Introduction to Abstract Algebra

MAT 534

George Miao
gm@miao.dev

Contents

Chapter 1

Sets and relations

1.1 Review on Sets

$B = \{2, 4, 6, 8\}$

$x \in A$

$x \notin A$

$2\mathbb{Z} = \{..., -6, -4, -2, 0, 2, 4, 6, ...\}, 2 \in 2\mathbb{Z}, 3 \notin 2\mathbb{Z}$

$\mathbb{Q} = \left\{\frac{a}{b} \mid a \in \mathbb{Z}, b \in \mathbb{Z} \setminus \{0\}\right\}, 4.4 \in \mathbb{Q}, \pi \notin \mathbb{Q}$

$I = \left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{R} \land \begin{pmatrix} a & b \\ c & d \end{pmatrix} \neq 0\right\}$

$A, \varnothing$

$\mathbb{Q}$ is a proper subset of $\mathbb{R}$.

$A \cap B = \{x \mid x \in A \land x \in B\}$

$A \cap B = \varnothing$

$A \cap B = \{a, 3\}$

$\varnothing$ is disjoint from A.

$A \times B = \{(a, b) \mid a \in A \land b \in B\}$

$\{(a, a), (a, 0), (a, 1), (b, a), (b, 0), (b, 1), (c, a), (c, 0), (c, 1)\}$

Definition. Let A, B be sets, a function $f : A \to B$ is a map that assigns each $a \in A$ to $f(a) \in B$.

A is the **domain** and B is the **codomain** of f.

Definition. $f(A) = \{f(a) \mid a \in A\}$ is the **range** of f.

Definition. f is one-to-one if $f(a_1) = f(a_2) \Rightarrow a_1 = a_2$

Definition. f is a **bijection** if it is both one-to-one and onto; in this case, f has an inverse function $f^{-1}: B \to A$ where

$$f(a) = b \iff a = f^{-1}(b)$$

1.2 Equivalence relation

Theorem (Equivalence relation)**.** An **Equivalence relation** $\sim$ on a set A is

1. (Reflexive) $a \sim a$
2. (Symmetric) $a \sim b \Rightarrow b \sim a$
3. (Transitive) $a \sim b, b \sim c \Rightarrow a \sim c$

Remark. Equality "=" is the strongest equivalence relation

Example (Eq. rel. 1)**.** $S = \{\Delta \text{ in the plane}\}$, $\sim$ can be defined as

$$\Delta_1 \sim \Delta_2 \iff \Delta_1, \Delta_2 \text{ are similar}$$

Example (Eq. rel. 2)**.** Define $\equiv$ on $\mathbb{Z}$ by

$$\begin{aligned} a \equiv b &\iff a - b \text{ is even} \\ &\iff a - b = 2n \text{ for some } n \in \mathbb{Z} \end{aligned}$$

Definition (Equivalence class)**.** $\sim$ on A and $a \in A$, the equivalence class of a is

$$\overline{a} := \{b \in A \mid a \sim b\}$$

Remark. Equivalence classes partition the set.

Example ($\sim$ on $\mathbb{Z}$)**.** $5 \in [1] = \{\text{odd integers}\} = [5] = [-17] = \ldots$

1.3 Binary Operation

Definition (Binary Operation)**.** Let S be a set. A **binary operation** on S is a function $\star : S \times S \to S$.

For each $(a, b) \in S \times S$, we write "a times b"

$$a \star b := \star\left((a, b)\right)$$

Remark. A binary operation on S is a way to multiply every pair of elements on S and get an element of S.

Example. "+", addition, on $\mathbb{Z}$ is a binary operation. Since the sun of intergers is an interger,

$$2 + (-3) = -1 \in \mathbb{Z}$$

Substraction is also a binary operation on $\mathbb{Z}$, since the difference of integers is an interger.

Example. $M_2(\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{R} \right\}$

Matrix multiplication is a binary operation on $M_2(\mathbb{R})$.

Example. let $C(\mathbb{R}) = \{f : \mathbb{R} \to \mathbb{R} \mid f \text{ continuous}\}$

Function composition, $\circ$ is a binary operation on $C(\mathbb{R})$. i.e. $f, g \in C(\mathbb{R})$, then $f \circ g$ is continuous.

Definition. Let $\star$ be a binary operation on a set S. It is
1. **commutative** if

$$\forall a, b \in S.\ a \star b = b \star a$$

2. **associative** if

$$(a \star b) \star c = a \star (b \star c)$$

Example. "+", addition, on $\mathbb{Z}$ is associative and commutative.

