h \in S, k \in T$ such that $g = hk$.*[a]

[a] ST denotes $\{hk : h \in S, k \in T\}$.

Proposition 3.20. *Let G be a group such that $G = HK$ for some $H,K \subseteq G$. Then for every $g \in G$ there exist unique $h \in H, k \in K$ such that $g = hk$ if and only if $H \cap K = \{e_G\}$, the trivial subgroup.*

Proof. The forward direction is clear. For the reverse direction, assume that $H \cap K = \{e_G\}$. Let $h, h' \in H, k, k' \in k$ be such that

$$hk = h'k'.$$

Then observe that $(h')^{-1} h = k'k^{-1} \in H \cap K$. So $(h')^{-1} h = k'k^{-1} = e_G$, which means $h = h', k = k'$. ∎

Def'n 3.8. **Internal Direct Product** of Subgroups

Let G be a group. We say G is the ***internal direct product*** of $H,K \leq G$ if

(a) $HK = G$;

(b) $H \cap K = \{e_G\}$; and

(c) $hk = kh$ for every $h \in H, k \in K$.

Theorem 3.21. *Let G be a group such that G is the internal direct product of $H,K \leq G$. Then $\varphi : H \times K \to G$ by*

$$\varphi((h,k)) = hk$$

for every $(h,k) \in G$ is an isomorphism.

Proof. Let $\varphi_H : H \to G, \varphi_K : K \to G$ by

$$\varphi_H(h) = h, \varphi_K(k) = k$$

for every $h \in H, k \in K$ are homomorphisms. Since G is the internal direct product of H,K, we have

$$\varphi_H(h)\varphi_K(k) = \varphi_K(k)\varphi_H(h)$$

for every $h \in H, k \in K$. So by Proposition 3.17, φ is a homomorphism. Moreover, every $g \in G$ can be uniquely written as $g = hk$ for some $h \in H, k \in K$ by Proposition 3.20, so φ is a bijection. ∎

Proposition 3.22. *Let G be a group such that G is the internal direct product of $H,K \leq G$. Then $H,K \trianglelefteq G$.*

Proof. Let $g \in G$, so write $g = hk$ for some $h \in H, k \in K$. Then

$$kHk^{-1} = \left\{khk^{-1} : h \in H\right\} = \left\{kk^{-1}h : h \in H\right\} = H,$$

so

$$gHg^{-1} = hkHk^{-1}h^{-1} = hHh^{-1} \subseteq H,$$

meaning $H \trianglelefteq G$. Similar proof holds for K. ∎

Proposition 3.23. *Let G be a group and let $H, K \leq G$. Then G is the internal direct product of H, K if and only if*

(a) $G = HK$;

(b) $H \cap K = \{e_G\}$; and

(c) $H, K \trianglelefteq G$.[a]

[a] Note that (c) is the only condition different from Def'n 3.8.

Def'n 3.9. **Commutator**

Let G be a group and let $g, h \in G$. Then the ***commutator*** of g, h, denoted as $[g, h]$, is defined as

$$[g,h] = ghg^{-1}h^{-1}.$$

Lemma 3.23.1. *Let G be a group and let $g, h \in G$. Then $[g, h] = e_G$ if and only if $gh = hg$.*

Proof of Proposition 3.23. The forward direction is clear. To show the reverse direction, let $h \in H, k \in K$. Then

$$[h,k] = \left(hkh^{-1}\right)k^{-1} \in K$$

since $K \trianglelefteq G$. Similarly

$$[h,k] = h\left(kh^{-1}k^{-1}\right) \in H$$

since $H \trianglelefteq G$. So $[h,k] \in H \cap K = \{e_G\}$, implying $[h,k] = e$. Thus by Lemma 3.23.1, $hk = kh$ for all $h \in H, k \in K$, as desired. ∎

4.
Quotient Groups

Quotient Groups

Proposition 4.1. *Let G be a group and let $H \leq G$. Then the relation R between $G/H \times G/H$ and G/H defined by*

$$([g],[h])\,R\,[gh]$$

is a function if and only if H is normal. Moreover, if H is normal, then $ghH = (gH)(hH)$, the setwise product.

Proof. Suppose that R is function and let $g \in G, h \in H$. Then

$$\left([g],\left[g^{-1}\right]\right) = [e_G].$$

Moreover,

$$\left([gh],\left[g^{-1}\right]\right) = \left[ghg^{-1}\right].$$

But $[g] = [gh]$, so $\left[ghg^{-1}\right] = [e]$ since R is a function. This means

$$ghg^{-1} \sim_H e_G,$$

meaning $ghg^{-1} \in H$, so $H \trianglelefteq G$. Conversely, suppose that H is normal. Then $h^{-1}Hh \subseteq H$, so

$$\left(h^{-1}Hh\right)H \subseteq H.$$

Since $e \in h^{-1}Hh$, so

$$\left(h^{-1}Hh\right)H = H.$$

Hence

$$(gH)(hH) = gh\left(h^{-1}Hh\right)H = ghH.$$

Now suppose that $S,T,U,U' \in G/H$ are such that

$$(S,T)\,RU, (S,T)\,RU'.$$

Then

$$U = ST = U',$$

so R is a function. ∎

Theorem 4.2. Universal Property of Quotients

Let G,K be groups and let $N \trianglelefteq G$. Let $\varphi : G \to K$ be a homomorphism and let $q : G \to G/N$ be the quotient homomorphism. Then there is a homomorphism $\psi : G/N \to K$ such that $\psi \circ q = \varphi$ if and only if $N \subseteq \ker(\varphi)$. Furthermore, if ψ exists, then it is unique.

Corollary 4.2.1. *Let G,K be groups and let $N \trianglelefteq G$. Then $q^* : \hom(G/N,K) \to \{\varphi \in \hom(G,K) : N \subseteq \ker(\varphi)\}$ by*

$$q^*(\psi) = \psi \circ q$$

for every $\psi \in \hom(G/N,K)$ is a bijection, where q is the quotient homomorphism.

Lemma 4.2.2. *Let S,T,U be sets and let $f:S\to T$ be surjective. Let $g_1,g_2:T\to U$. If $g_1\circ f=g_2\circ f$, then $g_1=g_2$.*

Proof. Let $t\in T$ be arbitrary. Then $s\in S$ such that $f(s)=t$. So

$$g_1(t)=g_1(f(s))=g_2(f(s))=g_2(t),$$

implying $g_1=g_2$. ∎

Proof of Theorem 4.2.

- ($\implies$) Suppose there exists $\psi:G/N\to K$ such that $\psi\circ q=\varphi$. Then given any $n\in N$, we have

  $$\varphi(n)=\psi(q(n))=\psi\left(e_{G/N}\right)=e_K,$$

  so $N\subseteq\ker(\varphi)$. ◁

- ($\impliedby$) Suppose $N\subseteq\ker(\varphi)$. Define $\psi:G/N\to K$ by

  $$\psi([g])=\varphi(g)$$

  for every $[g]\in G/N$. To show this ψ is well-defined, suppose that $[g]=[h]$ for some $g,h\in G$. Then $g^{-1}h\in N\subseteq\ker(\varphi)$, so

  $$\varphi(g)^{-1}\varphi(h)=\varphi\left(g^{-1}h\right)=e,$$

  so $\varphi(g)=\varphi(h)$. Hence $\psi([g])=\psi([h])$, implying that ψ is well-defined. Clearly

  $$\psi(q(g))=\psi([g])=\varphi(g)$$

  for all $g\in G$, so $\psi\circ q=\varphi$. To show that ψ is a homomorphism, observe that

  $$\psi([g][h])=\psi([gh])=\varphi(gh)=\varphi(g)\varphi(h)=\psi([g])\psi([h]).$$

  Since q is surjective, the uniqueness of ψ follows from Lemma 4.2.2.

The Isomorphism Theorems

Theorem 4.3. First Isomorphism Theorem

Let G,K be groups and let $\varphi:G\to K$ be a homomorphism. Then there exists isomorphism $\psi:G/\ker(\varphi)\to\varphi(G)$ such that $\varphi=\psi\circ q$, where $q:G\to G/\ker(\varphi)$ is the quotient homomorphism.

Proof. Clearly $\ker(\varphi)$ is a subset of itself, so by the universal property of quotients, there exists a homomorphism $\psi:G/\ker(\varphi)\to\varphi(G)$[1] such that $\psi\circ q=\varphi$, and in particular ψ is a surjection with $\psi([g])=\varphi(g)$ for every $g\in G$. Moreover, if $g\in G$ is such that $\psi([g])=e_K$, then $\varphi(g)=e_K$ so $g\in\ker(\varphi)$. This means $[g]=[e]$, implying that ψ is injective. Thus ψ is bijective, so an isomorphism. ∎

[1] Formally, the universal property guarantees the existence of $\psi:G/\ker(\varphi)\to K$ with such properties. However, since $\psi(G/\ker(\varphi))=\varphi(G)$ by definition, we can view ψ as a function to $\varphi(G)$.

Proposition 4.4. *Let G, H be groups and let $\varphi : G \to H$ be a homomorphism. Then*

(a) for every $G_1, G_2 \leq G$ such that $G_1 \leq G_2$, $f(G_1) \leq f(G_2)$; and

(b) for every $H_1, H_2 \leq H$ such that $H_1 \leq H_2$, $\varphi^{-1}(H_1) \leq \varphi^{-1}(H_2)$.

Proposition 4.5. *Let G, H be groups and let $\varphi : G \to K$ be a homomorphism. Then for every $H_1, H_2 \leq H$,*

$$\varphi^{-1}(H_1 \cap H_2) = \varphi^{-1}(H_1) \cap \varphi^{-1}(H_2).$$

Proposition 4.6. *Let G, H be groups and let $\varphi : G \to H$ be a surjective homomorphism. Then for every $K \leq H$,*

$$\varphi\left(\varphi^{-1}(K)\right) = K.$$

(4.1) Observe that Proposition 4.4, 4.5, 4.6 have (almost) nothing to do with the group theory; they are direct consequences of the properties of functions.

(4.2) Given a group G, write $\text{sub}(G)$ to denote the collection of subgroups of G. Now, suppose that we have groups G, H and a homomorphism $\varphi : G \to H$. Then φ induces a function $\varphi' : \text{sub}(G) \to \text{sub}(H)$. If this φ' is surjective, then we know that there is a left inverse $\varphi^* : \text{sub}(H) \to \text{sub}(G)$. Moreover, φ^* is injective. Now we have the following question: what is the image of φ^* in $\text{sub}(G)$?

Proposition 4.7. *Let G, H be groups and let $\varphi : G \to H$ be a homomorphism. Then*

(a) for every $K \leq H$, $\ker(\varphi) \leq \varphi^{-1}(K)$; and

(b) for every $K \leq G$ such that $\ker(\varphi) \leq K$, $\varphi^{-1}(\varphi(K)) = K$.

Proof.

(a) Observe that $\ker(\varphi) = \varphi^{-1}(\{e_H\}) \leq \varphi^{-1}(H)$. ◁

(b) Clearly $K \subseteq \varphi^{-1}(\varphi(K))$. Conversely, suppose that $y \in \varphi^{-1}(\varphi(K))$. Then $\varphi(y) \in \varphi(K)$, so $\varphi(y) = \varphi(k)$ for some $k \in K$. This means $\varphi\left(k^{-1}y\right) = e$, $k^{-1}y \in \ker(\varphi) \subseteq K$. Thus $y \in K$. ▮

Theorem 4.8. Correspondence Theorem / Fourth Isomorphism Theorem

Let G, H be groups and let $\varphi : G \to H$ be a surjective homomorphism. Write

$$\mathcal{F} = \{K \leq G : \ker(\varphi) \leq K\}.$$

(a) φ induces a bijection between $\mathcal{F}$, $\text{sub}(H)$ defined by

$$K \mapsto \varphi(K)$$

for every $K \in \mathcal{F}$.

(b) For every $K_1, K_2 \in \mathcal{F}$,

(i) $K_1 \leq K_2 \iff \varphi(K_1) \leq \varphi(K_2)$;

(ii) $\varphi(K_1 \cap K_2) = \varphi(K_1) \cap \varphi(K_2)$*; and*

(iii) $K_1 \trianglelefteq G \iff \varphi(K_1) \trianglelefteq H$.

Proof.

(a) Since φ is surjective, $\varphi\left(\varphi^{-1}(K')\right) = K'$ for every $K' \leq H$ by Proposition 4.6. Conversely, for every $K \in \mathcal{F}$, $\varphi^{-1}(\varphi(K)) = K$ by Proposition 4.7. Thus φ induces a bijection between $\mathcal{F}, K$. ◁

(b) (i) This follows from the fact that φ, φ^{-1} on subsets are bijections, so they preserve $\leq$.

(ii) Observe that

$$\varphi^{-1}(\varphi(K_1) \cap \varphi(K_2)) = \varphi^{-1}(\varphi(K_1)) \cap \varphi^{-1}(\varphi(K_2)) = K_1 \cap K_2,$$

since any pullback map preserves intersection. Hence

$$\varphi(K_1 \cap K_2) = \varphi\left(\varphi^{-1}(\varphi(K_1) \cap \varphi(K_2))\right) = \varphi(K_1) \cap \varphi(K_2).$$

(c) Homework. ∎

Corollary 4.8.1. Correspondence Theorem for Quotient Groups

Let G be a group and let $N \trianglelefteq G$. Let

$$\mathcal{F} = \{K \leq G : N \leq K\}.$$

(a) The quotient map $q : G \to G/N$ induces a bijection between $\mathcal{F}, \operatorname{sub}(H)$ by

$$K \mapsto q(K)$$

for every $K \in \mathcal{F}$.

(b) For every $K_1, K_2 \in \mathcal{F}$,

(i) $K_1 \leq K_2 \iff q(K_1) \leq q(K_2)$*;*

(ii) $q(K_1 \cap K_2) = q(K_1) \cap q(K_2)$*; and*

(iii) $K_1 \trianglelefteq G \iff q(K_1) \trianglelefteq G/N$.

Proof. This follows directly from Theorem 4.8 and the fact that the quotient map q is a surjective homomorphism. ∎

(4.3) Although we introduced Corollary 4.8.1 as a consequence of Theorem 4.8, we may proceed in the reverse direction also. From the first isomorphism theorem, given any surjective homomorphism $\varphi : G \to H$, where G, H are groups, we have $G/\ker(\varphi) \cong H$. Hence there is a bijection between $\operatorname{sub}(H)$ and $\operatorname{sub}(G/\ker(\varphi))$. Thus, when we combine the first isomorphism theorem with Corollary 4.8.1 (and the subgroup correspondence for isomorphisms), we obtain Theorem 4.8.

(4.4) Let G be a group, $N \trianglelefteq G$, and $K \leq G$ be such that $N \leq K$. Let $q_G : G \to G/N$ be the quotient map. Moreover, it is immediate that $N \trianglelefteq K$, so we also have the quotient map $q_K : K \to K/N$. Since $\ker(q_G \circ i_K) = N$, where $i_K : K \to G$ is the inclusion map (i.e. $i_K(k) = k$ for every $k \in K$), the first isomorphism theorem implies the existence of an isormorphism $\psi : K/N \to q_G \circ i_K(K)$. But $q_G \circ i_K(K) = q_G(K)$, so ψ is an isomorphism between $K/N, q_G(K)$ such that $\psi \circ q_K = q_G \circ i_K$. We summarize this result by the following proposition.

Proposition 4.9. *Let G be a group, $N \trianglelefteq G$, and $K \leq G$ be such that $N \leq K$. Let $q : G \to G/N$ be the quotient map. Then $\psi : K/N \to q(K)$ by*

$$\psi(kN) = kN$$

for every $kN \in K/N$ is an isomorphism.

Because of this isomorphism, we have the following notation: we denote the subgroup $q(K)$ corresponding to K in G/N by K/N.

Theorem 4.10. Third Isomorphism Theorem

Let G be a group and let $N, K \trianglelefteq G$ be such that $N \leq K$. Let

- *q_1 be the quotient map $G \to G/N$;*
- *q_2 be the quotient map $G/N \to (G/N)/(K/N)$; and*
- *q_1 be the quotient map $G \to G/K$.*

Then there is an isomorphism $\psi : G/K \to (G/N)/(K/N)$ such that $\psi \circ q_3 = q_2 \circ q_1$.

Proof. Note that

$$\ker(q_2 \circ q_1) = (q_2 \circ q_1)^{-1}\left(\left\{e_{(G/N)/(K/N)}\right\}\right) = q_1^{-1}\left(q_2^{-1}\left(\left\{e_{(G/N)/(K/N)}\right\}\right)\right) = q_1^{-1}(K/N) = K$$

by the correspondence theorem. Moreover, $q_2 \circ q_1(G) = (G/N)/(K/N)$, since both q_1, q_2 are surjective. Thus by the first isomorphism theorem, there exists an isomorphism $\psi : G/K \to (G/N)/(K/N)$ such that $\psi \circ q_3 = q_2 \circ q_1$. ∎

(4.5) When K is not normal, then G/K is not a group, so we cannot hope an analogous result to the third isomorphism theorem. However, we can still discuss about indexes: $[G : K], [G/N : K/N]$.

Proposition 4.11. *Let G be a group, $N \trianglelefteq G$, and $K \leq G$ be such that $N \leq K$. Then*

$$[G : K] = [G/N : K/N].$$

We can restate the above in terms of a surjective homomorphism, just as Theorem 4.8 and Corollary 4.8.1; the equivalence of Proposition 4.11, 4.12 is provided by the first isomorphism theorem.

Proposition 4.12. *Let G, H be groups and let $\varphi : G \to H$ be a surjective homomorphism. Then for every $K \leq G$ containing $\ker(\varphi)$, we have*

$$[G : K] = [H : \varphi(K)].$$

Proposition 4.13. *Define $f : G/K \to H/\varphi(K)$ by*

$$f(gK) = \varphi(g)\varphi(K)$$

for every $gK \in G/K$. To show that this f is well-defined, let $g, h \in G$ be such that $gK = hK$. Then $h^{-1}g \in K$, so

$$\varphi(h)^{-1}\varphi(g) = \varphi\left(h^{-1}g\right) \in \varphi(K),$$

implying $\varphi(g)\varphi(K) = \varphi(h)\varphi(K)$. Hence f is well-defined. Moreover, by the surjectivity of φ, f is surjective as well. To show that f is injective, let $gK, hK \in G/K$ be such that $f(gK) = f(hK)$. This means

$$\varphi(g)\varphi(K) = \varphi(h)\varphi(K).$$

Therefore

$$\varphi\left(h^{-1}g\right)=\varphi\left(h\right)^{-1}\varphi\left(g\right)\in\varphi\left(K\right),$$

so

$$h^{-1}g\in\varphi^{-1}\left(\varphi\left(K\right)\right)=K.$$

Hence $gK=hK$, implying that f is injective. Thus f is a bijection, and the result follows.

(4.6) We now move on to prove the second isomorphism theorem.

Proposition 4.14. *Let G be a group and let $H,K\leq G$. Then every element of HK can be written as hk for some unique $h\in H,k\in K$ if and only if $H\cap K=\{e_G\}$.*

By Proposition 4.14, if $H\cap K=\{e_G\}$, then $|HK|=|H|\,|K|$. But what is $|HK|$ if $H\cap K\neq\{e_G\}$? We note that

$$HK=\bigcup_{h\in H}hK,$$

a union of left cosets of K. So write

$$\mathcal{F}=\{hK:h\in H\}\subseteq G/K.$$

Then $\mathcal{F}$ is a partition of HK, so $|HK|=|X|\,|K|$. This brings us the next question: how large is X?

Proposition 4.15. *Let G be a group and let $H,K\leq G$. For every $h_1,h_2\in H$, $h_1K=h_2K$ if and only if $h_1\left(H\cap K\right)=h_2\left(H\cap K\right)$.*

Proof. Observe that

$$h_1K=h_2K\iff h_1^{-1}h_2\in K\iff h_1^{-1}h_2\in H\cap K\iff h_1\left(H\cap K\right)=h_2\left(H\cap K\right).$$ ∎

Corollary 4.15.1. *Consider the setting of Proposition 4.15. Then $\varphi:H/\left(H\cap K\right)\to X$ by*

$$\varphi\left(hH\cap K\right)=hK$$

is a bijection.

Proof. By Proposition 4.15 φ is well-defined and injective. But φ is clearly surjective also. ∎

Proposition 4.16. *Let G be a group and let $H,K\leq G$. Then*

$$|HK|\,|H\cap K|=|H|\,|K|.$$

(4.7) We may want to rephrase Proposition 4.16 in terms of indexes, just as Lagrange's theorem. In fact, by rearranging the equation,

$$[H:H\cap K]=|X|=\frac{|HK|}{|K|}.$$

However, the problem is HK may not be a group at all; the following proposition tells us when $HK\leq G$.

Proposition 4.17. *Let G be a group and let $H,K \leq G$. Then the following are equivalent.*

(a) $HK \leq G$.

(b) $HK = KH$.

(c) $KH \subseteq HK$.

Proof. Since (b) $\Longleftrightarrow$ (c) is clear, it suffices to show that (a) $\Longleftrightarrow$ (b). Suppose that $HK \leq G$ and fix $h \in H, k \in K$. Then $hk \in HK$, so $kh \in HK$ as well. Also $k^{-1}h^{-1} = (hk)^{-1} \in HK$, so $k^{-1}h^{-1} = h_0k_0$ for some $h_0 \in H, k_0 \in K$. Hence

$$hk = \left(k^{-1}h^{-1}\right)^{-1} = k_0^{-1}h_0^{-1} \in KH.$$

Hence we showed both inclusions $KH \subseteq HK, HK \subseteq KH$, implying (a) $\Longrightarrow$ (b). Conversely, suppose that $HK = KH$. Since $e_G \in H \cap K$, $e_G \in HK$. Moreover, given any $x, y \in HK$, we have

$$x = h_0k_0, y = h_1k_1$$

for some $h_0, h_1 \in H, k_0, k_1 \in K$. But we assumed $KH = HK$, so $x^{-1}h_1 = k_0^{-1}h_0^{-1}h_1 = h_2k_2$ for some $h_2 \in H, k_2 \in K$. Thus

$$x^{-1}y = \left(k_0^{-1}h_0^{-1}h_1\right)k_1 = h_2k_2k_1 \in HK,$$

as desired. ∎

Corollary 4.17.1. *Let G be a group and let $H,K \leq G$. If $KH \subseteq HK$, then $[H : H \cap K] = [HK : K]$.*

The next question to ask is: when is $KH \subseteq HK$? A sufficient condition would be

$$\forall h \in H \exists h' \in H \left[Kh = h'K\right].$$

This means there is an one-to-one correspondence between the left cosets and right cosets of H of the form kH, Hk for some $k \in K$, and surely this is more than enough. Since we know that $Kh = h'K$ implies $h'K = hK$, we can rephrase this as follows: $hKh^{-1} = K$ for every $h \in H$ or $H \subseteq N_G(K)$.

Corollary 4.17.2. *Let G be a group and let $H,K \subseteq G$. If $H \subseteq N_G(K)$, then $HK \leq G$. In particular,*

$$[H : H \cap K] = [HK : K].$$

Moreover, we can further investigate what else the condition $H \subseteq N_G(K)$ implies. We know that

$$hKh^{-1} = K, kKk^{-1} = K$$

for every $h \in H, k \in K$, so $H, K \subseteq N_{HK}(K)$. But $N_{HK}(K) \leq HK$ so we have $N_{HK}(K) = HK$. Hence $K \trianglelefteq HK$. Furthermore, for every $k \in H \cap K, h \in H$, we have

$$hkh^{-1} \in H \cap K$$

since $H \subseteq N_G(K)$ and $h, k \in H$. Therefore we also conclude that $H \cap K \trianglelefteq H$. But whenever we have a normal subgroup, its index is the order of the quotient group associated with it, which means the equation in Corollary 4.17.2 can be rewritten as

$$|H/(H \cap K)| = |HK/K|.$$

Since $H/(H \cap K), HK/K$ have the same order, we should really ask if there is an isomorphism between them. This is what the second isomorphism theorem is about.

Theorem 4.18. Second Isomorphism Theorem

Let G be a group and let $H, K \leq G$ be such that $H \subseteq N_G(K)$.

(a) $HK \leq G$.

(b) $K \trianglelefteq HK$.

(c) $H \cap K \trianglelefteq H$.

(d) Let $i_H : H \to HK$ *be the inclusion map and let* $q_1 : H \to H/(H \cap K), q_2 : HK \to HK/K$ *be the quotient maps. Then there exists an isomorphism* $\psi : H/H \cap K \to HK/K$ *such that* $\psi \circ q_1 = q_2 \circ i_H$.

Proof. We have shown (a), (b), (c) previously. Fix $h \in H, k \in K$. Then $hkK = hK$, so

$$HK/K = \{gK : g \in HK\} = \{hK : h \in H\}.$$

Hence

$$q_2 \circ i_H(H) = \{hK : h \in H\} = HK/K$$

and

$$\ker(q_2 \circ i_H) = i_H^{-1}\left(q_2^{-1}\left(\left\{e_{HK/K}\right\}\right)\right) = i_H^{-1}(K) = H \cap K.$$

Thus the result follows from the first isomorphism theorem. ∎

This page intentionally left blank.

5.
Group Actions

Group Actions

Def'n 5.1. **(Left) Action** of a Group on a Set

Let G be a group and let X be a set. A ***(left) action*** of G on X is a function $\cdot : G \times X \to X$ such that

(a) $e_G \cdot x = x$ for all $x \in X$; and

(b) $g \cdot (h \cdot x) = (gh) \cdot x$ for every $g, h \in G, x \in X$.

(EX 5.1) Examples of Group Actions

(a) For any $n \in \mathbb{N}$, S_n acts on $\{1, \ldots, n\}$.

(b) $\mathrm{GL}_n(\mathbb{F})$ acts on $\mathbb{F}^n$, where $\mathbb{F}$ is any field and $n \in \mathbb{N}$.

(c) Let X be any set and let G be any group. Then there always is an action $\cdot$ of G on X by

$$g \cdot x = x$$

for every $x \in X, g \in G$. This is called the ***trivial action*** of G on X.

(d) Let X be a set. The group S_X under composition $\circ$ acts on X via $f \cdot x = f(x)$.

Def'n 5.2. **Invariant** Subset

Let G be a group acting on a set X. A subset $Y \subseteq X$ is ***invariant*** under the action of G if $g \cdot y \in Y$ for every $g \in G, y \in Y$.

Proposition 5.1. *Let G be a group acting on a set X by $\cdot : G \times X \to X$ and let Y be an invariant subset of X. Then the restriction $\cdot|_{(G \times Y)} : G \times Y \to Y$ is an action on Y.*

Proposition 5.2. *Let G be a group acting on sets X, Y and for every $g \in G, f \in Y^X$, let $g \cdot_{Y^X} f : X \to Y$ be the function defined by*

$$x \mapsto g \cdot_Y f\left(g^{-1} \cdot_X x\right)$$

for every $x \in X$. Then $\cdot_{Y^X}$ is a left action of G on Y^X.

(5.2) Often we apply Proposition 5.2 with the trivial action $\cdot_Y$ on Y, so the action $\cdot_{Y^X}$ is such that

$$g \cdot_{Y^X} f(x) = f\left(g^{-1} \cdot_X x\right)$$

for every $x \in X$.

Proposition 5.3. *Let G be a group acting on a set X with $\cdot : G \times X \to X$. Then $\cdot$ induces an action of G on 2^X by*

$$g \cdot S = \{g \cdot s : s \in S\}$$

for every $S \subseteq X$.

(5.3) It is worth noting that every group *acts on itself*.

Proposition 5.4. *Let G be a group. Then G acts on itself. Specifically, $\cdot : G \times G \to G$ by*

$$g \cdot h = gh$$

for every $g, h \in G$ is a left action of G on G.

The action described in Proposition 5.4 is called the ***left regular action*** of G on G.

Proposition 5.5. *Let G be a group and let $H \leq G$. Then G acts on G/H by*

$$g \cdot (kH) = gkH$$

for every $g \in G, kH \in G/H$.

Observe that Proposition 5.5 generalizes Proposition 5.4, since $G/\{e_G\} \cong G$.

Permutation Representations

Proposition 5.6. *Let G be a group acting on a set X and given any $g \in G$, let $l_g : X \to X$ be defined by*

$$l_g(x) = g \cdot x$$

for every $x \in X$. Then

(a) $l_g \circ l_h = l_{gh}$ for every $g, h \in G$;

(b) l_{e_G} is the identity function on X; and

(c) l_g is a bijection.

Corollary 5.6.1. *Every left action of a group G on a set X defines a homomorphism $\varphi : G \to S_X$ such that*

$$\varphi(g)(x) = g \cdot x$$

for every $g \in G, x \in X$.

Def'n 5.3. **Permutation Representation** of a Group on a Set

Let G be a group acting on a set X. Then any homomorphism $\varphi : G \to S_X$ is called a ***permutation representation*** of G on X.

(5.4) Corollary 5.6.1 shows that every group acting on a set has a permutation representation in a canonical way. Moreover, the naming *permutation* comes from the fact that, if X is finite, say $|X| = n \in \mathbb{N}$, then $S_X \cong S_n$, which means any action on X defines a homomorphism to S_n.

Theorem 5.7. *Let G be a group and let X be a set.*

(a) *If G acts on X, then $\varphi : G \to S_X$ by*
$$\varphi(g)(x) = gx$$
for every $g \in G, x \in X$ is a homomorphism.

(b) *If $\varphi : G \to S_X$ is a homomorphism, then $gx = \varphi(g)(x)$ for every $g, \in G, x \in X$ defines a group action of G on X.*

Proof.

(a) See Corollary 5.6.1. ◁

(b) Observe that $e_G x = \varphi(e_G)(x) = x$ for every $x \in X$. Moreover, given any $g, h \in G, x \in X$, we have
$$g(hx) = \varphi(g)(\varphi(h)(x)) = (\varphi(g) \circ \varphi(h))(x) = \varphi(gh)x.$$ ∎

(5.5) Because of Theorem 5.7, we treat group actions and permutation representations interchangeably.

Def'n 5.4. **Kernel** of a Group Action

Let G be a group acting on a set X and let $\varphi : G \to S_X$ be the corresponding permutation representation.

(a) The ***kernel*** of the action is $\ker(\varphi)$.

(b) We say the action is ***faithful*** if $\ker(\varphi) = \{e_G\}$, the trivial subgroup.

Proposition 5.8. *Let G be a group acting on a set X. Then the action is faithful if and only if for every $g \in G \setminus \{e_G\}$, there exists $x \in X$ such that $gx \neq x$.*

Proof. This immediately follows from the definition of the kernel of a group action. ∎

(EX 5.6)

(a) Given any set X, S_X acts faithfully on X.

(b) The action of $\mathrm{GL}_n(\mathbb{K})$ on $\mathbb{K}^n$ by matrix multiplication is faithful.

(c) D_{2n} acts faithfully on vertices of the n-gon.

(d) Every trivial action is not faithful.

We previously saw that every group acts on some set, namely itself. Then, does every group act faithfully on some set?

Theorem 5.9. Cayley's Theorem

Let G be a group. Then G is isomorphic to a subgroup of S_G. In particular, if $|G| = n$, then G is isomorphic to a subgroup of S_n.

Lemma 5.9.1. *Let G be a group. Then the left regular action of G is faithful.*

Proof. For any $g \in G$ that is not the identity element, $ge_G = g \neq e_G$. Hence by Proposition 5.8 the left regular action is faithful. ▮

Proof of Theorem 5.9. By Lemma 5.9.1, the permutation representation $\varphi : G \to S_G$ corresponding to the left regular action is injective (since $\ker(\varphi)$ is trivial), implying that $G \cong \varphi(G) \leq S_G$ by the first isomorphism theorem. Moreover, when $|G| = n$, then $S_G \cong S_n$, so G is isomorphic to a subgroup of S_n. ▮

Def'n 5.5. **Left Regular Representation** of a Group
Let G be a group. Then the permutation representation corresponding to the left regular action of G on G is called the ***left regular representation*** of G.

Orbit

Def'n 5.6. **Orbit** of a Group on a Set
Let G be a group acting on a set X.

(a) Given $x \in X$, the G-***orbit*** of x, denoted as $\mathcal{O}_x$, is defined as

$$\mathcal{O}_x = \{gx : g \in G\}.$$

(b) A subset $\mathcal{O} \subseteq X$ is an ***orbit*** of G on X if there exists $x \in X$ such that $\mathcal{O} = \mathcal{O}_x$.

(c) A group action is ***transitive*** if there exists $x \in X$ such that $\mathcal{O}_x = X$.

(5.7) The point of the definition of the G-orbit of x is to define the *set of points that we can get to under the action of G from x.*

(EX 5.8)

(a) Let G be a group and let $H \leq G$ act on G by left multiplication. Then given any $g \in G$,

$$\mathcal{O}_g = Hg.$$

This action is transitive if and only if $H = G$.

(b) Let $n \in \mathbb{N}$ and consider the action of $\mathrm{GL}_n(\mathbb{K})$ on $\mathbb{K}^n$. Then

$$\mathcal{O}_{\mathbf{v}} = \begin{cases} \{\mathbf{0}\} & \text{if } \mathbf{v} = \mathbf{0} \\ \mathbb{K}^n \setminus \{\mathbf{0}\} & \text{if } \mathbf{v} \neq \mathbf{0} \end{cases}$$

for every $\mathbf{v} \in \mathbb{K}^n$.

Proposition 5.10. *Let G be a group acting on a set X. Then $\sim_G$[a] is an equivalence relation on X.*

[a] We write $x \sim_G y$ if there exists $g \in G$ such that $gx = y$ given any $x, y \in X$.

Corollary 5.10.1. *Let G be a group acting on a set X. Then orbits of G partition X. In particular, the action is transitive if and only if there is one orbit of G on X.*

Corollary 5.10.2. *Let G be a group acting on a set X and let $S \subseteq X$ be a set of representatives[a] for $\sim_G$. Then*

$$|X| = \sum_{x \in S} |\mathcal{O}_x|.$$

[a] We say $S \subseteq X$ is a ***set of representatives*** for $\sim_G$ if every equivalence class of $\sim_G$ has exactly one element of S. This exists by the axiom of choice.

(5.9) We also desire to know $|\mathcal{O}_x|$ given $x \in X$. To do so, we can use the mapping $g \mapsto gx$ for every $g \in G$. One problem, however, with this idea is that we may have distinct $g, h \in G$ such that $gx = hx$.

Def'n 5.7. **Stabilizer** of an Element of a Set

Let G be a group acting on a set X and let $x \in X$. Then the ***stabilizer*** of x, denoted as G_x, is

$$G_x = \{g \in G : gx = x\}.$$

Proposition 5.11. *Let G be a group acting on a set X. Then given any $x \in X$, $G_x \leq G$.*

Proof. Since $e_G x = x$, $e \in G_x$. Moreover, given any $g, h \in G_x$, observe that

$$\left(g^{-1}h\right)x = g^{-1}(hx) = g^{-1}x$$

but $\left(g^{-1}x\right)gx = e_G$ and $gx = e_G$ so $g^{-1}x = e_G$. Hence $g^{-1}h \in G_x$. ∎

Theorem 5.12. Orbit-stabilizer Theorem

Let G be a group acting on a set X. Then given any $x \in X$, $\varphi : G/G_X \to \mathcal{O}_x$ by

$$\varphi(gG_x) = gx$$

for every $g \in G$ is a bijection.

Proof. Given any $g, h \in G$ such that $gG_x = hG_x$, $g^{-1}h \in G_x$. So it follows that

$$g^{-1}hx = x,$$

implying $hx = gx$, so φ is well-defined. Moreover, if $g, h \in G$ are such that $gx = hx$, then $g^{-1}h \in G_x$ so $gG_x = hG_x$. The surjectivity is clear. ∎

Corollary 5.12.1. *Let G be a group acting on a set X. Then given any $x \in X$, $|\mathcal{O}_x| = [G : G_x]$.*

(EX 5.10) Let $G = S_n, X = \{1, \ldots, n\}$. We know that the action of G on X is transitive, so $\mathcal{O}_i = X$ for any $i \in X$. It follows that

$$n = |\mathcal{O}_i| = [G : G_i] = \frac{|G|}{|G_i|} = \frac{n!}{|G_i|}$$

for all $i \in X$, implying

$$|G_i| = (n-1)!.$$

In fact,

$$G_i = \{\pi \in S_n : \pi(i) = i\} \cong S_{n-1}$$

for every $i \in X$.

Proposition 5.13. *Let G be a group and let $H \leq G$. Then the left multiplication action of G on G/H is transitive and $G_H = H$.*

(5.11) Observe that, given a group G acting on a set X, the kernel of action can be written as

$$\{g \in G : \forall x \in X \, [gx = x]\}$$

whereas $G_x = \{g \in G : gx = x\}$ for every $x \in X$. Consequently, the kernel of the action is a subgroup of G_x for every $x \in X$. Moreover, we have the following result.

Proposition 5.14. *Let G be a group acting on a set X. Then the kernel of the action is $\cap_{x \in X} G_x$, the intersection of stabilizers.*

Theorem 5.15. *Let G be a finite group. Then for every $H \leq G$ such that $[G : H]$ is the smallest prime dividing $|G|$, then $H \trianglelefteq G$.*

Proof. Let $K \leq G$ be the kernel of action of G on G/H. Then by Proposition 5.13, 5.14, $K \leq G_H = H$. Denote

$$k = [H : K] = \frac{|H|}{|K|}, p = [G : H].$$

Now

$$[G : K] = \frac{|G|}{|K|} = \frac{|G|}{|H|}\frac{|H|}{|K|} = pk,$$

By Cayley's theorem, G/K is isomorphic to a subgroup of S_p. So

$$kp | p!$$

by Lagrange's theorem, since $|G/K| = kp, |S_p| = p!$. It follows that

$$k | (p-1)!.$$

But $k | |G|$. Since p is the smallest prime dividing $|G|$, it follows that $K = 1$. Thus $|H| = |K|$ so $H = K$, a normal subgroup of G. ∎

Conjugation

(5.12) Recall that given any group G, left multiplication defines a left action of G on G. It turns out that there is another natural left action.

Proposition 5.16. Conjugation Action

Let G be a group. Then

$$(g,h) \mapsto ghg^{-1}$$

for every $g,h \in G$ defines an action of G on G.

Proof. For every $g \in G$, observe that $e_G \cdot k = e_G k e_G = k$. Moreover, for every $g,h,k \in G$,

$$g \cdot (h \cdot k) = g \cdot hkh^{-1} = ghkh^{-1}g^{-1} = (gh)k(gh)^{-1} = (gh) \cdot k. \qquad ∎$$

Def'n 5.8. **Conjugation Action** of a Group on Iteslf

Let G be a group. Then the action $\cdot$ described in Proposition 5.16 is called the ***conjugation action*** of G on G.

Def'n 5.9. **Conjugacy Class, Centralizer** of an Element of a Group

Let G be a group. Given any $g \in G$,

(a) the ***conjugacy class*** of k in G, denoted $\text{conj}_G(g)$, is defined as the orbit of k under the conjugation action; and

(b) the ***centralizer*** of k in G, denoted as $C_G(g)$, is defined as the stabilizer of k under the conjugation action.

(5.13) Observe that, given $k \in G$,

$$\text{conj}_G(k) = \left\{gkg^{-1} : g \in G\right\}$$

and that

$$C_G(k) = \left\{g \in G : gkg^{-1} = k\right\}.$$

That is, the centralizer of any $k \in G$ is the set of elements in G commute with k. Furthermore, by the orbit stabilizer theorem,

$$|\text{conj}_G(k)| = [G : C_G(k)]$$

for every $k \in G$.

(5.14) The conjugation action of G on G induces an action of G on 2^G. Moreover, suppose $g \in G, S \subseteq G$ are given. Then

$$g \cdot S = \{g \cdot h : h \in S\} = \left\{ghg^{-1} : h \in S\right\} = gSg^{-1}.$$

So the stabilizer of S is $\left\{g \in G : gSg^{-1} = S\right\} = N_G(S)$, the normalizer of S in G.