Example. Matrix multiplication is associative and **not** commutative.

Definition. Let $\star$ be a binary on a set S. A subset $H \subseteq S$ is closed under $\star$ if

$$\forall h, g \in H.\ h \star g \in H$$

Example. $\mathbb{R}$ with $\cdot$ is a binary operation. $\mathbb{Z} \subseteq \mathbb{R}$ closed under $\cdot$

Example. $\mathbb{Q}^+$ with $\div$ is a binary operation. $\mathbb{Z}^+ \subseteq \mathbb{Q}^+$ is **not** closed under $\div$

1.4 Isomorphic Binary Structure

Definition (Binary Structure)**.** A **binary structure** $(S, \star)$ is a set S with a binary operation $\star$.

Example. $(\mathbb{R}, +), (M_2, \cdot)$

Definition (Identity Element)**.** An element $e \in S$ is an **identity element** for $\star$ if

$$\forall a \in S.\ e \star a = a \star e = a$$

Example.
- $(\mathbb{R}, +)$ has identity element 0
- $(M_2, \cdot)$ has identity element $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$
- $(\mathbb{Z}, \cdot)$ has identity element 1

Theorem. If $(S, \star)$ has an identity element, then it is unique.

proof. Assume $e, e' \in S$ are identity elements for $\star$, to show that $e = e'$. Then

$$e = e \star e' = e'$$

$\square$

Definition (Isomorphic Binary Structure)**.** Let $(S, \star)$ and $(T, \cdot)$ be binary structures. We say they are **isomorphic**, denoted by $S \cong T$, if there is a bijection $f : S \to T$ such that

$$\forall a, b \in S.\ f(a \star b) = f(a) \cdot f(b)$$

In this case, f is called an **isomorphism**.

Remark. $S \cong T$ means that S and T are the same in terms of their binary operation up to relabeling.

Theorem . If $f : (S, \star) \to (T, \star)$ is an isomorphism of binary structures, then the inverse bijection $f^{-1} : T \to S$ is an isomorphism. That is

$$\forall x, y \in T.\ f^{-1}(a \cdot b) = f^{-1}(a) \star f^{-1}(b)$$

proof. Exercise (see note on blackboard) $\square$

Chapter 2

Groups and subgroups

2.1 Groups

Definition (Group). A group $(G, \cdot)$ is a set G with a binary operation $\cdot$ on G such that
1) $\cdot$ is associative
2) has an identity element $e \in G$ s.t. $\forall a \in G.\ a \cdot e = e \cdot a = a$
3) has inverses $\forall g \in G.\ g \cdot g^{-1} = g^{-1} \cdot g = e$

We say a group $(G, \cdot)$ is **abelian** if $\cdot$ is commutative.

Example. $(\mathbb{Z}, +)$ is an abelian group
- $+$ is associative and commutative
- 0 is the identity element
- The inverse of $a \in \mathbb{Z}$ is $-a$

$(\mathbb{Q}, +)$ and $(\mathbb{R}, +)$ are also abelian groups

Example. $(\mathbb{R}^+, \cdot)$ is abelian group.
- $\cdot$ is associative and commutative
- 1 is the identity element
- The inverse of $a \in \mathbb{R}^+$ is $\frac{1}{a}$

Example. Let

$$S = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(\mathbb{R}) \mid ad - bc \neq 0 \right\}$$

Then $(S, \cdot)$ is a group is an example of a non-abelian group.
- $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is the identity element
- The inverse of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is $\frac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$

Example. $S = \{A \in M_n(\mathbb{R}) \mid \det(A) \neq 0\}$ is a group under matrix multiplication.

Example. $S_3 = \{\text{bijection from } \{1,2,3\} \text{ to itself}\}$ with composition as the binary operation is a group. There are 3! elements in S_3.

Proposition.
1. The identity element of a group is unique.
2. Inverses are unique.
3. Cancellation law: $a \cdot b = a \cdot c \Rightarrow b = c$
4. $g^{(-1)^{-1}}$ = g
5. $(g \cdot h)^{-1} = h^{-1} \cdot g^{-1}$

2.2 Subgroups

Definition (Order)**.** The **order** of a group G is

$$|G| = \begin{cases} \text{number of elements in } \; G & \text{if } G \text{ finite} \\ \infty & \text{if } G \text{ infinite} \end{cases}$$

Definition (subgroup)**.** Let $(G, \cdot)$ be a group. A **subgroup** of G is a subset $H \subseteq G$ such that the restriction of $\cdot$ on H makes H a group. We write $H \leq G$.