(EX 5.15) An important instance of the conjugation action is the general linear group, acting on the set of matrices by the conjugation action. Recall that, $A, B \in M_{n\times n}(\mathbb{K})$ $(n \in \mathbb{N})$ are called ***similar*** if there exists $C \in \text{GL}_n(\mathbb{K})$ such that

$$CAC^{-1} = B.$$

This is the equivalence relation $\sim_{\text{GL}_n(K)}$. Orbits of conjugation of $\text{GL}_n(\mathbb{K})$ on $M_n(\mathbb{K})$ are called ***similarity classes***. Moreover, $A \in M_{n\times n}(\mathbb{K})$ is called ***diagonalizable*** if it is similar to a diagonal matrix (i.e. the similarity class of A contains a diagonal matrix). When $\mathbb{K} = \mathbb{C}$, by the Jordan normal form theorem, every similarity class has exactly one matrix in Jordan normal form (up to permutation of Jordan blocks). Hence matrices in Jordan normal form give a set of representatives for $\sim_{\text{GL}_n(\mathbb{K})}$.

Proposition 5.17. *Let G be a group. Then for any $k \in G$, the following are equivalent:*

(a) $|\operatorname{conj}_G(k)| = 1$;

(b) $C_G(k) = G$; *and*

(c) $k \in Z(G)$.

Proof. Observe that

$$|\operatorname{conj}_G(k)| = 1 \iff \forall g \in G\left[gkg^{-1} = k\right] \iff C_G(k) = G \iff k \in Z(G). \qquad \blacksquare$$

Theorem 5.18. Class Equation

Let G be a finite group. Then

$$|G| = |Z(G)| + \sum\nolimits_{g\in T} |\operatorname{conj}_G(g)|,$$

where T is a set of representatives for conjugacy classes not in the center.

Proof. Observe that

$$|G| = \sum\nolimits_{g\in S} |\operatorname{conj}_G(g)|$$

for any set $S \subseteq G$ of representatives of the conjugacy classes by Corollary 5.10.2. But by Proposition 5.17, $g \in Z(G)$ if and only if $|\operatorname{conj}_G(g)| = 1$, so every element $g \in Z(G)$ is the representative of the conjugacy class $\{g\}$. It follows that $Z(G) \subseteq S$, so by defining $T = S \setminus Z(G)$,

$$|G| = \sum\nolimits_{g\in S} |\operatorname{conj}_G(g)| = \sum\nolimits_{g\in \operatorname{conj}_G(g)} |\operatorname{conj}_G(g)| + \sum\nolimits_{g\in T} |\operatorname{conj}_G(g)| = |Z(G)| + \sum\nolimits_{g\in T} |\operatorname{conj}_G(g)|. \qquad \blacksquare$$

Theorem 5.19. Cauchy's Theorem

Let G be a finite group. Then for any prime $p \in \mathbb{N}$ dividing $|G|$, there exists an element of G of order p.

Proof. Let $m \in \mathbb{N}$ be such that $|G| = pm$. Note that the result is provided by Corollary 2.12.1 when G is cyclic. We first verify the result for the case which G is abelian.

- *Claim 1. The result holds when G is abelian.*

  Proof. We induct on m. When $m = 1$, G has a prime order so cyclic, so has an element of order p. Let $m \in \mathbb{N}, m \geq 2$ and suppose that every group of order $p, 2p, \ldots, (m-1)p$ has an element of order p. Let $a \in G \setminus \{e_G\}$, where we may assume that $|a| < |G|$ (otherwise we are done). If $p \mid |a|$, then by the inductive hypothesis we have $b \in \langle a \rangle$ with $|b| = p$. In case p does not divide the order of a, we use the fact that every subgroup of an abelian group is normal. So denote

  $$N = \langle a \rangle \trianglelefteq G.$$

  Then

  $$|G/N| = \frac{|G|}{|n|} < |G|.$$

  Since p divides $|G|$ but not $|N|$, p divides $|G/N|$. Therefore by induction G/N has element gN of order p. Let $n = |g|$. Since $g^n = e_G$, $q(g)^n = gN = e_G$ where $q : G \to G/N$ is the quotient map. This means $p|n$. Now if $\langle g \rangle = G$, then we are done. Otherwise, $|\langle g \rangle| < |G|$ but p divides $|\langle g \rangle|$, so $\langle g \rangle$ has an element of order p by the inductive hypothesis. ◁

We proceed inductively on $|G|$. If $|G| = p$ then we are done. Now suppose that the result holds for every group of order $p, 2p, \ldots, (m-1)p$, where $m \in \mathbb{N}, m \geq 2$. Let T be a set of representatives for the conjugacy classes not in $Z(G)$. Then by the class equation

$$|G| = |Z(G)| + |\mathrm{conj}_G(g)|.$$

If p does not divide $|\mathrm{conj}_G(g)|$ for some $g \in G$, then $p|C_G(g)$ since $|\mathrm{conj}_G(g)| = \frac{|G|}{|C_G(g)|}$. Since $g \notin Z(G)$ and $|\mathrm{conj}_G(g)| > 1$, $|C_G(g)| < |G|$. Hence by induction $C_G(g)$ contains an element of order p. On the other hand, if p divides $|\mathrm{conj}_G(g)|$ for every $g \in T$, then p divides $|Z(G)|$. But $Z(G)$ is abelian, so has an element of order p by Claim 1. ∎

p-group

Def'n 5.10. Let $p \in \mathbb{N}$ be prime. A group G is called a ***p*-group** if $|G| = p^k$ for some $k \in \mathbb{N}$.

Theorem 5.20. *For every p-group G, $Z(G) \neq \{e_G\}$.*

Proof. Let T be a set of representatives for the conjugacy classes not in $Z(G)$. Then by the class equation

$$|G| = |Z(G)| + \sum\nolimits_{g \in T} [G : C_G(g)].$$

But $[G : C_G(g)]$ divides $|G|$, and for any $g \in T$, since $g \notin Z(G)$, $[G : C_G(g)] > 1$, implying that p divides $[G : C_G(g)]$ for every $g \in T$. Thus p divides $|Z(G)|$ also, implying that $Z(G)$ is nontrivial. ∎

6.
Classification of Groups

Classification of Groups

Proposition 6.1. *For every group G such that $|G| = p^2$ for some prime $p \in \mathbb{N}$, exactly one of the following holds.*

(a) G is cyclic.

(b) $G \cong (\mathbb{Z}/p\mathbb{Z})^2$.

Proof. Clearly (a), (b) exclude each other. Now suppose that G is not cyclic, and fix $a \in G \setminus \{e_G\}$. Since G is not cyclic and a is not the identity, $|a| = p$. So fix $b \in G \setminus \langle a \rangle$, where we know $|b| = p$ as well. Now denote

$$H = \langle a \rangle, K = \langle b \rangle.$$

Since $H \cap K < K$, $|H \cap K| = 1$, so $H \cap K = \{e_G\}$. Moreover,

$$|HK| = \frac{|H|\,|K|}{|H \cap K|} = p^2,$$

so $HK = G$. Also, $[G : H] = [G : K] = p$, the smallest prime dividing $|G|$, so $H, K \trianglelefteq G$. Hence G is an internal direct product of H, K, implying that

$$G \cong H \times K \cong (\mathbb{Z}/p\mathbb{Z})^2. \blacksquare$$

(6.1) We can generalize an argument that appeared in the proof of Proposition 6.1.

Proposition 6.2. *Let G be a group and let $H, K \trianglelefteq G$ be such that $\gcd(|H|, |K|) = 1, |H|\,|K| = |G|$. Then $G \cong H \times K$.*

Proof. Since $|H \cap K|$ divides both $|H|, |K|$, $|H \cap K| = 1$. So $H \cap K = \{e_G\}$. Moreover,

$$|HK| = \frac{|H|\,|K|}{|H \cap K|} = |G|,$$

so $HK = G$. Thus it follows that $G \cong H \times K$. $\blacksquare$

Classification of Finite Abelian Groups

Proposition 6.3. *Let G be an abelian group and for every $m \in \mathbb{N}$, write $G^{(m)}$ to denote*

$$G^{(m)} = \{g \in G : g^m = e_G\}.$$

Then $G^{(m)} \leq G$ for all $m \in \mathbb{N}$.

Proof. Clearly $e_G \in G^{(m)}$ for every $m \in \mathbb{N}$. Moreover, given any $g, h \in G^{(m)}$,

$$\left(g^{-1}h\right)^m = g^{-m}h^m = e_G. \blacksquare$$

Def'n 6.1. ***m*-torsion Subgroup** of an Abelian Group

Let G be an abelian group. For every $m \in \mathbb{N}$, the ***m*-tortion subgroup** of G, denoted as $G^{(m)}$, is defined as

$$G^{(m)} = \{g \in G : g^m = e_G\}.$$

Proposition 6.4. *Let G be a finite abelian group with $|G| = mn$ for some $m, n \in \mathbb{N}$ such that $\gcd(m,n) = 1$. Then*

(a) $\varphi : G \to G^{(m)} \times G^{(n)}$ defined by

$$\varphi(g) = (g^n, g^m)$$

for every $g \in G$ is an isomorphism; and

(b) $\left|G^{(m)}\right| = m, \left|G^{(n)}\right| = n$.

Proof.

(a) Let $g \in G$. Then $g^{mn} = e_G$, so $g^n \in G^{(m)}$ and $g^m \in G^{(n)}$ so φ is well-defined. Moreover, since n, m are coprime, there exist $a, b \in \mathbb{Z}$ such that

$$an + bm = 1$$

by Bezout's lemma. Given any $h \in G$, if $\varphi(h) = e_G$, then $h^n = h^m = e_G$, implying that

$$h = h^{an+bm} = e_G,$$

so φ is injective. Furthermore, suppose $g \in G^{(m)}, h \in G^{(n)}$ are given. Then

$$g^{an} = g^{an+bm} = g$$

and

$$h^{bm} = h^{an+bm} = h$$

so

$$\varphi\left(g^a h^b\right) = \left(g^{an} h^{bm}, g^{am} h^{bm}\right) = (g, h),$$

implying that φ is surjective. Lastly, given any $g, h \in G$,

$$\varphi(gh) = (g^n h^n, g^m h^m) = (g^n, g^m)(h^n, h^m) = \varphi(g)\varphi(h),$$

so φ is a homomorphism. Thus φ is an isomorphism, as required. ◁

(b) Since $G \cong G^{(m)} \times G^{(n)}$,

$$|G| = \left|G^{(m)}\right| \left|G^{(n)}\right|.$$

Let

$$|G| = \prod_{j=1}^{k} p_j^{a_j}$$

be the prime factorization of $|G|$, where $p_1, \ldots, p_k \in \mathbb{N}$ are distinct primes and $a_1, \ldots, a^k \in \mathbb{N}$. Since $|G| = mn$ and m, n are coprime,

$$n = \prod_{j=1}^{k} p_j^{b_j}, m = \prod_{j=1}^{k} p_j^{c_j}$$

for some $b_1, \ldots, b_k, c_1, \ldots, c_k \in \mathbb{N}$ such that $a_j = b_j + c_j$ and exactly one of b_j, c_j is nonzero for every $j \in \{1, \ldots, k\}$. Fix $j \in \{1, \ldots, k\}$ and suppose $b_j = a_j$. If we assume p_j divides $\left|G^{(n)}\right|$ for the sake of contradiction, then by Cauchy's theorem $G^{(n)}$ has an element a of order p_j. But

$$p_j | m \implies a \in G^{(m)} \implies a \in \ker(\varphi) \implies a = e_G,$$

which is a contradiction. Hence p_j divides $\left|G^{(m)}\right|$, and in conclusion m divides $\left|G^{(m)}\right|$ and n divides $\left|G^{(n)}\right|$. Thus $\left|G^{(m)}\right| = m, \left|G^{(n)}\right| = n$. ∎

Corollary 6.4.1. *Let G be a finite abelian group with*

$$|G| = \prod_{j=1}^{k} p_j^{a_j}$$

for some distinct primes $p_1, \dots, p_k \in \mathbb{N}$ and $a_1, \dots, a_k \in \mathbb{N}$. Then

$$G \cong G_1 \times \cdots \times G_k,$$

where $\left|G_j\right| = p_j^{a_j}$ for all $j \in \{1, \dots, k\}$.

Theorem 6.5. Classification of Finite Abelian Groups

Let G be a finite abelian group. Then

$$G \cong (\mathbb{Z}/a_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/a_k\mathbb{Z})$$

for some unique prime powers $a_1, \dots, a_k \in \mathbb{N}$, up to reordering.

Proof. TL;DR. ∎

Free Groups and Finite Generated Groups

(6.2) Free Groups

Given an arbitrary set S, we may want to *generate* a group from it.

Def'n 6.2. **Word** over a Set

Let S be a set. A ***word*** over S is a formal expression of the form

$$s_1^{a_1} \cdots s_k^{a_k}$$

for some $k \in \mathbb{N} \cup \{0\}, s_1, \dots, s_k \in S^a$ and $a_1, \dots, a_k \in \mathbb{Z}$. When $k = 0$, we obtain the ***empty word***, denoted as ε. Given two words

$$w_1 = s_1^{a_1} \cdots s_k^{a_k}, w_2 = t_1^{b_1} \cdots t_l^{b_l}$$

for some $k, l \in \mathbb{N} \cup \{0\}, s_1, \dots, s_k, t_1, \dots, t_l \in S, a_1, \dots, a_k, b_1, \dots, b_l \in \mathbb{Z}$, we define the ***concatenation*** of w_1, w_2, denoted as $w_1 w_2$, by

$$w_1 w_2 = s^{a_1} \cdots s_k^{a_k} t_1^{b_1} \cdots t_l^{b_l}.$$

[a] Note that we are not assuming that $s_1, \dots, s_k$ are distinct.

A word like $s_1 s_2^2 s_2^{-3} s_3$ for some $s_1, s_2, s_3 \in S$ is clearly a word over S, but it should also be equal to $s_1 s_2^{-1} s_3$.

Def'n 6.3. **Reduced** Word

Let S be a set and let

$$w = s_1^{a_1} \cdots s_k^{a_k}$$

be a word over S, where $k \in \mathbb{N} \cup \{0\}, s_1, \dots, s_k \in S, a_1, \dots, a_k \in \mathbb{Z}$. We say w is ***reduced*** if $s_j \neq s_{j+1}$ for every $j \in \{1, \dots, k-1\}$ and $a_j \neq 0$ for every $j \in \{1, \dots, k\}$.

Equivalent Words

Def'n 6.4. Let w, v be words over a set S. We say w, v are ***equivalent*** if w can be changed to v by

(a) inserting or deleting s^0;

(b) replacing s^{a+b} with $s^a s^b$; or

(c) replacing $s^a s^b$ with s^{a+b}

for some $s \in S, a, b \in \mathbb{Z}$.

Proposition 6.6. *Let S be a set. Then every word over S is equivalent to a unique reduced word.*

Free Group Generated by a Set

Def'n 6.5. Let S be a set. The ***free group*** generated by S, denoted as $\mathcal{F}(S)$, is the set of reduced words over S, with operation

$$w_1 \cdot w_2 = r$$

for every $w_1, w_2 \in \mathcal{F}(S)$, where r is the reduced word equivalent to the concatenation $w_1 w_2$.

Proposition 6.7. *Let S be a set. Then $\mathcal{F}(S)$ is a group with identity ε.*

Theorem 6.8. Universal Property of Free Groups

Let S be a set and let G be a group. Then for every $\varphi : S \to G$, there exists a unique group homomorphism $\tilde{\varphi} : \mathcal{F}(S) \to G$ such that

$$\tilde{\varphi}(s) = \varphi(s)$$

for every $s \in S$.

(6.3) Group Presentations

Recall the following definition.

Normal Subgroup Generated by a Set

Recall 6.6. Let G be a group and let $S \subseteq G$. Then the ***normal subgroup*** generated by S, denoted as $\langle S \rangle$, is the intersection

$$\langle S \rangle = \bigcap_{N \trianglelefteq G : S \subseteq N} N.$$

We know that $\langle S \rangle \trianglelefteq G$, as its name suggests.

Group Presentation

Def'n 6.7. Let S be a set and let $R \subseteq \mathcal{F}(S)$. The ***group presentation*** $\langle S : R \rangle$ denotes the group $\mathcal{F}(S) / K$, where $K = \langle R \rangle$.

The idea of group presentations is to pick generators (i.e. elements of S) first and then pick elements of $\mathcal{F}(S)$ to set to the identity. For convenience, we use the following conventions for group presentations.

(a) If $k \in \mathbb{N} \cup \{0\}, s_1, \ldots, s_k \in S, a_1, \ldots, a_k \in \mathbb{Z}$, then

$$[s_1]^{a_1} \cdots [s_k]^{a_k} \in \langle S : R \rangle$$

is simply denoted as

$$s_1^{a_1} \cdots s_k^{a_k}.$$

(b) We can write $w_1 = w_2$ for some $w_1, w_2 \mathcal{F}(S)$ instead of writing $w_1 w_2^{-1}$. We can drop the curly braces on sets also. For instance,

$$\langle s, r : s^n = r^2 = e, rs = s^{-1} r \rangle$$

means

$$\langle \{s, r\} : \{s^n, r^2, rsr^{-1}s\} \rangle .$$

Def'n 6.8. **Presentation** of a Group

Let G be a group. If

$$G \cong \langle S : R \rangle$$

for some set S and $R \subseteq \mathcal{F}(S)$, then $S : R$ is called a ***presentation*** of G.

Presentation of a group needs not be unique. Moreover, every group G has a presentation:

$$G \cong \langle G : g \cdot h = gh, e_G = \varepsilon \rangle .$$

Def'n 6.9. **Finitely Presentable** Group

Let S be a set and let $R \subseteq \mathcal{F}(S)$. If both S, R are finite, then the presentation $\langle S : R \rangle$ is called ***finite***. Moreover, a group G is said to be ***finitely presentable*** if G is isomorphic to some finite presentation.

Theorem 6.9. Universal Property of Finitely Presented Groups

Let $G = \langle S : R \rangle$ for some set S and $R \subseteq \mathcal{F}(S)$ and let H be a group. If $\varphi : S \to H$ is a function such that

$$\varphi(s_1)^{a_1} \cdots \varphi(s_k)^{a_k} = e_H$$

for every $s_1^{a_1} \cdots s_k^{a_k} \in R$, where $k \in \mathbb{N}, s_1, \ldots, s_k \in S, a_1, \ldots, a_k \in \mathbb{Z}$, then there is a unique homomorphism $\tilde{\varphi} : G \to H$ such that

$$\tilde{\varphi}(s) = \varphi(s)$$

for all $s \in S$.

Proof. Let $\psi : \mathcal{F}(S) \to H$ be the homomorphism such that

$$\psi(s) = \varphi(s)$$

for every $s \in S$, which exists and is unique by Theorem 6.8. Let $K = \langle R \rangle \trianglelefteq \mathcal{F}(S)$. For any $r = s_1^{a_1} \cdots s_k^{a_k} \in R$, where $k \in \mathbb{N} \cup \{0\}, s_1, \ldots, s_k \in S, a_1, \ldots, a_k \in \mathbb{Z}$, observe that

$$\varphi(s_1)^{a_1} \cdots \varphi(s_k)^{a_k} = \psi(r) = e_H,$$

so $r \in \ker(\psi)$. This implies $R \subseteq \ker(\varphi)$ so $K \subseteq \ker(\varphi)$ as well. Let $q : \mathcal{F}(S) \to \mathcal{F}(S)/K$ be the quotient map. By the univalsal property of quotients, there exists a homomorphism $\tilde{\varphi} : \mathcal{F}(S)/K \to H$ such that $\psi = \tilde{\varphi} \circ q$. But this means

$$\tilde{\varphi}(s) = \psi(s) = \varphi(s)$$

for every $s \in S$, as required. ∎

II.
Ring Theory

7.
Rings

Rings

(7.1) Motivation

Observe that many algebraic structures, such as

$$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, M_{n\times n}(\mathbb{K}), \mathbb{Z}/n\mathbb{Z}, \mathbb{R}^{\mathbb{R}}, \mathbb{R}[x], \ldots,$$

have two operations: addition and multiplication. *Ring* is an abstract structure designed to capture what all these examples have in common.

Def'n 7.1. **Ring**

A ***ring*** is a tuple $(R,+,\cdot)$ such that

(a) $(R,+)$ is an abelian group; and

(b) $\cdot$ is an associative binary operation on R such that

- *left distributive property*: $a\cdot(b+c) = a\cdot b + a\cdot c$; and
- *right distributive property*: $(a+b)\cdot c = a\cdot c + b\cdot c$

for every $a,b,c \in R$.

The operation $+$ is called ***addition*** and $\cdot$ is called ***multiplication***.

Here are some remarks.