Remark. H being a subgroup of $(G, \cdot)$ means that
1. $\cdot$ is a binary operation on H
2. $e \subseteq H$
3. $\forall h \in H.\ h^{-1} \subseteq H$

Example. $\{-1, 1\}$ is a subgroup of $(\mathbb{R} \setminus \{0\}, \cdot)$. $(-1)^{-1} = -1 \in \{-1, 1\}$.

Example.

$$H := \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \mid a, b \neq 0 \right\} \leq \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid ad - bc \neq 0 \right\}$$

$$\text{Let } \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}, \begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix} \in H$$

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in H$$

$$\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}^{-1} = \begin{bmatrix} \frac{a}{1} & 0 \\ 0 & \frac{b}{1} \end{bmatrix} \in H$$

$$\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \cdot \begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix} = \begin{bmatrix} ac & 0 \\ 0 & bd \end{bmatrix} \in H$$

Definition (Proper subgroup)**.** Let $H \leq G$, we say H is a **proper subgroup** of G if $H \neq G$. We write $H < G$. If $H = \{e\}$, then H is called the **trivial** subgroup. Otherwise H is called a **nontrivial** subgroup.

Theorem (Subgroup test). Let $(G, \bullet)$ be group, and $H \subseteq G$, then H is a subgroup of G iff $H \neq \emptyset$ and $\forall a, b \in H.\ a \bullet b^{-1} \in H$.

Example. Let $H := \left\{ \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \mid a \in \mathbb{R} \right\}$. Then H is a subgroup of $M_2(\mathbb{R})$.

proof. H is not empty. Now take $A = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}, B = \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} \in H$. Then

$$B^{-1} = \begin{bmatrix} 1 & -b \\ 0 & 1 \end{bmatrix}$$

$$AB^{-1} = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & -b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a-b \\ 0 & 1 \end{bmatrix} \in H$$

□

Definition. Let $(G, \bullet)$ be a group and $g \in G$. For $n \in \mathbb{Z}$ define

$$g^n := \begin{cases} \overbrace{g \bullet \ldots \bullet g}^{n \text{ times}} & \text{if } n > 0 \\ e & \text{if } n = 0 \\ \underbrace{(g^{-1}) \bullet \ldots \bullet (g^{-1})}_{n \text{ times}} & \text{if } n < 0 \end{cases}$$

Definition. Let $(G, \bullet)$ be a group and $g \in G$. The **cyclic subgroup generated by g** is

$$\langle g \rangle := \{ g^n \mid n \in \mathbb{Z} \}$$

Example. $G = (\mathbb{Z}, +)$,

$$\begin{aligned} \langle -1 \rangle &= \mathbb{Z} \\ \langle 2 \rangle &= 2\mathbb{Z} \\ \langle 3 \rangle &= 3\mathbb{Z} \\ &\vdots \end{aligned}$$

Example. $G = S_3$,

$$\begin{aligned} \langle (1\ 2) \rangle &= \{ \mathrm{id}, (1\ 2) \} \\ \langle (1\ 2\ 3) \rangle &= \{ \mathrm{id}, (1\ 2\ 3), (1\ 3\ 2) \} \end{aligned}$$

Proposition. For a group G, $\langle g \rangle \leq G$ for all $g \in G$.

proof. Since $g \in \langle g \rangle$, $G \neq \emptyset$. Let $a, b \in \langle g \rangle$, then by definition, $a = g^m$ and $b = g^n$ for some $m, n \in \mathbb{Z}$.

$$
\begin{aligned}
a \bullet b^{-1} &= g^m \bullet (g^n)^{-1} \\
&= g^m \bullet g^{-n} \\
&= g^{m-n} \in \langle g \rangle
\end{aligned}
$$

Thus $ab^{-1} \in \langle g \rangle$ and so by theorem we have $\langle g \rangle \leq G$. □

Definition. A group G is **cyclic** if there exists $g \in G$ such that $G = \langle g \rangle$. In this case, g is called a **generator** of G.

Proposition. Every cyclic group is abelian.

proof. Let G be cyclic, then there is $g \in G$ such that $G = \langle g \rangle$ and $\langle g \rangle$ is abelian. Thus G is abelian. □

Theorem. Every subgroup of a cyclic group is cyclic.

proof. Let G cyclic and $H \leq G$. If $H = \{e\}$, then H is cyclic. Otherwise, let $g \in G$ be a generator of G and m be the smallest positive integer such that $g^m \in H$. Show that $H \subseteq \langle g^m \rangle$. Let $h \in H$, then $h = g^n$ for some $n \in \mathbb{Z}$. Using Division Algorithm on $\mathbb{Z}$, there exists $q, r \in \mathbb{Z}$ with $0 \leq r \leq m$ such that

$$n = qm + r$$

Also, note that $(g^m)^{-q} \in H$ since $(g^m)^{-q} \in \langle g^m \rangle \subseteq H$. Finally, we obtain that

$$(g^m)^{-g} h \in H$$

Now notice

$$
\begin{aligned}
(g^m)^{-q} h &= (g^m)^{-q} g^n \\
&= g^{-mq} \bullet g^n \\
&= g^{-mq} \bullet g^{qm+r} \\
&= g^{-mq+qm+r} \\
&= g^r \in \langle g^m \rangle
\end{aligned}
$$

By the choice of m and since $0 \leq r < m$ with $g^r \in H$, we conclude that $r = 0$. Therefore, $0 = n = gm$ and hence

$$h = g^n = g^{qm} = (g^m)^q \in \langle g^m \rangle$$

thus, $H \subseteq \langle g^m \rangle$ and so $H = \langle g^m \rangle$. Therefore, by definition, H is cyclic. □

Corollary. Every subgroup of $(\mathbb{Z}\ +)$ has the form $n\mathbb{Z} = \langle n \rangle$ for some $n \in \mathbb{Z}$.

Example. Fix $m \in \mathbb{Z}$ with $m > 0$. Let

$$\mathbb{Z}_m = \{0, 1, ..., m-1\}$$

and defines $+$ on $\mathbb{Z}_m$ by $a + b = r$ where $r < m \equiv a + b \pmod m$.

Remark. $+$ is an associative, commutative binary operation on $\mathbb{Z}_m$. Also 0 is the identity element and $a^{-1} = m - a$ is the inverse of a.

Definition. Let $(G, \cdot), (H, \star)$ be groups, we say G is **isomorphic** to H if they are isomorphic as binary structures. We write $G \cong H$.

Remark. $G \cong H$ means there is a bijection $f : G \to H$, called a group isomorphism, such that

$$f(g_1 \cdot g_2) = f(g_1) \star f(g_2)$$

for all $g_1, g_2 \in G$.

Example. let $G = (\mathbb{Z}_2, +)$, $H = (\{-1, 1\}, \cdot)$, claim $G \cong H$.

proof. Define $f : \mathbb{Z}_2 \to \{-1, 1\}$ be $f(0) = 1$ and $f(1) = -1$. Then

$$\begin{aligned} f(0+0) &= f(0) = 1 = 1 \cdot 1 = f(0) \cdot f(0) \\ f(1+0) &= f(1) = -1 = -1 \cdot 1 = f(1) \cdot f(0) \\ f(1+1) &= f(1) = 1 = -1 \cdot -1 = f(0) \cdot f(0)) \end{aligned}$$

thus f is an isomorphism. □

Example. $\mathbb{Z}_6 \not\cong S_3$ because $\mathbb{Z}_6$ is abelian and cyclic and S_3 is not.

Example. Let $G = \mathbb{Z}_4$, $H = (\{\pm i, \pm 1\}, \cdot)$, $G \cong H$ by

$$\begin{aligned} f : G &\longrightarrow H \\ 0 &\longmapsto 1 \\ 1 &\longmapsto i \\ 2 &\longmapsto -1 \\ 3 &\longmapsto -i \end{aligned}$$

Definition (Order of group element)**.** Let G be a group and $g \in G$, then **order of g** is the smallest positive integer such that $g^n = e$. If there is no m then $|g| := \infty$.

Example. $G = \mathbb{Z}_4$, then $|2| = 1$, $|3| = 4$, $|1| = 4$, $|0| = 1$.