(a) Similar to groups, we refer to a ring $(R,+,\cdot)$ by simply writing R. Moreover, $a\cdot b$ is often written as ab for all $a,b\in R$.

(b) We always use *additive notation* for the group $(R,+)$.

(c) We denote the identity of $(R,+)$ by 0_R or 0 and inverse of any $a\in R$ with respect to $+$ by $-a$.

Def'n 7.2. **Commutative Ring**

Let R be a ring. If

$$ab = ba$$

for every $a,b\in R$, then we say R is a ***commutative*** ring.

Proposition 7.1. Basic Properties of Rings

Let R be a ring. Then for every $a,b\in R$,

(a) $0a = a0 = 0$*;*

(b) $(-a)b = a(-b) = -(ab)$*; and*

(c) $(-a)(-b) = ab$*.*

Proof. Let $a,b\in R$.

(a) Observe that

$$0a = (0+0)a = 0a + 0a$$

implying that $0a = 0$. $a0 = 0$ can be shown similarly. ◁

(b) Observe that

$$0 = 0b = (a + (-a))\, b = ab + (-a)\, b$$

so $-(ab) = (-a)\, b$. Similarly $a(-b) = -(ab)$ can be shown. ◁

(c) Observe that

$$(-a)(-b) = -(a(-b)) = -(-(ab)) = ab.$$

■

Def'n 7.3. Unital Ring

Let R be a ring. If R has a multiplicative inverse, then we say R is ***unital***.

(7.2) From now, we are going to say a *ring* to mean a *unital ring* for convenience. We are going to write 1 to denote the multiplicative identity.

Proposition 7.2. *Let R be a ring. Then*

$$-a = (-1)\, a$$

for all $a \in R$.

Proof. Observe that, for any $a \in R$,

$$0 = 0a = (1 + (-1))\, a = 1a + (-1)\, a = a + (-1)\, a.$$

■

(7.3) The smallest possible ring is $R = \{0\}$, with multiplication $00 = 0$. R is called the ***trivial ring***. The trivial ring is often an annoyance in ring theory, since there is a special property that holds only for the trivial ring.

Proposition 7.3. *Let R be a ring. Then $1 = 0$ if and only if R is trivial.*

Proof. Clearly the multiplicative identity of $\{0\}$ is 0 so $1 = 0$. Conversely, if $1 = 0$, then

$$a = 1a = 0a = 0$$

for all $a \in R$ so R is trivial. ■

Fields

Def'n 7.4. Unit of a Ring

Let R be a ring. $a \in R$ is called a ***unit*** if a has a multiplicative inverse. Moreover, we denote the set of units in R by $R^{\times}$.

(7.4) Let R be a ring. Then given any $a \in R^{\times}$, a has a unique inverse, which is denoted by a^{-1}. Moreover, we know that $R^{\times}$ is a group, so called the ***group of units*** of R.

Def'n 7.5. **Field**
Let R be a ring.

(a) If R is nontrivial with $R^\times = R \setminus \{0\}$, then we say R is a ***division*** ring.

(b) If R is a commutative division ring, then we say R is a ***field***.

Proposition 7.4. *Let $n \in \mathbb{N}$. Then $[x] \in \mathbb{Z}/n\mathbb{Z}$ is a unit if and only if $\gcd(x,n) = 1$.*

Proof. If $\gcd(x,n) = 1$, then $ax + bn = 1$ for some $a, b \in \mathbb{Z}$ by Bezout's lemma. Since $n|ax-1$, $[ax] = 1$ in $\mathbb{Z}/n\mathbb{Z}$. Conversely, if $[ax] = 1$, then $ax - 1 = bn$ for some $b \in \mathbb{Z}$, implying $\gcd(x,n) = 1$. ∎

Corollary 7.4.1. *Let $n \in \mathbb{N}$. Then $\mathbb{Z}/n\mathbb{Z}$ is a field if and only if n is prime.*

Theorem 7.5. Weddeerburn's Little Theorem
Every finite division ring is a field.

Subrings

Def'n 7.6. **Subring** of a Ring
Let R be a ring. A subset $S \subseteq R$ is called a ***subring*** of R if

(a) S is a subgroup of $(R, +)$;

(b) *closure under multiplication*: for every $a, b \in S$, $ab \in S$; and

(c) $1 \in S$.

(7.5) An important remark: $\{0\}$, the trivial ring, is not a subring of any ring.

Proposition 7.6. *Let R be a ring and let $S \subseteq R$ be a subring. Then S is a ring.*

(7.6) Let R be a ring and suppose that $a \in R, n \in \mathbb{Z}$ are given. Since R is a group under addition,

$$nx = \underbrace{x + \cdots + x}_{n \text{ terms}}$$

is well-defined. This means we can think of n as the element $n1 \in R$, in the sense that for every $x \in R$ we can talk about $xn, nx, x+n$.

Proposition 7.7. *Let R be a ring. Then for every $x \in R, n, m \in \mathbb{Z}$,*

(a) $n1x = xn1 = nx$; and

(b) $n(mx) = (nm)x$.

Proposition 7.8. Prime Subrings

Let R be a ring. Then the set

$$R_0 = \{n1 : n \in \mathbb{Z}\}$$

is a subring of R, and is contained in every subring of R. Furthermore,

$$R_0 \cong \mathbb{Z}/k\mathbb{Z}$$

as a group, where $k = \min\{m \in \mathbb{N} : m1 = 0\} \cup \{0\}$.[a]

[a] By convention, we write $\mathbb{Z}/0\mathbb{Z}$ to mean $\mathbb{Z}$.

Def'n 7.7. **Prime Subring, Characteristic** of a Ring

Consider the setting of Proposition 7.8.

(a) We call R_0 the ***prime subring*** of R.

(b) We call k the ***characteristic*** of R, denoted as $\operatorname{char}(R)$.

Def'n 7.8. **Center** of a Ring

Let R be a ring. Then the ***center*** of R, denoted as $Z(R)$, is

$$Z(R) = \{x \in R : \forall y \in R[xy = yx]\}.$$

Proposition 7.9. *Let R be a ring. Then $Z(R)$ is a subring of R.*

Corollary 7.9.1. *Let R be a ring. If R is nontrivial, then $Z(R)$ is nontrivial.*

Ring Homomorphisms

Def'n 7.9. **Homomorphism**

Let R, S be rings. A function $\varphi : R \to S$ is called a ***homomorphism*** if

(a) φ is a group homomorphism of the additive groups;

(b) $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in R$; and

(c) $\varphi(1_R) = \varphi(1_S)$.

If (a), (b) are satisfied but not (c), we say φ is ***non-unital***.

Def'n 7.10. **Isomorphism**

Let R, S be rings. A homomorphism $\varphi : R \to S$ is called an ***isomorphism*** if bijective.

(EX 7.7) Let R be a ring and let $n = \operatorname{char}(R)$. Then $\varphi : \mathbb{Z}/n\mathbb{Z} \to R_0$ by

$$\varphi([x]) = x1$$

is a ring isomorphism.

Proposition 7.10. Properties of Ring Homomorphisms

Let R, S be rings and let $\varphi : R \to S$ be a homomorphism.

(a) For every $a \in R, n \in \mathbb{N} \cup \{0\}$, $\varphi(a^n) = \varphi(a)^n$.

(b) For every $u \in R^\times$, $\varphi(u) \in S^\times$, and $\varphi(u^n) = \varphi(u)^n$ for all $n \in \mathbb{Z}$.

(c) If φ is bijective, then φ^{-1} is a homomorphism.

Proposition 7.11.

Let R, S be groups with $S \neq \{0\}$ and let $\varphi : R \to S$ be a homomorphism.

(a) $\varphi(R)$ is a subring of S.

(b) $\ker(\varphi)$ is a non-unital subring of R.

Polynomial Rings

Def'n 7.11. **Polynomial Ring** over a Ring

Let R be a ring. We define the ***polynomial ring*** over R, denoted as $R[x]$, as

$$R[x] = \{(a_i)_{i=0}^\infty \subseteq R : \exists n \geq 0 \forall i > n [a_i = 0]\}.$$

(7.8) We define operations $+, \cdot$ on $R[x]$ by

$$(a_i)_{i=0}^\infty + (b_i)_{i=0}^\infty = (a_i + b_i)_{i=0}^\infty$$

and

$$(a_i)_{i=0}^\infty (b_i)_{i=0}^\infty = \left(\sum_{i=0}^k a_i b_{k-i}\right)_{k=0}^\infty$$

for all $(a_i)_{i=0}^\infty, (b_i)_{i=0}^\infty \in R[x]$. We often write

$$\sum_{i=0}^n a_i x^i = (a_i)_{i=0}^\infty$$

by convention, where $n \in \mathbb{N} \cup \{0\}$ is such that $a_i = 0$ for all $i > n$.

Proposition 7.12. Polynomial Ring Is a Ring

Let R be a ring. Then $(R[x], +, \cdot)$ is a ring.

Def'n 7.12. **Degree** of a Polynomial

Let R be a ring and let $p \in R[x]$. The ***degree*** of p, denoted as $\deg(p)$, is defined as

$$\deg(p) = \begin{cases} -\infty & \text{if } p = 0 \\ \max\{n \in \mathbb{N} \cup \{0\} : a_n \neq 0\} & \text{otherwise} \end{cases}.$$

Proposition 7.13. *Let R be a ring. Then the set of constant polynomials in $R[x]$ is a subring of $R[x]$, and is isomorphic to R.*

Proposition 7.14. *Let R be a ring. If R is commutative, then $R[x]$ is commutative.*

Def'n 7.13. **Evaluation** of a Polynomial at an Element of a Ring
Let R be a ring and let $p \in R[x]$ be such that $p = \sum_{i=0}^{n} a_i x^i$ for some $n \in \mathbb{N} \cup \{0\}$. Given any $c \in R$, we define the ***evaluation*** of p at c, denoted as $p(c)$, to be

$$p(c) = \sum\nolimits_{i=0}^{n} a_i c^i.$$

Proposition 7.15. *Let R be a ring. If R is commutative, then for every $c \in R$, $\varphi : R[x] \to R$ by*

$$\varphi(p) = p(c)$$

is a homomorphism.

Proposition 7.16. *Let $\mathbb{K}$ be a field. Then*

(a) $\deg(fg) = \deg(f) + \deg(g)$ *for all $f, g \in \mathbb{K}[x]$; and*

(b) $\mathbb{K}[x]^\times \cong \mathbb{K}^\times$.

Group Rings

Def'n 7.14. **Group Ring** of a Group with Coefficients in a Ring
Let G be a group and let R be a ring. The ***group ring*** of G with coefficients in R, denoted as RG, is the set of formal sums

$$\left\{\sum\nolimits_{g\in G} c_g g : \forall g \in G\,[c_g \in R] \wedge \exists X \subseteq G\,[|X| \in \mathbb{N} \cup \{0\} \wedge \forall g \in G \setminus X\,[c_g = 0]]\right\}.$$

(7.9) We define the operations on RG as follows:

$$\sum\nolimits_{g\in G} a_g g + \sum\nolimits_{g\in G} b_g g = \sum\nolimits_{g\in G} (a_g + b_g)\, g$$

and

$$\left(\sum\nolimits_{g\in G} a_g g\right)\left(\sum\nolimits_{g\in G} b_g g\right) = \sum\nolimits_{g,h\in G} a_g b_h gh = \sum\nolimits_{k\in G}\left(\sum\nolimits_{g\in G} a_g b_{g^{-1}k}\right) k$$

for all $\sum_{g\in G} a_g g, \sum_{g\in G} b_g g \in RG$.

This page intentionally left blank.

8.
Ideals and Quotient Rings

Ideals

Def'n 8.1. **Ideal** of a Ring

Let R be a ring. $I \subseteq R$ is called an ***ideal*** of R if

(a) I is a subgroup of the additive group of R; and

(b) for all $m \in I, r \in R$, $rm, mr \in I$.

Proposition 8.1. *Let R, S be rings and let $\varphi : R \to S$ be a homomorphism. Then $\ker(\varphi)$ is an ideal.*

Proof. Let $r \in R, m \in \ker(\varphi)$. Then observe that

$$\varphi(rm) = \varphi(r)\varphi(m) = \varphi(r)0_S = 0 = 0_S\varphi(r) = \varphi(m)\varphi(r) = \varphi(mr). \qquad \blacksquare$$

Proposition 8.2. *For any $m \in \mathbb{Z}$, $m\mathbb{Z}$ is an ideal of $\mathbb{Z}$.*

Proof. We know that $m\mathbb{Z}$ is a subgroup of the additive group of $\mathbb{Z}$. Moreover, given any $r \in \mathbb{Z}, s \in m\mathbb{Z}$, $s = mk$ for some $k \in \mathbb{Z}$ so $rs = sr = rmk \in m\mathbb{Z}$. Thus $m\mathbb{Z}$ is an ideal. ∎

(8.1) Given any ring R, $\{0_R\}$ is an ideal of R, called the ***trivial ideal***, and often denoted by (0).

Proposition 8.3. Ideal Test

Let R be a ring and let $I \subseteq R$. Then I is an ideal of R if and only if

(a) $I \neq \varnothing$; and

(b) for all $r \in R, f, g \in I$, $rf + g, fr + g \in I$.

Proof. The forward direction is clear. For the backward direction, given any $f, g \in I$,

$$(-1)g + f = f - g \in I$$

by (b), so I is a subgroup of the additive group of R. Moreover, given any $m \in I, r \in R$,

$$rm = rm + 0 \in I$$

and

$$mr = mr + 0 \in I$$

by (b). Thus I is an ideal of R. ∎

Proposition 8.4. *Let R be a ring and let I be an ideal of R. If $1_R \in I$, then $I = R$.*

Proof. For every $r \in R$, since $1_R \in I$ and I is an ideal of R, $r = 1_R r \in I$. ∎

Corollary 8.4.1. *Let $\mathbb{K}$ be a field. Then the only ideals in $\mathbb{K}$ are $(0), \mathbb{K}$.*

Proof. Clearly (0) is an ideal of $\mathbb{K}$. Let I be a nontrivial ideal of $\mathbb{K}$. Then there is nonzero $x \in I$, so $xx^{-1} \in I$. But $xx^{-1} = 1_{\mathbb{K}}$, so $I = \mathbb{K}$. ∎

Corollary 8.4.2. *Let R be a nontrivial ring and let $\mathbb{K}$ be a field. Let $\varphi : \mathbb{K} \to R$ be a ring homomorphism. Then φ is injective.*

Proof. $\ker(\varphi)$ is an ideal of $\mathbb{K}$, so $\ker(\varphi) = (0)$ or $\ker(\varphi) = \mathbb{K}$. But assuming $\ker(\varphi) = \mathbb{K}$ implies $0_R = \varphi(1_{\mathbb{K}}) = 1_R$, so R is trivial, contradicting the assumption. Hence $\ker(\varphi) = (0)$. But φ is also a group homomorphism, so φ is injective. ∎

Quotient Rings

Theorem 8.5. *Let R be a ring and let I be an ideal of R. Define $+, \cdot : R/I \times R/I \to R/I$ by*

$$[x] + [y] = [x+y]$$

and

$$[x][y] = [xy]$$

for all $[x], [y] \in R$.

(a) *$(R/I, +, \cdot)$ is a ring.*

(b) *The quotient map $q : R \to R/I$ by*

$$q(x) = [x]$$

is a surjective ring homomorphism with $\ker(q) = I$.

Proof.

(a) We know R/I is an abelian group under addition from group theory, and also that $\cdot$ is well-defined. So we show few things:

- *associativity of* $\cdot$: Let $x, y, z \in R$. Then
$$[x]([y][z]) = [x][yz] = [xyz] = [xy][z] = ([x][y])[z].$$
- *identity for* $\cdot$: Observe that
$$[1][x] = [1x] = [x] = [x1] = [x][q]$$
for all $x \in R$, so $[1]$ is an identity for $\cdot$.
- *distributivity of $\cdot$ over* $+$: Let $x, y, z \in R$. Then
$$[x]([y]+[z]) = [x][y+z] = [x(yz)] = [xy+xz] = [xy]+[xz] = [x][y]+[x][z].$$
Similar argument holds for right distributivity. ◁

(b) We know that q is a group homomorphism. Moreover,

$$q(xy) = [xy] = [x][y] = q(x)q(y)$$

for all $x, y \in R$ and

$$q(1) = [1]$$

so q is a ring homomorphism. ∎

Def'n 8.2. **Quotient** of a Ring by an Ideal

Let R be a ring and let I be an ideal of R. Then the ring R/I defined in Theorem 8.5 is called the ***quotient*** of R by I.[a]

[a] Also calld simply a ***quotient ring*** for convenience.

Corollary 8.5.1. *Every ideal is the kernel of some homomorphism.*

Ideals Generated by a Subset

Proposition 8.6. *Let R be a ring and let $\mathcal{F}$ be a collection of ideals in R. Then*

$$\bigcap_{I \in \mathcal{F}} I$$

is an ideal of R.

Def'n 8.3. **Ideal** Generated by a Subset

Let R be a ring and let $X \subseteq R$. The ***ideal*** generated by X, denoted as (X), is

$$(X) = \bigcap_{I \in \mathcal{F}} I,$$

where $\mathcal{F} = \{I \text{ is an ideal of } R : I \supseteq X\}$.

(8.2) Let X be a set.

(a) Sometimes $\langle X \rangle$ is used instead of (X).

(b) When the elements of X are known, say $X = \{x_1, x_2, \ldots\}$, then we write

$$(x_1, x_2, \ldots)$$

instead of $(\{x_1, x_2, \ldots\})$. This also explains the *notation* (0) for the trivial group.

Proposition 8.7. *Let R be a ring and let $X \subseteq R$. Then*

$$(X) = \left\{ \sum_{i=1}^{k} s_i x_i t_i : k \in \mathbb{N} \cup \{0\}, \forall i \in \{1, \ldots, k\} \left[s_i, t_i \in R, x_i \in X \right] \right\}.$$

Proof. Denote

$$I = \left\{ \sum_{i=1}^{k} s_i x_i t_i : k \in \mathbb{N} \cup \{0\}, \forall i \in \{1, \ldots, k\} \left[s_i, t_i \in R, x_i \in X \right] \right\}$$

for convenience. Consider the following claims.

- *Claim 1. I is an ideal.*

  Proof. Since the empty sum is 0_R, $0_R \in I$. Moreover, given any $r \in R, x, y \in I$, we may write

  $$x = \sum_{i=1}^{k} s_i x_i t_i, y = \sum_{j=1}^{l} s'_j y_j t'_j$$

  for some $k, l \in \mathbb{N} \cup \{0\}, s_1, \ldots, s_k, t_1, \ldots, t_k, s'_1, \ldots, s'_l, t'_1, \ldots, t'_l \in R, x_1, \ldots, x_k, y_1, \ldots, y_l \in X$. So it follows that

  $$rx + y = \sum_{i=1}^{k} (rs_i) x_i t_i + \sum_{j=1}^{l} s'_j y_j t'_j \in I.$$

  Similarly $xr + y \in I$. Thus I is an ideal. ◁

- *Claim 2. $(X) \subseteq I$.*

  Proof. For every $x \in X$, observe that

  $$x = 1x1 = \sum_{1}^{1} s_1 x_1 t_1$$

  with $s_1 = t_1 = 1, x_1 = x$, so $x \in I$. ◁

- *Claim 3. $I \subseteq (X)$.*

  Proof. Let $k \in \mathbb{N} \cup \{0\}$ and let $s_i, t_i \in R, x_i \in X$ for all $i \in \{1, \ldots, k\}$. Since $X \subseteq (X)$, $x_i \in (X)$, which means $s_i x_i t_i \in (X)$ for all $i \in \{1, \ldots, k\}$. So $\sum_{i=1}^{k} s_i x_i t_i \in (X)$. ◁

Combining Claim 1, 2, 3 gives the desired result. ∎

Corollary 8.7.1. *Let R be a commutative ring and let $X \subseteq R$. Then*

$$(X) = \left\{ \sum_{i=1}^{k} r_i x_i : k \in \mathbb{N} \cup \{0\}, \forall i \in \{1, \ldots, k\} \left[r_i \in R, x_i \in X \right] \right\}.$$

(8.3) Let R be a ring and let $I, J \subseteq R$. We write $I + J$ to denote

$$I + J = \{x + y : x \in I, y \in J\}.$$

Corollary 8.7.2. *Let R be a ring and let I, J be ideals of R. Then $I + J = (I \cup J)$.*

Proof. Clearly $I + J \subseteq (I \cup J)$. For the reverse direction, let $k \in \mathbb{N} \cup \{0\}, s_1, \ldots, s_k, t_1, \ldots, t_k \in R, x_1, \ldots, x_k \in I \cup J$. Let

$$S = \{i \in \{1, \ldots, k\} : x_i \in I\}.$$

Then observe that

$$\sum_{i=1}^{k} s_i x_i t_i = \underbrace{\sum_{i \in S} s_i x_i t_i}_{\in I} + \underbrace{\sum_{i \in \{1,\ldots,k\} \setminus S} s_i x_i t_i}_{\in J} \in I + J.$$

∎

Corollary 8.7.3. *Let R be a ring and let $X \subseteq R$. Then $R/(X) = (0)$ if and only if there exist $k \in \mathbb{N} \cup \{0\}, s_1, \ldots, s_k, t_1, \ldots, t_k \in R, x_1, \ldots, x_k \in X$ such that*

$$1 = \sum_{i=1}^{k} s_i x_i t_i.$$

Def'n 8.4. **Principal** Ideal

Let R be a ring and let I be an ideal of R. If there exists $x \in R$ such that $I = (x)$, then we say I is ***principal***.

Isomorphism Theorems for Rings

Theorem 8.8. Universal Property of Quotient Rings

Let R, S be rings and let $\varphi : R \to S$ be a ring homomorphism. Let I be an ideal of R and let $q : R \to R/I$ be the quotient homomorphism. Then there is a ring homomorphism $\psi : R/I \to S$ such that $\psi \circ q = \varphi$ if and only if $I \subseteq \ker(\varphi)$. Moreover, if ψ exists, then is unique.

Lemma 8.8.1. *Let R, S, T be rings and let $\varphi_1 : R \to T$ be a ring homomorphism. If ψ_1 is surjective, then for every group homomorphism $\varphi_2 : T \to S$ such that $\psi_2 \circ \psi_1$ is a ring homomorphism, ψ_2 is a ring homomorphism.*

Proof. Suppose that φ_1 is surjective and let $\varphi_2 : T \to S$ be a group homomorphism such that $\varphi = \psi_2 \circ \psi_1$ is a ring homomorphism. Let $x, y \in T$. Then by the surjectivity of ψ_1, there exists $a, b \in R$ such that $\psi_1(a) = x, \psi_1(b) = y$. So

$$\psi_2(xy) = \psi_2(\psi_1(a)\psi_1(b)) = \psi_2(\psi_1(ab)) = \varphi(ab) = \varphi(a)\varphi(b) = \psi_2(\psi_1(a))\psi_2(\psi_1(b)) = \psi_2(x)\psi_2(y).$$

Moreover,

$$\psi_2(1_T) = \psi_2(\psi_1(1_R)) = \varphi(1_R) = 1_S.$$

Thus ψ_2 is a ring homomorphism. ∎

Proof of Theorem 8.8.

- ($\Longrightarrow$) For the existence part, let ψ be the group homomorphism provided by the universal property of quotient groups (Theorem 4.2). Then by applying Lemma 8.8.1 with $\psi_1 = q, \psi_2 = \psi, T = R/I$ shows that ψ is a ring homomorphism. The uniqueness of ψ follows from the uniqueness part of the universal property of quotient groups and the fact that any ring homomorphism is a group homomorphism. ◁
- ($\Longleftarrow$) This immediately follows from the universal property of quotient groups. ∎

Theorem 8.9. First Isomorphism Theorem for Rings

Let R,S be rings and let $\varphi : R \to S$ be a ring homomorphism. Then there exists a ring isomorphism $\psi : R/\ker(\varphi) \to \varphi(R)$ such that $\varphi = \psi \circ q$, where $q : R \to R/I$ is the quotient homomorphism.

Proof. By Theorem 8.8, there eixsts a ring homomorphism $\psi : R/\ker(\varphi) \to \varphi(R)$ such that $\psi \circ q = \varphi$. But this ψ is the isomorphism provided by the first isomorphism theorem by the universal property of quotient groups, so ψ is bijective. Thus ψ is a ring isomorphism such that $\varphi = \psi \circ q$. ∎

Proposition 8.10.

Let R be a commutative ring. Then for every $c \in R$,

$$R[x]/(x-c)R[x] \cong R.$$

Proof. Let $c \in R$. Recall that

$$(x-c)R[x] = \ker(\mathrm{ev}_c).$$

But for every $r \in R$, $\mathrm{ev}_c(r) = r$, so $\mathrm{ev}_c(R[x]) \cong R$. Thus by the first isomorphism theorem

$$R[x]/(x-c)R[x] \cong \mathrm{ev}_c(R[x]) \cong R.$$ ∎

Proposition 8.11.

Let R,S be rings and let $\varphi : R \to S$ be a ring homomorphism.

(a) If J is an ideal of S, then $\varphi^{-1}(J)$ is an ideal of R.

(b) If I is an ideal of R and φ is surjective, then $\varphi(I)$ is an ideal of S.

Theorem 8.12. Correspondence Theorem for Rings

Let R,S be rings and let $\varphi : R \to S$ be a surjective ring homomorphism. Then there is a bijection between subgroups of $(R,+)$ containing $\ker(\varphi)$ and subgroups of $(S,+)$. Moreover, for every subgroup $K \le (R,+)$ containing $\ker(\varphi)$, K is an ideal if and only if $\varphi(K)$ is an ideal.

Proof. The bijection part is provided by the correspondence theorem for groups. The remaining part can be proven by using Proposition 8.11. ∎

(8.4) Here is a special case of an application of correspondence theorem for rings. Let R be a ring and let I be an ideal of R. Then by applying the correspondence theorem on $q : R \to R/I$, the quotient homomorphism, if $K \le (R,+)$ contain I, then K is an ideal of R if and only if K/I is an ideal of R/I.

(EX 8.5) Let R be a commutative ring, where we desire to find the ideals of $R[x]$ containing (x). Observe that

$$(x) = \ker(\mathrm{ev}_0),$$

where $\mathrm{ev}_0 : R[x] \to R$ is a surjective homomorphism. So ideals of $R[x]$ containing (x) correspond to ideals of R, such that

$$\mathrm{ev}_0^{-1}(I) = \{f \in R[x] : f(0) \in I\} = \left\{\sum_{i=0}^{n} a_i x^i : n \in \mathbb{N} \cup \{0\}, a_0 \in I, \forall i \in \{0,\dots,n\}[a_i \in R]\right\}$$

corresponds to an ideal I of R.

Theorem 8.13. Second Isomorphism Theorem for Rings

Let R be a ring and let S be a subring of R. Let I be an ideal of R.

(a) $S+I$ is a subring of R and $S\cap I$ is an ideal of S.

(b) Let $i_S : S \to S+I$ be the inclusion map and let $q_1 : S \to S/S\cap I, q_2 \to S+I \to S+I/I$ be the quotient maps. Then there is a ring isomorphism $\psi : S/S\cap I \to S+I/I$ such that $\psi\circ q_1 = q_2\circ i_S$.

Proof.

(a) Exercise. ◁

(b) By the second isomorphism theorem for groups, there exists a group isomorphism $\psi : S/S\cap I \to S+I/I$ such that $\psi\circ q_1 = q_2\circ i_S$. It follows from Lemma 8.8.1 that ψ is a ring isomorphism. ▮

(EX 8.6) Let R be a commutative ring and let J be an ideal of R. Let

$$I = \{f\in R[x] : f(0)\in J\} = \mathrm{ev}_0^{-1}(J).$$

Then

(a) R is (isomorphic to) a subring of $R[x]$;

(b) $R+I = R[x]$; and

(c) $R\cap I = J$;

so $R/J\cong R[x]/I$ by the second ismorphism theorem.

Theorem 8.14. Third Isomorphism Theorem for Rings

Let R be a ring and let K,I be ideals of R such that $I\subseteq K$. Let

$$q_1 : R\to R/I, q_2 : R/I \to (R/I)/(K/I), q_3 : R\to R/K$$

be the quotient homomorphisms. Then there is a ring isomorphism $\psi : R/K \to (R/I)/(K/I)$ such that

$$\psi\circ q_3 = q_2\circ q_1.$$

(EX 8.7) Let $m,n\in\mathbb{Z}$. Then $(\mathbb{Z}/mn\mathbb{Z})/(m\mathbb{Z}/mn\mathbb{Z})\cong\mathbb{Z}/m\mathbb{Z}$ as rings.

A Construction of Complex Numbers

(8.8) We know that, given a ring R and $X\subseteq R$, we can construct a new ring by $R/(X)$. We can use this technique to construct the field of complex numbers. The starting point is to use $R=\mathbb{R}$, and add an element x such that $x^2=-1$. So let us look at

$$\mathbb{R}[x]/(x^2+1),$$

since $x^2=-1$ if and only if $x^2+1=0$. If we look at $[x]\in R[x]/(x^2+1)$, then

$$[x]^2+[1] = [x^2+1] = [0].$$

Hence it is natural to expect the following result.

Proposition 8.15. $\mathbb{R}[x]/\left(x^2+1\right)\cong\mathbb{C}$.

Before proving Proposition 8.15, let us recall the following defining properties of $\mathbb{C}$.

(a) $\mathbb{C}=\{a+bi : a,b\in\mathbb{R}\}$.

(b) $(a+bi)+(c+di)=(a+b)+(c+d)\,i$.

(c) $(a+bi)(c+di)=(ac-bd)+(ad+bc)\,i$.

We first show that $\mathbb{R}[x]/\left(x^2+1\right)$ satisfies (a).

Lemma 8.15.1. *Every element of $\mathbb{R}[x]/\left(x^2+1\right)$ can be written uniquely in the form $a+b[x]$ for some $a,b\in\mathbb{R}$.*

This page intentionally left blank.

9. Maximal and Prime Ideals

Maximal Ideals

Def'n 9.1. **Maximal** Ideal

Let R be a ring and let I be an ideal I of R. We say I is ***maximal*** if the only ideals of R containing I are I, R.

(9.1) That is, I is maximal if and only if I is a proper ideal of R maximal under $\subseteq$.

Proposition 9.1. *Let R be a ring and let I be an ideal of R. If R/I is a field, then I is maximal.*

Proof. This follows immediately from the correspondence theorem. ∎

Proposition 9.2. *Let R be a commutative ring. Then R is a field if and only if R is nontrivial and the only ideals in R are $(0), R$.*

Proof. The forward direction is clear. For the backward direction, let $x \in R$ be nonzero. Then $(x) = R$. This means $1 \in (x) = xR$ (where the equality holds since R is commutative), so there exists $y \in R$ such that $xy = 1$. Thus every nonzero element of R is a unit, as required. ∎

Theorem 9.3. *Let R be a commutative ring and let I be an ideal of R. Then R/I is a field if and only if I is maximal.*

(EX 9.2)

(a) Given any field $\mathbb{K}$, $\mathbb{K}[x]/(x-c) \cong \mathbb{K}$ for all $c \in \mathbb{K}$, so $(x-c)$ is a maximal ideal of $\mathbb{K}[x]$.

(b) $\mathbb{R}[x]/\left(x^2+1\right) \cong \mathbb{C}$, so $\left(x^2+1\right)$ is a maximal ideal of $\mathbb{R}[x]$.

(9.3) Given a ring R, the ideals of R are partially ordered under $\subseteq$. Although R is the maximum element with respect to $\subseteq$, we are more interested in the collection of *proper* ideals orderd under $\subseteq$.

Def'n 9.2. **Chain** of a Poset

Let $(X, \preceq)$ be a poset. We say $S \subseteq X$ is a ***chain*** of X if for every $s, t \in S$, $s \preceq t$ or $t \preceq s$.

Proposition 9.4. *Let R be a ring and let $\mathcal{F}$ be a chain of ideals of R. Then $\cup\mathcal{F}$ is an ideal of R.*

Corollary 9.4.1. *Let R be a ring and let $\mathcal{F}$ be a chain of proper ideals of R. Then there exists a proper ideal of R which is an upper bound for $\mathcal{F}$.*

Proof. Since $\mathcal{F}$ is a chain of proper ideals, $1 \notin I$ for all $I \in \mathcal{F}$, so $1 \notin \cup\mathcal{F}$. Hence $\cup\mathcal{F}$ is a proper ideal and an upper bound for $\mathcal{F}$. ∎

Proposition 9.5. *Let R be a commutative ring and let J be a proper ideal of R. Then there exists a maximal ideal K of R containing J.*

Proof. Let $\mathcal{I}$ be the collection of proper ideals of R containing J, ordered under $\subseteq$. By Corollary 9.4.1, every chain in $\mathcal{I}$ has an upper bound in $\mathcal{I}$. Thus by Zorn's lemma, $\mathcal{I}$ has a maximal element. ▮

Corollary 9.5.1. *Let R be a nontrivial commutative ring. Then there exists a field $\mathbb{K}$ such that there is a homomorphism from R to $\mathbb{K}$.*

Proof. By Proposition 9.5 R has a maximal ideal, say I. Then R/I is a field by Theorem 9.3, so we have the quotient homomorphism $q : R \to R/I$. ▮

Integral Domains

Def'n 9.3. **Zero Divisor** of a Ring

Let R be a ring. A nonzero element $x \in R$ is called a ***zero divisor*** of R if there exists nonzero $y \in R$ such that $xy = 0$ or $yx = 0$.[a]

[a] Often times, if $xy = 0$ but $yx \neq 0$, then we say x is a ***left zero divisor*** and vice versa.

(EX 9.4)
Examples of Zero Divisors

(a) Suppose that $n \in \mathbb{N}$ is not prime. Then $n = ab$ for some $a, b \in \{2, \ldots, n-1\}$, so $[a], [b] \neq 0_{\mathbb{Z}n/\mathbb{Z}}$. But

$$[a]\,[b] = [ab] = 0_{\mathbb{Z}/n\mathbb{Z}},$$

so $[a], [b]$ are zero divisors of $\mathbb{Z}/n\mathbb{Z}$.

(b) Let R, S be nontrivial rings and let $a \in R, b \in S$ be nonzero. Then $(a, 0), (0, b)$ are nonzero in $R \times S$, but

$$(a,0)\,(0,b) = (0,0) = 0_{R\times S},$$

so $(a, 0), (0, b)$ are zero divisors.

(c) Let R be a ring. Then $[x]$ is a zero divisor in $R[x]/\left(x^2\right)$, since

$$[x]^2 = \left[x^2\right] = 0_{R[x]/(x^2)}.$$

(d) Let R be a ring. Then

$$[x]\,[y] = [xy] = 0_{R[x,y]/(xy)}$$

so $[x], [y]$ are zero divisors in $R[x,y]/(xy)$.

(e) Let $n \in \mathbb{N}$. Then for every $A \in M_{n\times n}(\mathbb{K})$, A is a zero divisor if and only if $\operatorname{rank}(A) < n$.

(f) Let G be a group and let $g \in G$ with $|g| = 2$ (this guarantees $g \neq e_G$). Then

$$(e_G + g)\,(e - g) = e_G - g^2 = e_G - e_G = 0_{\mathbb{Z}G},$$

so $e_G + g, e_G - g$ are zero divisor in $\mathbb{Z}G$.

We also have the following open problem about zero divisors.

Statement 9.6. Kaplansky Zero Divisor Conjecture

Let G be a group. If every nonidentity element of G has infinite order, then $\mathbb{K}G$ has no zero divisors for every field $\mathbb{K}$.

Proposition 9.7.

Let R be a ring and let $u \in R$ be a unit. Then u is not a zero divisor.

Proof. Suppose $v \in R$ is such that $uv = 0$. Then

$$v = u^{-1}uv = 0.$$

Similarly, if $vu = 0$, then $v = vuu^{-1} = 0$. Thus u is not a zero divisor. ∎

Corollary 9.7.1.

Every field does not have a zero divisor.

Proof. It follows immediately from the fact that every element of a field is a unit. ∎

(9.5) Although units are not zero divisors, an element of a ring can be non-zero-divisor without being a unit.

(a) $\mathbb{Z}$ does not have any zero divisor, but $\mathbb{Z}^{\times} = \{-1, 1\}$.

(b) By the degree formula, $fg = 0$ if and only if $f = 0$ or $g = 0$ for every $f, g \in \mathbb{K}[x]$, where $\mathbb{K}$ is a field. But $\mathbb{K}[x]^{\times} = \mathbb{K}$.

Proposition 9.8. Cancellation Property

Let R be a ring and let $x \in R$ be a nonzero element which is not a zero divisor. Then for every $a, b \in R$, if $xa = xb$ or $ax = bx$, then $a = b$.

Proof. Observe that $xa = xb$ implies $x(a-b) = 0$. But x is not a zero divisor, so $a - b = 0$, hence $a = b$. The case $ax = bx$ can be verified similarly. ∎

Corollary 9.8.1.

Let R be a finite ring and let $x \in R$ be nonzero. If x is not a zero divisor, then x is a unit.

Proof. Observe that $xa \neq xb$ and $ax \neq bx$ for every distinct $a, b \in R$, so $xR = R = Rx$, since R is finite. Hence there exists $y, z \in R$ such that $xy = zx = 1_R$. But x has both left and right inverses if and only if invertible, since multiplication on R is associative. Thus x is a unit. ∎

Def'n 9.4. **Integral Domain**

An ***integral domain*** is a nontrivial, commutative ring with no zero divisor.

(9.6) From Corollary 9.8.1, the following result is immediate.

Corollary 9.8.2.

Every finite integral domain is a field.

(9.7) One of the reasons why we are interested in integral domains is that they work well as *coefficient rings for polynomials*.

Proposition 9.9. *Let R be an integral domain.*

(a) For every $f, g \in R[x]$, $\deg(fg) = \deg(f) + \deg(g)$.

(b) $R[x]$ is an integral domain.

Proof.

(a) We may assume $f, g \in R[x]$ are nonzero. Let f_n, g_m be the leading coefficients of f, g, respectively, where $n = \deg(f), m = \deg(g)$. Then observe that

$$fg = f_n g_m x^{n+m} + \cdots.$$

But R is an integral domain, so $f_n g_m \neq 0$. Thus $\deg(fg) = n + m = \deg(f) + \deg(g)$. $\triangleleft$

(b) Suppose that $f, g \in R[x]$ are nonzero. Then $\deg(fg) + \deg(f) + \deg(g) \geq 0$ by (a), so $fg \neq 0$. ■

Proposition 9.10. *Let $\mathbb{K}$ be a field. Then every subring of $\mathbb{K}$ is an integral domain.*

Proof. Since $\mathbb{K}$ is a field, $\mathbb{K}$ is commutative and $1_{\mathbb{K}} \neq 0_{\mathbb{K}}$. So R is commutative and $1_R \neq 0_R$. Moreover, given any nonzero $x \in R$, suppose $xy = 0_R$ for some $y \in R$. Then

$$y = x^{-1}xy = 0_{\mathbb{K}}$$

in $\mathbb{K}$, so it follows that $y = 0_R$ in R. Thus R has no zero divisors. ■

Proposition 9.11. *For every $\alpha \in \mathbb{C}$ such that $\alpha^2 \in \mathbb{Z}$,*

$$\{a + b\alpha : a, b \in \mathbb{Z}\}$$

is a subring of $\mathbb{C}$.[a]

[a] We write $\mathbb{Z}[\alpha] = \{a + b\alpha : a, b \in \mathbb{Z}\}$.

(9.8) Proposition 9.11 leads to interesting integral domains such as the domain of Gaussian integers: $\mathbb{Z}[i]$.

Prime Ideals

(9.9) A motivation for prime ideals is to construct *interesting* integral domains of the form

$$R[x]/(p)$$

where R is a commutative ring and $p \in R[x]$. To do so, we have to answer the following question.

Let R be a commutative ring and let I be an ideal of R. When is R/I an integral domain?

To answer this, suppose that R/I is an integral domain. Then for any $a,b \in R$, if $[a][b] = 0_{R/I}$, then one of $[a],[b]$ is zero in R/I, which is equivalent to saying that $a \in I$ or $b \in I$. But, for any $r \in R$,

$$[r] = 0_{R/I} \iff r \in I,$$

so

$$[a][b] = [ab] = 0_{R/I} \iff ab \in I.$$

This gives the following *necessary* condition for I: I is proper and such that for every $a,b \in R$, if $ab \in I$, then $a \in I$ or $b \in I$.

Def'n 9.5. **Prime Ideal**

Let R be a commutative ring and let I be an ideal of R. We say I is ***prime*** if I is proper and for every $a,b \in R$, if $ab \in I$, then $a \in I$ or $b \in I$.

In fact, I being prime is also *sufficient* to conclude that R/I is an integral domain.

Theorem 9.12. *Let R be a commutative ring and let I be an ideal of R. Then R/I is an integral domain if and only if I is prime.*

Proof. Since R is commutative, by the surjectivity of quotient homomorphism $q : R \to R/I$, R/I is commutative. Moreover, R/I is nontrivial if and only if I is proper. Lastly

$$R/I \text{ has no zero divisors} \iff \forall a,b \in R\left[[a][b] = 0_{R/I} \implies [a] = 0_{R/I} \vee [b] = 0_{R/I}\right]. \qquad [9.1]$$

But for any $r \in R$, $[r] = 0_{R/I}$ if and only if $r \in I$, so it follows that [9.1] is equivalent to

$$R/I \text{ has no zero divisors} \iff \forall a,b \in R\,[ab \in I \implies a \in I \vee b \in I].$$

Thus R/I is nontrivial and has no zero divisors if and only if I is prime, and the commutativity of R/I is guaranteed by the commutativity of R. ∎

Corollary 9.12.1. *Maximal ideals are prime.*

Proof. Given any commutative ring R and a maximal ideal I of R, R/I is a field, hence an integral domain. Thus I is prime. ∎

(EX 9.10) Let $\mathbb{K}$ be a field. Then $\mathbb{K}[x,y]/\left(y-x^2\right) \cong \mathbb{K}[x]$, where $\mathbb{K}[x]$ is an integral domain but not a field. Thus $\left(y-x^2\right)$ is a prime ideal which is not maximal.

Proposition 9.13. *Let R be an integral domain and let $f,g \in R[x]$ have degree at least 1. Then $fgR[x]$is not prime.*

Proof. For any nonzero $h \in R[x]$, $\deg(fgh) \geq \deg(fg) = \deg(f) + \deg(g) > \max\{\deg(f), \deg(g)\}$. So $fg \in fgR[x]$, but $f,g \notin fgR[x]$. ∎

(9.11) The intuition for Proposition 9.13 is that, given an integral domain R, if $h \in R[x]$ factors into a product of lower degree polynomials, then the principal ideal $hR[x]$ is not prime.

10.
Fields of Fractions

Fields of Fractions

Theorem 10.1. *Let R be a ring. Then R is an integral domain if and only if it is a subring of a field, up to isomorphism.*

(10.1) To prove Theorem 10.1, observe that the reverse direction is already provided by Proposition 9.10. For the forward direction, we would want to construct a field containing R, given an integral domain R. We first try this with $R = \mathbb{Z}$.

Proposition 10.2. *Let $\mathbb{K}$ be a field containing $\mathbb{Z}$ as a subring. Then $\mathbb{K}$ contains $\mathbb{Q}$ as a subfield.*[a]

[a] Given a field $\mathbb{K}$ and a subset $S \subseteq \mathbb{K}$, we say S is a ***subfield*** of $\mathbb{K}$ if S is a field with respect to the operations of $\mathbb{K}$.

Proof. Since $\mathbb{K}$ contains $\mathbb{Z}$ as a subring, $\varphi : \mathbb{Z} \to \mathbb{K}$ by

$$\varphi(a) = a$$

for all $a \in \mathbb{Z}$ is an injective homomorphism.[1] Define $\varphi : \mathbb{Q} \to \mathbb{K}$ by

$$\psi\left(\frac{a}{b}\right) = \varphi(a)\varphi(b)^{-1}$$

for all $a, b \in \mathbb{Z}, b \neq 0$. We now have the following claims.

- *Claim 1. ψ is well-defined.*

  Proof. Suppose $\frac{a}{b} = \frac{c}{d}$ for some $a, b, c, d \in \mathbb{Z}, b, d \neq 0$. This means $ad = bc$. So

  $$\varphi(a)\varphi(d) = \varphi(ad) = \varphi(bc) = \varphi(b)\varphi(c),$$

  so

  $$\varphi(a)\varphi(b)^{-1} = \varphi(c)\varphi(d).$$

  Thus ψ is welll-defined. ◁

- *Claim 2. ψ is a homomorphism.*

  Proof. Let $a, b, c, d \in \mathbb{Z}, b, d \neq 0$. Then observe that

  $$\psi\left(\frac{a}{b}\right)\psi\left(\frac{c}{d}\right) = \varphi(a)\varphi(b)^{-1}\varphi(c)\varphi(d)^{-1} = \varphi(ac)\varphi(bd)^{-1} = \psi\left(\frac{ac}{bd}\right).$$ ◁

- *Claim 3. ψ is injective.*

  Proof. Since $\mathbb{K}$ is a field, $\mathbb{K}$ is a nontrivial ring. So by Corollary 8.4.2, ψ is injective. ∎

By Proposition 10.2, we may think $\mathbb{Q}$ as the *smallest field containing* $\mathbb{Z}$.

[1] We call this φ a ***subgroup inclusion map***.

Field of Fractions of an Integral Domain

Def'n 10.1. Let R be an integral domain. Then the ***field of fractions*** Q of R is the set

$$Q = \left\{ \frac{a}{b} : a, b \in R, b \neq 0_R \right\}$$

such that $\frac{a}{b} = \frac{c}{d}$ if and only if $ad = bc$ for all $a, b, c, d \in R, b, d \neq 0_R$,[a] together with the operations $+, \cdot$ by

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$$

and

$$\frac{a}{b}\frac{c}{d} = \frac{ac}{bd}.$$

[a] Formally speaking, we have *equivalence classes* instead of fractions, such that $\frac{a}{b}, \frac{c}{d}$ are in the same equivalence class if $ad = bc$.

(10.2) The reason why we would use an integral domain over any ring in defining field of fractions is that, given a ring R, if $y, z \in R$ are nonzero and such that $yz = 0$, then

$$\frac{0}{y}\frac{0}{z} = \frac{0}{0}.$$

But $0a = 0b$ for all $a, b \in R, b \neq 0$, so

$$\frac{a}{b} = \frac{0}{0}.$$

Hence our field of fractions end up with a single element. However, by disallowing zero divisors from entering the denominator, it turns out we can construct something similar for any commutative ring, not necessarily an integral domain.

(10.3) Localization

Let R be a commutative ring, where we want to construct a field-of-fraction-like structure. But as seen in (10.2), we cannot put zero divisors in the denominator. Therefore, if we write $S \subseteq R$ to denote the set of elements that can be placed in the denominator, then $0 \neq S$ and moreover S does not have any zero divisor. Furthermore, given any fractions $\frac{a}{b}, \frac{c}{d}$ for some suitable $a, c \in R, b, d \in S$, we would want our operation to be

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}, \frac{a}{b}\frac{c}{d} = \frac{ac}{bd}.$$

For this operation to be well-defined, at least we have to ensure $bd \in S$ whenever $b, d \in S$.

Multiplicatively Closed Set

Def'n 10.2. Let R be a ring. We say $S \subseteq R$ is ***multiplicatively closed*** if $1 \in S$ and for every $b, d \in S$, $bd, db \in S$.[a]

[a] We require both bd, db to be in S since we defined R to be any ring.

Theorem 10.3. Localization of Commutative Rings

Let R be a commutative ring and let $S \subseteq R$ be a multiplicatively closed subset of R such that $0 \neq S$ and no zero divisor is in S. Then there exist a commutative ring Q and an injective homomorphism $\varphi : R \to Q$ such that

(a) $\varphi(a) \in Q^\times$ for all $a \in S$;

(b) every element of Q is of the form $\varphi(a)\varphi(b)^{-1}$ for some $a \in R, b \in S$; and

(c) if there exists a ring T and a homomorphism $\psi : R \to T$ such that $\psi(x) \in T^\times$ for all $x \in S$, then

there is a homomorphism $\tilde{\psi} : Q \to R$ such that $\tilde{\psi} \circ \varphi = \psi$.

Proof. Let

$$Q_0 = \{(a,b) : a \in R, b \in S\}$$

and define a relation $\sim$ on Q_0 by $(a,b) \sim (c,d)$ if $ad = bc$ for all $(a,b),(c,d) \in Q_0$.

- *Claim 1. $\sim$ is an equivalence relation.*

  Proof. Fix $(a,b),(c,d),(e,f)$.

  - *reflexivity*: By commutativity of R, $ab = ba$, so $(a,b) \sim (a,b)$.
  - *symmetry*: Suppose $(a,b) \sim (c,d)$. Then $ad = bc$, so by commutativity $cb = da$. Thus $(c,d) \sim (a,b)$.
  - *transitivity*: Suppose $(a,b) \sim (c,d)$ and $(c,d) \sim (e,f)$. Then $ad = bc, cf = de$, so

    $$afd = bcf = bed.$$

    Since $d \in S$, d is nonzero and not a zero divisor, so

    $$af = be$$

    by the cancellation law. Thus $(a,b) \sim (e,f)$. ◁

Since $\sim$ is an equivalence relation, we may define the collection of equivalence classes of $\sim$: let

$$Q = Q_0 / \sim .$$

For convenience, write $\frac{a}{b}$ to denote the equivalence class of (a,b), $[(a,b)]$, for every $a \in R, b \in S$. We desire to put a ring structure on Q, so let us define the operations: let $+, \cdot : Q \times Q \to Q$ be defined by

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$$

and

$$\frac{a}{b}\frac{c}{d} = \frac{ac}{bd}$$

for all $\frac{a}{b}, \frac{c}{d} \in Q$.

- *Claim 2. $+$ is well-defined.*

  Proof. Let $\frac{a}{b}, \frac{c}{d} \in Q$. We first note that, since S is multiplicatively closed, $bd \in S$, so $\frac{ad+bc}{bd}$ is a well-defined element of Q. Now suppose that $\frac{a}{b} = \frac{a'}{b'}$ for some $a' \in R, b' \in S$. Then

  $$ab' = ba',$$

  which means

  $$(ad+bc)(b'd') = ba'dd' + bb'dc' = (a'd' + b'c')(bd),$$

  so

  $$\frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'},$$

  as desired. ◁

- *Claim 3. $\cdot$ is well-defined.*

  Proof. This can be proven similarly to Claim 2. ◁

- *Claim 4. Let $\frac{a}{b} \in Q$. Then $\frac{a}{b} = \frac{0}{1}$ if and only if $a = 0$.*

  Proof. Observe that
  $$\frac{a}{b} = \frac{0}{1} \iff 1a = b0 \iff a = 0.$$ ◁

- *Claim 5. $(Q, +)$ is an abelian group, with $0_Q = \frac{0}{1}$ and $-\frac{a}{b} = \frac{-a}{b}$ for all $\frac{a}{b} \in Q$.*

  Proof. Let $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in Q$.

  · *associativity of* $+$: Observe that
  $$\left(\frac{a}{b} + \frac{c}{d}\right) + \frac{e}{f} = \frac{ad + bc}{bd} + \frac{e}{f} = \frac{adf + bcf + ebd}{bdf} = \cdots = \frac{a}{b} + \left(\frac{c}{d} + \frac{e}{f}\right)$$
  since the addition on R is associative.

  · *identity of* $+$: Observe that
  $$\frac{a}{b} + \frac{0}{1} = \frac{a1 + b0}{b1} = \frac{a}{b}.$$

  · *additive inverse*: Observe that
  $$\frac{a}{b} + \frac{-a}{b} = \frac{ab - ba}{b^2} = \frac{0}{b^2} = \frac{0}{1}$$
  by Claim 4.

  · *commutativity of* $+$: Observe that
  $$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} = \frac{c}{d} + \frac{a}{b}$$
  since the addition on R is commutative. ◁

- *Claim 6. $(Q, +, \cdot)$ is a commutative ring, with $1_Q = \frac{1}{1}$.*

  Proof. Let $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in Q$.

  · *associativity of* $\cdot$: Observe that
  $$\left(\frac{a}{b}\frac{c}{d}\right)\frac{e}{f} = \frac{ace}{bdf} = \frac{a}{b}\left(\frac{c}{d}\frac{e}{f}\right)$$
  since the multiplication on R is associative.

  · *identity of* $\cdot$: Observe that
  $$\frac{a}{b}\frac{1}{1} = \frac{a1}{b1} = \frac{a}{b}.$$

  · *commutativity of* $\cdot$: Observe that
  $$\frac{a}{b}\frac{c}{d} = \frac{ab}{cd} = \frac{ba}{dc} = \frac{c}{d}\frac{a}{b}$$
  since the multiplication on R is commutative.

- *distributivity of $\cdot$ over $+$*: Observe that
$$\frac{a}{b}\left(\frac{c}{d}+\frac{e}{f}\right)=\frac{a}{b}\frac{cf+de}{df}=\frac{acf+ade}{bdf}=\frac{acfb+adeb}{b^2df}=\frac{ac}{bd}+\frac{ae}{df}.$$
The right distributivity follows from the commutativity of $\cdot$. ◁

Define $\varphi : R \to Q$ by
$$\varphi(a)=\frac{a}{1}$$
for all $a \in R$.

- *Claim 7. φ is a homomorphism.*

  Proof. Observe that, given any $a,b \in R$,
$$\varphi(1)=\frac{1}{1}=1_Q$$
and
$$\varphi(a+b)=\frac{a+b}{1}=\frac{a}{1}+\frac{b}{1}=\varphi(a)+\varphi(b)$$
and
$$\varphi(ab)=\frac{ab}{1}=\frac{a}{1}\frac{b}{1}=\varphi(a)\varphi(b).$$
◁

- *Claim 8. φ is injective.*

  Proof. Let $a,b \in R$ and observe that
$$\varphi(a)=\varphi(b) \iff \frac{a}{1}=\frac{b}{1} \iff a1=1b \iff a=b.$$
◁

- *Claim 9. For all $a \in S$, $\varphi(a) \in S^{\times}$.*

  Proof. Let $a \in S$. Then
$$\varphi(a)\frac{1}{a}=\frac{a}{1}\frac{1}{a}=\frac{a}{a}=\frac{1}{1}=1_Q.$$
◁

- *Claim 10. Every element of Q is of the form $\varphi(a)\varphi(b)^{-1}$ for some $a \in R, b \in S$.*

  Proof. Given any $\frac{a}{b} \in Q$, $a \in R, b \in S$ and $\frac{a}{b}=\frac{a}{1}\frac{1}{b}=\varphi(a)]\varphi(b)^{-1}$. ◁

This completes the proof upto part (b). (c) is left as an exercise. ∎

Corollary 10.3.1. *Let R be a commutative ring and let $S \subseteq R$ be such that S is multiplicatively closed and does not have 0 or any zero divisor. If Q_1, Q_2 are commutative rings and $\varphi_1 : R \to Q_1, \varphi_2 : R \to Q_2$ are injective homomorphisms satisfying the conditions (a), (b), (c) of Theorem 10.3, then there is an isomorphism $\alpha : Q_1 \to Q_2$ such that $\alpha \circ \varphi_1 = \varphi_2$.*

Proof. By (c) of Theorem 10.3, there are $\alpha : Q_1 \to Q_2, \beta : Q_2 \to Q_1$ such that

$$\alpha \circ \varphi_1 = \varphi_2, \beta \circ \varphi_2 = \varphi_1.$$

But given any $x \in Q_1$,

$$x = \varphi_1 (a) \varphi_1 (b)^{-1}$$

for some $a \in R, b \in S$ by (a) of Theorem 10.3. Hence

$$\beta (\alpha (x)) = \varphi (a) \varphi (b)^{-1} = x,$$

which means β is a left inverse to α. But by symmetry α is a left inverse to β, so α, β are bijections. Thus α is the isomorphism satisfying the condition. ▮

Def'n 10.3. **Localization** of a Ring at a Multiplicatively Closed Subset

Let R be a ring and let Q be the ring defined in Theorem 10.3. We say Q is the ***localization*** of R at S (or with respect to S), denoted as $S^{-1}R$.

(10.4) Precisely speaking, Corollary 10.3.1 only guarantees that $S^{-1}R$ is defined *up to isomorphism*, given a commutative ring R and a multiplicatively closed subset $Ss \subseteq R$ without 0 and any zero divisor. Usually we take the definition given in Theorem 10.3 for convenience, however.

(10.5) We can finally prove that the field of fractions of an integral domain is indeed a field.

Proposition 10.4. *Let R be an integral domain. Then $(R \setminus \{0\})^{-1} R$ is a field.*

Proof. Clearly $R \setminus \{0\}$ is multiplicatively closed and does not have 0 or any zero divisor. Moreover, R is a subring of $S^{-1}R$, so $S^{-1}R$ is nontrivial. Given any $\frac{a}{b} \in S^{-1}R$, $\frac{a}{b} = \frac{0}{1}$ if and only if $a = 0$, so if $\frac{a}{b} \neq 0$, then $\frac{a}{b}$ is invertible, with $\frac{a}{b}\frac{b}{a} = \frac{1}{1}$. ▮

We can compactly define the field of fractions of an integral domain R as $(R \setminus \{0\})^{-1} R$.

Proposition 10.5. $(\mathbb{Z} \setminus \{0\})^{-1} \mathbb{Z} = \mathbb{Q}$.

Proof. This is clear from the constructions of $(\mathbb{Z} \setminus \{0\}) \mathbb{Z}$ and $\mathbb{Q}$. ▮

Def'n 10.4. **Field of Rational Functions** over an Integral Domain

Let R be a domain. The field of fractions of $R[x]$, denoted as $R(x)$, is called the ***field of rational functions*** over R.

By construction $R(x) = \left\{ \frac{f}{g} : f, g \in R[x], g \neq 0 \right\}$.

Proposition 10.6. *Let R be an integral domain and let Q be the field of fractions of R. Then $Q(x) \cong R(x)$.*

Proof. Since $R[x]$ is a subring of $Q[x]$ and $Q[x]$ is a subring of $Q(x)$, there exists an injective homomorphism $\varphi : R[x] \to Q(x)$. But $Q(x)$ is a field, so every nonzero element of $R[x]$ is sent to a unit of $Q(x)$ by φ. So by part (c) of Theorem 10.3, there exists a homomorphism $\psi : R(x) \to Q(x)$ such that

$$\psi\left(\frac{f}{g}\right) = \frac{f}{g}$$

for all $\frac{f}{g} \in R(x)$. Since $R(x)$ is also a field, ψ is injective. But given any $\frac{a}{b} \in Q$, $\frac{a}{b} \in R(x)$, and by using this fact it can be easily verified that ψ is surjective. Thus $Q(x) \cong R(x)$. ∎

Proposition 10.7. *Let R be a commutative ring and let $I \subseteq R$ be an ideal. Then $R \setminus I$ is multiplicatively closed if and only if I is prime.*

Proposition 10.8. *Let R be a commutative ring and let $P \subseteq R$ be a prime ideal. Then $R \setminus P$ does not have 0 or any zero divisor.*

Def'n 10.5. **Localization** of a Commutative Ring at a Prime Ideal

Let P be a prime ideal of an integral domain R. We define the ***localization*** of R at P, denoted as R_P, to be the ring

$$R_P = (R \setminus P)^{-1} R.$$

Proposition 10.9. *Let $\mathbb{K}$ be a field and let $c \in \mathbb{K}$. Then the localization $\mathbb{K}[x]_{(x-c)} \cong R(c)$.*[a]

[a] $R(c)$ is the set of rationoal functions over $\mathbb{K}$ with c in the domain.

Proposition 10.10. *Let R be a domain and let $I \subseteq R$ be an ideal. If I is prime, then R_I has a unique maximal ideal.*

Def'n 10.6. **Local** Commutative Ring

Let R be a commutative ring. If R has a unique maximal ideal, then we say R is ***local***.

Product Ideals

Def'n 10.7. **Product Ideal** of Ideals

Let R be a ring and let $I, J \subseteq R$ be ideals. Then the ***product ideal*** of I, J, denoted as IJ, is the ideal

$$IJ = (\{ab : a \in I, b \in J\}).$$

Proposition 10.11. Properties of Product Ideals

Let R be a ring and let $I, J \subseteq R$ be ideals.

(a) $IJ = \left\{\sum_{i=1}^{k} a_i b_i : k \in \mathbb{N} \cup \{0\}, a_1, \ldots, a_k \in I, b_1, \ldots, b_k \in J\right\}$.

(b) If R is commutative, and $S, T \subseteq R$ are some generators of I, J, respectively (i.e. $I = (S), J = (T)$), then

$$IJ = (\{a, b : a \in S, b \in T\}).$$

(10.6) Note that another way of saying (a) of Proposition 10.11 is that IJ is the subgroup of the additive group of R generated by products of elements of I, J.

Proof of Proposition 10.11.

(a) Let

$$K=\left\{\sum_{i=1}^{k} a_ib_i : k\in\mathbb{N}\cup\{0\},a_1,\dots,a_k\in I,b_1,\dots,b_k\in J\right\}.$$

Then from the definition of K, it is clear that $K\neq\varnothing$, $-x\in K$ whenever $x\in K$ and that K is closed under addition. Hence K is a subgroup of the additive group of R. Moreover, given any $r,s\in R$ and $x\in K$, we may write

$$x=\sum_{i=1}^{k} a_ib_i$$

for some $k\in\mathbb{N}\cup\{0\},a_1,\dots,a_k\in I,b_1,\dots,b_k\in J$, so

$$rxs=r\left(\sum_{i=1}^{k} a_ib_i\right)s=\sum_{i=1}^{k} ra_ib_is=\sum_{i=1}^{k}(ra_i)(b_is).$$

But $ra_i\in I,b_is\in J$ for all $i\in\{1,\dots,k\}$ since I,J are ideals. Hence K is an ideal. Clearly a generating set for IJ is contained in K:

$$\{ab:a\in I,b\in J\}\subseteq\underbrace{\left\{\sum_{i=1}^{k} a_ib_i : k\in\mathbb{N}\cup\{0\},a_1,\dots,a_k\in I,b_1,\dots,b_k\in J\right\}}_{=K}.$$

This means $K\supseteq IJ$. Conversely, since IJ is closed under addition and every element of K is a sum of generators of IJ, $K\subseteq IJ$. Thus $K=IJ$.

(b) Let

$$K=(\{ab:a\in S,b\in T\}).$$

It is clear from the definition that $K\subseteq IJ$, since a generating set for K is a subset of a generating set for IJ. Conversely, suppose $a\in I,b\in J$. Then

$$a=\sum_{i=1}^{k} a_is_i, b=\sum_{j=1}^{l} b_jt_j$$

for some $k,l\in\mathbb{N}\cup\{0\},a_1,\dots,a_k,b_1,\dots,bl\in R,s_1,\dots,s_k\in S,t_1,\dots,t_l\in T$. Hence

$$ab=\left(\sum_{i=1}^{k} a_is_i\right)\left(\sum_{j=1}^{l} b_jt_j\right)=\sum_{i=1}^{k}\sum_{j=1}^{l} a_is_ib_jt_j=\sum_{i=1}^{k}\sum_{j=1}^{l}(a_ib_j)(s_it_j)$$

since R is commutative. Hence $ab\in K$, so a generating set for IJ is contained in K, which means $K\supseteq IJ$. Thus $K=IJ$, as required. ∎

Proposition 10.12. *Let R be a ring and let $I,J\subseteq R$ be ideals. Then*

$$IJ\subseteq I\cap J.$$

Proof. Given any $a\in I,b\in J$, $ab\in I\cap J$ since I,J are ideals, so $I\cap J$ contains a generating set for IJ. But $I\cap J$ is an intersection of ideals so an ideal, and in particular closed under operations. Thus $IJ\subseteq I\cap J$. ∎

Generalized Chinese Remainder Theorem

(10.7) Chinese Remainder Theorem

From group theory, given coprime $m, n \in \mathbb{N} \cup \{0\}$, we know that

$$\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

In particular, the canonical (group) isomorphism is defined as follows. Let $\varphi : \mathbb{Z}/mn\mathbb{Z} \to n\mathbb{Z}/mn\mathbb{Z} \times m\mathbb{Z}/mn\mathbb{Z}$ be defined by

$$x \mapsto (nx, mx)$$

for all $x \in \mathbb{Z}/mn\mathbb{Z}$ and let $\psi : n\mathbb{Z}/mn\mathbb{Z} \times m\mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ be defined by

$$(nx, mx) \mapsto (x, x)$$

for all $(nx, mx) \in n\mathbb{Z}/mn\mathbb{Z} \times m\mathbb{Z}/mn\mathbb{Z}$. Then the composition $\psi \circ \varphi$ is the canonical (group) isomorphism. In particular, it implies the following result.

Theorem 10.13. Chinese Remainder Theorem

Let $n, m \in \mathbb{N} \cup \{0\}$ be coprime. Then for every $a \in \{0, \ldots, m-1\}, b \in \{0, \ldots, n-1\}$, there exists unique $x \in \{0, \ldots, mn-1\}$ such that

$$\begin{cases} x \equiv a \bmod m \\ x \equiv b \bmod n \end{cases}.$$

Observe that $\mathbb{Z}/mn\mathbb{Z}$ and $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ are rings, so we may ask if $\psi \circ \varphi$ is a ring isomorphism as well. More generally, we can also ask if there is any connection to ring theory from the Chinese remainder theorem. First, observe that one of the hypothesis is that m, n are coprime. But it is well-known result that

$$m, n \text{ are coprime} \iff \gcd(m, n) = 1 \iff \operatorname{lcm}(m, n) = mn,$$

where $\operatorname{lcm}(m, n)$ denotes the *least common multiple* of m, n, the smallest nonnegative integer $k \in \mathbb{N} \cup \{0\}$ such that $k = xm = yn$ for some $x, y \in \mathbb{Z}$. But $k = xm$ if and only if $k \in (m)$ and $k = yn$ if and only if $k \in (n)$. This means, $k = \operatorname{lcm}(m, n)$ if and only if

$$(m) \cap (n) = (k).$$

In particular, m, n are coprime if and only if

$$(m) \cap (n) = (mn).$$

But $(m)(n) = (mn)$ so

$$(m) \cap (n) = (m)(n)$$

if and only if m, n are coprime. Hence we can restate the group theory version of the Chinese remainder theorem as follows: *given $n, m \in \mathbb{N} \cup \{0\}$, if $(m)(n) = (m) \cap (n)$, then $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.* We however want a statement for general rings. To do so, we first record the following results.

Proposition 10.14.

Let R, S, T be rings and let $\varphi : R \to S, \psi : R \to T$ be homomorphisms. Then $\zeta : R \to S \times T$ by

$$\zeta(r) = (\varphi(r), \psi(r))$$

for all $r \in R$ is a homomorphism.

Product of Homomorphisms

Def'n 10.8. Let R, S, T be rings and let $\varphi : R \to S, \psi : R \to T$ be homomorphisms. Then the ***product*** of φ, ψ, denoted as $\varphi \times \psi$, is defined by

$$(\varphi \times \psi)(r) = (\varphi(r), \psi(r))$$

for all $r \in R$.

Proposition 10.15. *Let R be a ring and let $I, J \subseteq R$ be ideals. Let $\varphi = q_1 \times q_2$, where $q_1 : R \to R/I, q_2 : R \to R/J$ are the quotient maps.*

(a) $\ker(\varphi) = I \cap J$.

(b) There exists a homomorphism $\psi : R/IJ \to R/I \times R/J$ such that

$$\psi([x]) = (q_1(x), q_2(x))$$

for all $[x] \in R/IJ$ and that $\ker(\psi) = I \cap J/IJ$.

Proof.

(a) Let $x \in R$. Then observe that

$$x \in \ker(\varphi) \iff (q_1(x), q_2(x)) = (0,0) \iff x \in \ker(q_1) \cap \ker(q_2) \iff x \in I \cap J.$$

(b) Since $IJ \subseteq I \cap J = \ker(\varphi)$, there exists $\psi : R/IJ \to R/I \times R/J$ such that

$$\psi([x]) = \varphi(x)$$

for all $x \in R$ by the universal property of quotients. But by the correspondence theorem

$$\ker(\psi) = I \cap J/IJ.$$ ∎

We want some sufficient condition for the homomorphism ψ in Proposition 10.15 to be an isomorphism. We immediately observe that the condition $I \cap J = IJ$ is necessary, since $\ker(\psi)$ has to be trivial in order for ψ to be injective, and $\ker(\psi) = I \cap J/IJ$. However, this condition is not sufficient, as the following example shows.

(EX 10.8) Let $R = \mathbb{Z}[x], I = (2), J = (x)$.

- *Claim 1.* $(2) \cap (x) = (2x)$.

  Proof. Clearly $(2x) \subseteq (2) \cap (x)$. Conversely, given any $f \in (2) \cap (x)$, every coefficient of f is even and f does not have a constant term, so

  $$f = \sum_{i=1}^{k} 2a_i x^i$$

  for some $a_1, \ldots, a_k \in \mathbb{Z}$. But this means

  $$f = 2x \sum_{i=1}^{k} a_i x^{i-1} = 2x \sum_{i=0}^{k-1} a_{i-1} x^i$$

  so $f \in (2x)$. Thus $(2x) = (2) \cap (x)$, as desired. ◁

Since $(2)(x) = (2x)$, it immediately follows that $I \cap J = IJ$. So define $\psi : \mathbb{Z}[x]/(2x) \to \mathbb{Z}[x]/(2) \times \mathbb{Z}[x]/(x)$ by

$$\psi([p]) = ([p],[p])$$

for all $[p] \in \mathbb{Z}[x]/(2x)$.

- *Claim 2. ψ is not surjective.*

  Proof. Suppose there exists $p \in \mathbb{Z}[x]$ such that

  $$\psi([p]) = (0,1)$$

  for the sake of contradiction. Since $[p] = 0$ in $\mathbb{Z}[x]/(2)$, every coefficient of p is even. But $p = 1$ in $\mathbb{Z}[x]/(x)$, so the constant term of p is 1. Hence we face a desired contradiction. $\triangleleft$

(10.9) Because $I \cap J = IJ$ is not sufficient, we need to change our approach. For this time, we are going to get our motivation from the famous *Bezout's lemma*: given $m,n \in \mathbb{Z}$, m,n are coprime if and only if there exists $x,y \in \mathbb{Z}$ such that

$$xm + yn = 1.$$

In fact, many well-known proofs of the Chinese remainder theorem utilize this fact.

Proposition 10.16. *Let $n,m \in \mathbb{Z}$. Then* $\gcd(m,n) = 1$ *if and only if $(m)+(n) = \mathbb{Z}$.*

Proof. We know that $(m)+(n)$ is an ideal, so

$$(m)+(n) = \mathbb{Z} \iff 1 \in (m)+(n) \iff \exists x,y \in \mathbb{Z}\,[xm+yn=1].$$ ∎

Def'n 10.9. **Comaximal (Coprime) Ideals**
Let R be a ring and let $I,J \subseteq R$ be ideals. We say I,J are ***comaximal*** (or ***coprime***) if $I+J = R$.

It is immediate from the definition that

$$I,J \text{ are comaximal} \iff 1 \in I+J.$$

Theorem 10.17. Generalized Chinese Remainder Theorem I

Let R be a commutative ring and let $I,J \subseteq R$ be ideals. If I,J are comaximal, then the map $\psi : R/IJ \to R/I \times R/J$ in Proposition 10.15 is an isomorphism, where

$$\psi([r]) = ([r],[r])$$

for all $[r] \in R/IJ$.

Proof. Since I,J are maximal, fix $a \in I, b \in J$ such that $a+b=1$.

- *Claim 1. ψ is surjective.*

  Proof. Given $r \in R$,

  $$ra + rb = r\underbrace{(a+b)}_{=1} = r$$

so

$$r - rb = ra \in I, r - ra = rb \in J.$$

Hence $[r] = [rb]$ in R/I and $[r] = [ra]$ in R/J. But $ra \in I, rb \in J$, so $[rb] = 0$ in R/J and $[ra] = 0$ in R/I. Hence, for all $([r_1], [r_2]) \in R/I \times R/J$, we have

$$\psi([r_1 b + r_2 a]) = ([r_1], [r_2]).$$

◁

- *Claim 2. ψ is injective.*

  Proof. It suffices to show that $I \cap J = IJ$. Let $x \in I \cap J$. Then $x = x(a+b) = xa + xb \in IJ$ since R is commutative. This means $I \cap J \subseteq IJ$. But $IJ \subseteq I \cap J$ clearly, so $I \cap J = IJ$. ∎

(10.10) Continuing the Decomposition

Let $n \in \mathbb{N}$ and let

$$n = \prod_{i=1}^{k} p_i^{a_i}$$

be the prime factorization of n, where $k \in \mathbb{N}, p_1, \ldots, p_k \in \mathbb{N}$ are distinct primes, and $a_1, \ldots, a_k \in \mathbb{N}$. Then by induction

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{a_1}\mathbb{Z} \times \mathbb{Z}/p_2^{a_2} \cdots p_k^{a_k}\mathbb{Z} \cong \cdots \cong \prod_{i=1}^{k} \mathbb{Z}/p_i^{a_i}\mathbb{Z},$$

since $p_i^{a_i}$ is coprime to $p_{i+1}^{a_{i+1}} \cdots p_k^{a_k}$ for all $i \in \{1, \ldots, k-1\}$. This is by the fact that, given $a, b, c \in \mathbb{Z}$, a is coprime to both b, c, then a is coprime to bc. We can generalize this for comaximal ideals.

Proposition 10.18. *Let R be a ring and let $I, J, K \subseteq R$ be ideals. If I, J and I, K are comaximal, then I, JK are comaximal.*

Proof. Since I, J are comaximal, there exist $a \in I, b \in J$ such that $a + b = 1$. Similarly, there exist $a' \in I, c \in K$ such that $a' + c = 1$. So it follows that

$$b = b\left(a' + c\right) = ba' + bc,$$

which means

$$1 = a + b = a + ba' + bc = \underbrace{\left(a + ba'\right)}_{\in I} + \underbrace{bc}_{JK} \in I + JK.$$

∎

This allows us to generalize the Chinese remainder theorem even further.

Theorem 10.19. Generalized Chinese Remainder Theorem II

Let R be a commutative ring and let $I_1, \ldots, I_k \subseteq R$ be ideals, where $k \in \mathbb{N}, k \geq 2$, such that I_i, I_j are comaximal for all distinct $i, j \in \{1, \ldots, k\}$. Then $\psi : R/I_1 \cdots I_k \to \prod_{i=1}^{k} R/I_i$ defined by

$$\psi([r]) = ([r], \ldots, [r])$$

for all $[r] \in R/I_1 \cdots I_k$ is an isomorphism.

This page intentionally left blank.

11.
PIDs and UFDs

Divisors and Greatest Common Divisors

Def'n 11.1. **Divisor** of an Element of a Commutative Ring

Let R be a ring and let $x, y \in R$. We say x ***divides*** y, written as $x|y$, if $y = xr$ for some $r \in R$.

Proposition 11.1. *Let R be a commutative ring and let $x, y \in R$. Then $x|y$ if and only if $y \in (x)$.*

Def'n 11.2. **Associates** of a Commutative Ring

Let R be a commutative ring and let $x, y \in R$. We say x, y are ***associates***, denoted as $x \sim y$, if $y = ux$ for some unit $u \in R$.

Proposition 11.2. *Let R be a commutative ring and let $x_1, x_2, y_1, y_2 \in R$.*

(a) $\sim$ is an equivalence relation.

(b) If $x_1 \sim x_2, y_1 \sim y_2$, then $x_1|y_1$ if and only if $x_2|y_2$.

(c) If $x \sim y$, then $x|y$ and $y|x$.

Proposition 11.3. *Let R be a commutative ring and let $x, y \in R$. Then $x|y$ and $y|x$ if and only if $(x) = (y)$.*

Proposition 11.4. Characterization of Associates in Integral Domains

Let R be a domain and let $x, y \in R$. Then $x \sim y$ if and only if $x|y$ and $y|x$.

Proof. The forward direction is provided by (c) of Proposition 11.2. For the reverse direction, suppose

$$y = xr, x = yt$$

for some $r, t \in R$. It suffices to show r, t are units. We may assume $y = 0$, since otherwise $x = 0$ as well. Now

$$y = xr = yrt,$$

so

$$(1 - rt)y = 0.$$

Since $y \neq 0$ and R is a domain, $1 - rt = 0$. Thus r, t are units, as required. ∎

Def'n 11.3. **Common Divisor, Greatest Common Divisor** of Elements of a Commutative Ring

Let R be a commutative ring and let $a, b \in R$. $d \in R$ is called a ***common divisor*** of a, b if $d|a, d|b$. We say d is a ***greatest common divisor*** if for all $d' \in R$ that is a common divisor of a, b, $d'|d$.

(11.1) For arbitrary rings, greatest common divisor of two elements need not be unique. We however write

$$d = \gcd(x, y)$$

to mean that d is *a* greatest common divisor of x, y.

Proposition 11.5. Characterization of Divisors

Let R be a commutative ring and let $a,b,d \in R$. Then the following are equivalent.

(a) d is a common divisor of a,b.

(b) $d|xa+yb$ for all $x,y \in R$.

(c) $(a,b) \subseteq (d)$.

Proof.

- (1) $\iff$ (2) Observe that

$$d|a \wedge d|b \iff \forall x,y \in R\,[d|xa \wedge d|yb] \iff \forall x,y \in R\,[d|xa+yb]\,.$$

- (2) $\iff$ (3) Observe that

$$\forall x,y \in R\,[d|xa+yb] \iff \forall y \in (a,b)\,[d|y] \iff \forall y \in (a,b)\,[y \in (d)]\,.$$ ∎

(11.2) Let R be a domain and let $x,y \in R$. If $d,d' \in R$ are greatest common divisors of x,y, then $d|d', d'|d$. Hence $d \sim d'$, and we say that greatest common divisors in integral domains are *unique up to units*.

Proposition 11.6. Characterization of the Existence of Greatest Common Divisors

Let R be a commutative ring and let $a,b \in R$.

(a) Then a,b have a greatest common divisor if and only if there exists a principal ideal $I \subseteq R$ such that

(i) $(a,b) \subseteq I$; and

(ii) if $J \subseteq R$ is a principal ideal with $(a,b) \in J$, then $I \subseteq J$.

(b) If I exists, then it is unique, and

$$I = (d) \iff d = \gcd(a,b)$$

for all $d \in R$.

Corollary 11.6.1. *Let R be a commutative ring and let $a,b \in R$. If (a,b) is principal, then a greatest common divisor of a,b exists. Consequently, if $d \in R$ is a common divisor of a,b such that $d = xa+yb$ for some $x,y \in R$, then d is a greatest common divisor of a,b.*

Corollary 11.6.2. *Let R be a commutative ring and let $a,b \in R$. If $(a),(b)$ are comaximal, then 1 is a greatest common divisor of a,b.*

Principal Ideal Domains

Def'n 11.4. **Principal Ideal Domain (PID)**
Let R be an integral domain. We say R is a ***principal ideal domain*** if every ideal of R is principal.

(EX 11.3)

(a) $\mathbb{Z}$ is a PID.

(b) For any field $\mathbb{K}$, $\mathbb{K}[x]$ is a PID.

(c) $\mathbb{Z}[x]$ is not a PID, since $(2,x)$ is not principal.

(d) $\mathbb{K}[x,y]$ is not a PID for any field $\mathbb{K}$, since (x,y) is not principal.

Proposition 11.7. *Let R be a PID and let $a,b \in R$.*

(a) a,b has a greatest common divisor.

(b) For any $d \in R$, d is a greatest common divisor of a,b if and only if d is a common divisor of a,b and $d = xa + yb$ for some $x,y \in R$.

Proposition 11.8. *Let R be a PID. Then given any ideal $I \subseteq R$, I is prime if and only if maximal.*

Proof.

- ($\Longrightarrow$) Let $I \subseteq R$ is a nonzero prime ideal and let $J \subseteq R$ be a proper ideal of R containing I. Since R is a PID, $I = (a), J = (b)$ for some $a,b \in R$. Hence

$$(a) = I \subseteq J = (b),$$

implying $a = br$ for some $r \in R$. Since I is prime and $br \in I$, $b \in I$ or $r \in I$. Suppose, for the sake of contradiction, $r \in I$. Then $(r) \subseteq I = (a)$, and since $a = br \in (r)$, $(a) \subseteq (r)$, so $(a) = (r)$. Since R is a domain, $a \sim r$, so $a = ur$ for some unit $u \in R$. So $br = a = ur$, which means $(b-u)r = 0$. Since I is nonzero, $r \neq 0$, so $b = u$. But this means $J = (b) = (u) = R$, a desired contradiction. Hence $b \in I$, implying $J \subseteq I$ as well. This means $I = J$, so I is maximal, as required.

- ($\Longleftarrow$) This direction holds for any arbitrary commutative ring (see Corollary 9.12.1). ∎

Corollary 11.8.1. *Let R be a commutative ring such that $R[x]$ is a PID. Then R is a field.*

Proof. Since $R[x]$ is a PID, $R[x]$ is an integral domain. So as a subring of $R[x]$, R is also an integral domain. Since

$$R \cong R[x]/(x),$$

(x) is prime, so by Proposition 11.8, (x) is maximal. Thus R is a field. ∎

Euclidean Domain

Def'n 11.5. Let R be an integral domain. We say R is a ***Euclidean domain*** if there exists a function $N : R \to \mathbb{N} \cup \{0\}$ such that

(a) $N(0) = 0$; and

(b) for all $x, y \in R$ with $x \neq 0$, $y = qx + r$ for some $q, r \in R$ with $r = 0$ or $N(r) < N(x)$.

We say N is a ***norm*** on R.

Proposition 11.9. *Every Euclidean domain is a PID.*

Proof. Let R be a Euclidean domain and let $I \subseteq R$ be an ideal in R. We may assume I is nontrivial. Let $x \in I$ be such that

$$N(x) = \min\{N(y) : y \in I \setminus \{0\}\}$$

Then for every $y \in I$, $y = qx + r$ for some $q, r \in R$ with $r = 0$ or $N(r) < N(x)$. Since

$$r = y - qx \in I,$$

by the minimality of $N(x)$, $r = 0$. Hence $y = qx$, implying that $I \subseteq (x)$. But $x \in I$ means $(x) \subseteq I$, so $I = (x)$. Thus R is a PID. ∎

Proposition 11.10. *Let $\mathbb{K}$ be a field. Then $\mathbb{K}[x]$ is a Euclidean domain.*

Proof. It is a well-known result that deg is a norm on $\mathbb{K}[x]$. ∎

Corollary 11.10.1. *Let R be a commutative ring. Then the following are equivalent.*

(a) $R[x]$ is a Euclidean domain.

(b) $R[x]$ is a PID.

(c) R is a field.

Proof. This result immediately follows from Corollary 11.8.1, Proposition 11.9, Proposition 11.10. ∎

(11.4) Euclidean domains are nice because there is an algorithm called the *Euclidean algorithm* which computes greatest common divisors, runs fast as long as division is fast.

Primes and Irreducibles

(11.5) Let $p \in \mathbb{Z} \setminus \{-1, 0, 1\}$. Recall that prime numbers in $\mathbb{Z}$ have two equivalent definitions.

(a) p is prime if for every $a, b \in \mathbb{Z}$, $p | ab$ implies $p | a$ or $p | b$.

(b) p is prime if $p = ab$ implies a is a unit or b is a unit.

In an arbitrary ring, prime ideals generalize definition (a). But we also want prime *elements*, rather than prime ideals. We also want to generalize definition (b).

Def'n 11.6. Prime, Irreducible, Reducible Elements of an Integral Domain

Let R be an integral domain and let $p \in R$ be nonzero and nonunit.

(a) p is called ***prime*** if for every $a, b \in R$, if $p|ab$, then $p|a$ or $p|b$.

(b) p is called ***irreducible*** if for every $a, b \in R$, if $p = ab$, then one of a, b is a unit.

(c) p is called ***reducible*** if not irreducible.

Proposition 11.11. *Let R be an integral domain and let $p \in R$.*

(a) p is prime if and only if p is nonzero and (p) is prime.

(b) Given any $q \in R$ such that p, q are associates, p is prime (resp. irreducible) if and only if q is prime (resp. irreducible).

(c) If p is prime, then p is irreducible.

Proposition 11.12. *Let R be a PID and let $p \in R$. Then p is irreducible if and only if prime.*

Proof. The reverse direction is provided by (c) of Proposition 11.11. For the forward direction, suppose p is irreducible and let $I \subsetneq R$ be an ideal containing (p). Since R is a PID, there exists $q \in R$ such that $I = (q)$. But $p \in I$, so $p = kq$ for some $k \in R$. Since p is irreducible, at least one of k, q is a unit. If q is a unit, then $I = R$. On the other hand, if k is a unit, then p, q are associates, so $(p) = (q)$. Hence (p) is maximal, implying that (p) is prime. Hence p is prime by (a) of Proposition 11.11. ∎

Def'n 11.7. Complete Factorization into Irreducibles

Let R be an integral domain and let $r \in R$.

(a) We say r has a ***complete factorization into irreducibles*** if $r = r_1 \cdots r_k$ for some $k \in \mathbb{N}$ and irreducible $r_1, \ldots, r_k \in R$.

(b) We say R has ***complete factorizations into irreducibles*** if every nonzero element of R has a complete factorization.[a]

[a] In fact, we only have to require nonzero nonunits to have a complete factorization into irreducibles, since units can be factorized into irreducibles in a trivial way.

Proposition 11.13. *Let R be an integral domain and let $r \in R$ be an irreducible that can be written as a product of primes. Then r is a prime.*

Proof. Write

$$r = p_1 \cdots p_k$$

for some primes $p_1, \ldots, p_k \in R$, where $k \in \mathbb{N}$. For the sake of contradiction, assume $k \geq 2$. Then $(p_1 \cdots p_{k-1})$ or p_k is a unit, since r is irreducible. Since primes cannot be units, p_k is not a unit. But if $p_1 \cdots p_{k-1}$ is a unit, then $p_i | 1$ for all $i \in \{1, \ldots, k-1\}$, so p_i is a unit for all $i \in \{1, \ldots, k-1\}$. Thus we have a contradiction, implying that $k = 1$ (i.e. r is prime). ∎

(11.6) Complete Factorization into Irreducibles

Let R be an integral domain and let $r \in R$ be nonzero and nonunit. We desire to show that r can be factored into a product of irreducibles. To do so, we propose the following algorithm.

(a) If r is irreducible, then we are done.

(b) Otherwise, $r = r_1r_2$ for some nonunits $r_1, r_2 \in R$ (of course, r_1, r_2 are nonzero).

(c) Start over at (a) and try to write r_1, r_2 as a product of irreducibles.

To show that this algorithm works, it suffices to show that it terminates.

Proposition 11.14. *Let R be a domain and let $r \in R$ be nonzero. Write $r = r_1r_2$ for some $r_1, r_2 \in R$. Then $(r) = (r_2)$ if and only if r_1 is a unit.*

Proof. If r_1 is a unit, then r, r_2 are associates, so $(r) = (r_2)$. Conversely, if $(r) = (r_2)$, then $r = ur_2$ for some unit $u \in R$, so

$$0 = r - r = r_1r_2 - ur_2 = (r_1 - u)r_2.$$

Since r, r_2 are nonzero, $r_1 = u$ by cancellation, so r_1 is a unit. ∎

By Proposition 11.14, given any reducible $r \in R$ such that $r = r_1r_2$ for some nonunits $r_1, r_2 \in R$, (r) is a proper subset of $(r_1), (r_2)$. As a result, if the algorithm does not terminate, then we have an infinite strictly increasing sequence of principal ideals

$$(r) \subset (r_{i_2}) \subset (r_{i_3}) \subset \cdots$$

in R. Hence to make our algorithm work, we have to ensure that R does not admit such sequence.

Def'n 11.8. **Ascending Chain Condition for Principal Ideals** for an Integral Domain

Let R be an integral domain. We say R satisfies the ***ascending chain condition for principal ideals*** if there does not exist an infinite strictly increasing sequence

$$I_1 \subset I_2 \subset \cdots$$

of principal ideals $I_1, I_2, \ldots \subseteq R$.

Proposition 11.15. *Let R be a domain. If R satisfies the ascending chain condition for principal ideals, then R has complete factorizations into irreducibles.*

Proposition 11.16. *Every PID satisfies the ascending chain condition for principal ideals.*

Proof. Let R be a PID and let $I_1, I_2, \ldots \subseteq R$ be principal ideals such that

$$I_1 \subseteq I_2 \subseteq \cdots.$$

Then it suffices to show that there exists $k \in \mathbb{N}$ such that $I_k = I_n$ for all $n \in \mathbb{N}, n \geq k$. We observe that

$$I = \bigcup_{i=1}^{\infty} I_i$$

is an ideal, and since R is a PID, $I = (x)$ for some $x \in R$. This means $x \in I$, so $x \in I_k$ for some $k \in \mathbb{N}$. Then $(x) \subseteq I_k$, so

$$I_k \subseteq I_n \subseteq I = (x) \subseteq I_k$$

for all $n \geq k$, which means $I_k = I_n$ for all $n \geq k$, as required. ∎

Unique Factorizations

(11.7) Unique Factorizations

In $\mathbb{Z}$, factorizations are unique *up to multiplying* $1,-1$. For instance,

$$-12 = -1 \cdot 2^2 \cdot 3 = (-1)^3 \cdot (-2)^2 \cdot 3.$$

Similarly, for an arbitrary integral domain R, we say a complete factorization of $r \in R$ is *unique* to mean that, given two complete factorizations

$$r = a_1 \cdots a_n = b_1 \cdots b_m$$

for some $n,m \in \mathbb{N}$ and irreducibles $a_1,\dots,a_n,b_1,\dots,b_m \in R$, $n=m$ and there is a permutation $\sigma \in S_n$ such that $a_i \sim b_{\sigma(i)}$ for all $i \in \{1,\dots,n\}$. That is, factorizations are unique *up to multiplying units of* R.

Proposition 11.17. *Let R be an integral domain and let $r_1,\dots,r_n \in R$ be irreducible, where $n \in \mathbb{N}$. Then $r_1 \cdots r_n$ is not a unit.*

Proof. A proof is outlined in the proof of Proposition 11.13. ∎

Proposition 11.18. *Let R be an integral domain. If every irreducible in R is prime, then complete factorizations are unique when exist.*

Def'n 11.9. **Unique Factorization Domain**

Let R be an integral domain. We say R is a ***unique factorization domain*** (or ***UFD***) if R has complete factorizations into irreducibles and complete factorizations are unique when exist.

Proposition 11.19. *Every PID is a UFD.*

Proof. We know that

(a) every PID has the ascending chain condition for principal ideals, so has complete factorizations (Proposition 11.15, 11.16); and

(b) every irreducible in any PID is prime, so every PID has unique complete factorizations when they exist (Proposition 11.12, 11.18). ∎

Theorem 11.20. Characterization of UFDs

Let R be a domain. Then R is a UFD if and only if R satisfies the ascending chain condition for principal ideals and every irreducible in R is prime.

Lemma 11.20.1. *Let R be a UFD and let $a,b \in R$ be nonzero nonunits. If $a|b$, then the number of factors in the prime factorization of a is at most the number of factors in the prime factorization of b, and equality holds if and only if $(a) = (b)$.*

Proof. Assume $a|b$, so $ca = b$ for some $c \in R$. We may write

$$a = p_1 \cdots p_m, b = q_1 \cdots q_n, c = ug_1 \cdots g_l$$

for some $m, n \in \mathbb{N}, l \in \mathbb{N} \cup \{0\}$, irreducibles $p_1, \ldots, p_m, q_1, \ldots, q_n, g_1, \ldots, g_l \in R$, and a unit $u \in R$. Then

$$g_1 \cdots g_l u p_1 \cdots p_m = q_1 \cdots q_n,$$

so $m \leq m + l = n$. In particular,

$$(a) = (b) \iff c \in R^\times \iff l = 0 \iff m = n.$$

Proof of Theorem 11.20. The reverse direction is clear. For the forward direction, let R be a UFD. We verify the following claims.

- *Claim 1. Every irreducible in R is prime.*

  Proof. Let $r \in R$ be irreducible and assume $kr = ab$ for some $k, a, b \in R$, where it suffices to show that $r|a$ or $r|b$. We may assume a, b are nonzero and nonunit. So we may write

  $$a = a_1 \cdots a_n, b = b_1 \cdots b_m$$

  for some $n, m \in \mathbb{N}$ and irreducibles $a_1, \ldots, a_n, b_1, \ldots, b_m \in R$. Also write

  $$k = uk_1 \cdots k_l$$

  for some $l \in \mathbb{N}$, irreducibles $k_1, \ldots, k_l \in R$, and a unit $u \in R$. Then we have

  $$uk_1 \cdots k_l r = a_1 \cdots a_n b_1 \cdots b_m.$$

  Since R is a UFD, it follows that $r \sim a_i$ for some $i \in \{1, \ldots, n\}$ or $r \sim b_j$ for some $j \in \{1, \ldots, m\}$. Thus r divides a or b. ◁

- *Claim 2. R satisfies the ascending chain condition for principal ideals.*

  Proof. Let $x_1, x_2, \ldots \in R$ be such that

  $$(x_1) \subseteq (x_2) \subseteq \cdots,$$

  where it suffices to show that there exist $k \in \mathbb{N}$ such that $(x_k) = (x_n)$ for all $n \in \mathbb{N}, n \geq k$. Without loss of generality assume x_i is nonzero and nonunit for all $i \in \mathbb{N}$. For every $i \in \mathbb{N}$, let $f_i \in \mathbb{N}$ be the nubmer of factors in prime factorization of x_i. Since $x_{i+1}|x_i$, by Lemma 11.20.1, $f_i \geq f_{i+1}$ for all $i \in \mathbb{N}$. This means the sequence $(f_i)_{i=1}^\infty$ is nonincreasing. But $(f_i)_{i=1}^\infty$ is bounded below by 1, so there exists $k \in \mathbb{N}$ such that $f_k = f_n$ for all $n \geq k$ by the well-ordering principle. By Lemma 11.20.1, this is equivalent to saying that $(x_k) = (x_n)$ for all $n \geq k$.

Corollary 11.20.2. *Every irreducible in a UFD is prime.*

Proposition 11.21. *Let R be a UFD. Then $R[x]$ is a UFD.*

(11.8) Let R be a UFD and suppose that we are given nonzero $x \in R$. Then

$$x = ug_1 \cdots g_n$$

for some $n \in \mathbb{N} \cup \{0\}$, a unit $u \in R$, and irreducibles $g_1, \ldots, g_n \in R$. But this representation is *inefficient* when there exist distinct $i, j \in \{1, \ldots, n\}$ such that $g_i \sim g_j$. For, $g_i = g_j v$ for some unit $u' \in R$, which means

$$x = ug_1 \cdots g_n = uu' g_1 \cdots g_{i-1} g_{i+1} \cdots g_j^2 \cdots g_n.$$

Continuing this process, we can eventually write

$$x = vh_1^{a_1} \cdots h_m^{a_m}$$

for some $m \in \mathbb{N} \cup \{0\}$, unit $v \in R$, and irreducibles $h_1, \ldots, h_m \in R$, such that h_i, h_j are not associates for all distinct $i, j \in \{1, \ldots, m\}$.

Proposition 11.22. *Let R be a and let $x \in R$ be nonzero. Let $y \in R$.*

(a) There exists $n \in \mathbb{N} \cup \{0\}$, a unit $u \in R$, and irreducibles $g_1, \ldots, g_n \in R$ with g_i, g_j are not associates for all distinct $i, j \in \{1, \ldots, n\}$ such that

$$x = ug_1^{a_1} \cdots g_n^{a_n}.$$

(b) $y | x$ if and only if

$$y = vg_1^{b_1} \cdots g_n^{b_n}$$

for some unit $v \in R$ and $b_1, \ldots, b_n \in \mathbb{N} \cup \{0\}$ such that $b_i \leq a_i$ for all $i \in \{1, \ldots, n\}$.

(c) If $x = y$, then $u = v$ and $a_i = b_i$ for all $i \in \{1, \ldots, n\}$.

Proposition 11.23. *Let R be a UFD and let $u, v \in R$ be units. Let $n \in \mathbb{N} \cup \{0\}$ and let $g_1, \ldots, g_n \in R$ be primes such that g_i, g_j are not associates for all distinct $i, j \in \{1, \ldots, n\}$. Then for every $a_1, \ldots, a_n, b_1, \ldots, b_n \in \mathbb{N} \cup \{0\}$,*

$$g_1^{\min(a_1, b_1)} \cdots g_n^{\min(a_n, b_n)}$$

is a greatest common divisor of $ug_1^{a_1} \cdots g_n^{a_n}, vg_1^{b_1} \cdots g_n^{b_n}$.

12. Polynomial Rings

Irreducible Polynomials

(12.1) We desire to show that $R[x]$ is a UFD for every UFD R. The first step is to study irreducible polynomials. We first consider the case where $R = \mathbb{K}$ for some field $\mathbb{K}$.

Proposition 12.1. *Let $\mathbb{K}$ be a field and let $f \in \mathbb{K}[x]$. Then f is irreducible if and only if $\deg(f) \geq 1$ and $f \neq gh$ for all $g, h \in \mathbb{K}[x]$ with $\deg(g), \deg(h) < \deg(f)$.*

Def'n 12.1. **Root of a Polynomial**
Let R be an integral domain and let $f \in R[x]$. We say $r \in R$ is a ***root*** of f (in R) if $\mathrm{ev}_r(f) = 0$.

Proposition 12.2. *Let R be an integral domain and let $f \in R[x]$ be such that $\deg(f) \geq 2$. If f has a root in R, then f is reducible.*

Proof. Let $c \in R$ be a root of f. Then $f = (x-c)g$ for some $g \in R[x]$. Since $\deg(f) \geq 2$, $\deg(g) \geq 1$. So $x - c, g$ are nonunits, implying that f is reducible. ∎

Recall the following theorem.

Theorem 12.3. Fundamental Theorem of Algebra
Every nonconstant polynomial in $\mathbb{C}[x]$ has a root in $\mathbb{C}$.

Corollary 12.3.1. *The irreducible polynomials over $\mathbb{C}$ are precisely the polynomials of degree 1.*

Corollary 12.3.2. *Let $f \in \mathbb{R}[x]$. Then f is irreducible if and only if $\deg(f) = 1$ or $\deg(f) = 2$ and f does not have a root in $\mathbb{R}$.*

Proposition 12.4. *Let R be an integral domain and let $p \in R[x]$ be constant. Then p is irreducible in $R[x]$ if and only if p is irreucible in $R[x]$.*

Proof. This follows immediately from the fact that $R[x]^\times = R^\times$. ∎

Proposition 12.5. *Let R be an integral domain and let $p \in R[x]$ be constant. Then p is prime in $R[x]$ if and only if p is prime in R.*

Proposition 12.6. *Let R be an integral domain and let $ax + b \in R[x]$. Then $ax + b$ is irreducible if and only if a greatest common divisor of a, b is 1.*

Proof. Observe that

$$ax + b \text{ is irreducible} \iff \text{only common divisor of } a, b \text{ are units.}$$ ∎

Def'n 12.2. **Primitive** Polynomial

Let R be a UFD and let $f \in R[x]$. We say f is ***primitive*** if there does not exist irreducible $r \in R$ such that $r|f$.

(12.2) Equivalently, given $a_0, \ldots, a_n \in R$ where $n \in \mathbb{N}$ and R is a UFD, $\sum_{i=0}^{n} a_i x^i$ is primitive if 1 is a greatest common divisor of $a_0, \ldots, a_n$.

Proposition 12.7. *Let R be a UFD and let $f \in R[x]$ be nonzero. Then there exists $d \in R$ such that $d|f$ and that $\frac{f}{d}$ is primitive.*

Proposition 12.8. *Let R be a UFD and let $f \in R[x]$. If f is irreducible and $\deg(f) \geq 1$, then f is primitive.*

Proof. Suppose $p|f$ for some prime $p \in R$ (so p is prime in $R[x]$ as well). Then $f = p \cdot \frac{f}{p}$ where $p, \frac{f}{p}$ are nonunits, so f is reducible. ∎

Proposition 12.9. *Let R be a UFD and let $f \in R[x]$ be primitive with $\deg(f) \geq 1$. Then f is reducible if and only if $f = gh$ for some $g, h \in R[x]$ with $\deg(g), \deg(h) < \deg(f)$.*

Theorem 12.10. Gauss' Lemma

Let R be a UFD with field of fractions $\mathbb{K}$. If $f \in R[x]$ and $f = gh$ for some $g, h \in \mathbb{K}[x]$, then there exists a unit $u \in \mathbb{K}$ such that $ug, u^{-1}h \in R[x]$.