Example. $G = S_3$, $|(123)| = 3$

Lemma. Let G be a group and $g \in G$ where $|g| = m < \infty$. Then

$$\langle g \rangle = \{e, g, g^2, ..., g^{m-1}\}$$

Theorem. Let $G = \langle g \rangle$ cyclic, then

$$G \cong \begin{cases} \mathbb{Z} & \text{if } |G| = \infty \\ \mathbb{Z}_n & \text{if } |G| = n \end{cases}$$

and more over, when $G \cong \mathbb{Z}_m$ then $|g| = m$.

proof. When $|G| = \infty$, want to show $G \cong \mathbb{Z}$. Define $f : \mathbb{Z} \to G$ by $f(n) = g^n$. Then

$$f(n+m) = g^{n+m} = g^n \cdot g^m = f(n) + f(m)$$

It's clear that f is surjective. Still need to show it's injective. Suppose it's not, then there're $g^k, g^n \in G$ where $k \neq n$ and $f(k) = f(n)$. But

$$f(g^k) = f(g^n) \Rightarrow g^k = g^n \Rightarrow g^{k-n} = e$$

which means $|g| \leq k - n < \infty$, a contradiction. Thus f is injective, hence an isomorphism. □

Fact (Euclidean Algorithm)**.** $m, n \in \mathbb{Z}$, their gcd is denoted by $\gcd(m, n)$ is the largest integer that divides both m and n. There exists $a, b \in \mathbb{Z}$ such that

$$\gcd(m, n) = am + bn$$

we say m and n are **relatively prime** if $\gcd(m, n) = 1$.

Example. $\gcd(5, 7) = 1$, $5, 7$ relatively prime.

$$1 = 3 \cdot 5 + (-2) \cdot 7$$

Theorem. Let $G = \langle g \rangle$ with $G \cong \mathbb{Z}_m$, then

$$|g^n| = \frac{m}{\gcd(m, n)}$$

In particular, g^n is a generator for G iff m, n are relatively prime.

Example. $\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$, the theorem says $1, 3, 5, 7$ are generators! Also, it says

$$|2| = \frac{8}{\gcd(8, 2)} = 4$$

Definition. Let $m \in \mathbb{Z}$ with $m > 0$. Define

$$\varphi(m) = |\{n \in \mathbb{Z} \mid 0 \leq n < m \wedge \gcd(m, n) = 1\}|$$

Corollary. If $G \cong \mathbb{Z}_m$, then G has $\varphi(m)$ generators.

Fact. If $k, m > 0 \in \mathbb{Z}$ and $\gcd(k, m) = 1$, then

$$\varphi(km) = \varphi(k)\varphi(m)$$

Example. The **Klein 4-group** is

$$V_4 := \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \right\}$$

with matrix multiplication. It is a subgroup of $M_2(\mathbb{R})$.

Remark. V_4 is the smallest group that is not cyclic.

2.3 Generating sets

Proposition. Let G be a group and consider a collection of subgroups $\{H_i\}_{i \in I}$ of G. Then $\bigcap_{i \in I} H_i$ is a subgroup of G. In particular, if $H, K \leq G$ then $H \cap K \leq G$.

proof. Since each H_i is a subgroup of G, we have $e \in H_i$ for all $i \in I$. Hence by definition, $e \in \bigcap_{i \in I} H_i$, therefore $\bigcap_{i \in I} H_i \neq \emptyset$. Let $a, b \in \bigcap_{i \in I} H_i$. By definition, $a, b \in H_i$ for all $i \in I$. Also, since H_i is a subgroup and $b \in H_i$ for all $i \in I$, we have that $b^{-1} \in H_i$ for all $i \in I$. Thus $ab^{-1} \in H_i$ for all $i \in I$ and so $ab^{-1} \in \bigcap_{i \in I} H_i$. Therefore, by the subgroup test, $\bigcap_{i \in I} H_i \leq G$. $\square$

Definition. The **subgroup generated by S** is

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

That is, $\langle S \rangle$ is the intersection over all subgroups of G containing S when $S = \{a_1, ..., a_n\}$, we write $\langle a_1, ..., a_n \rangle$ for $\langle S \rangle$.

Remark. $\langle S \rangle$ is the smallest subgroup of G containing S.

Fact. $S \leq H \Rightarrow \langle S \rangle \leq H$

Proposition. Let n be a positive number

Every permutation is a product of transpositions. That is,

$$\{(i \;\; j) : 1 \leq i \leq j \leq n\}$$

is a generating set of S_n.

2.4 Orbits, Cycles and Alternating Groups

Proposition. No permutation is a product of an even number of transpositions and a product of an odd number of transpositions.

proof. Let $\sigma \in S_n$ and write

$$\sigma = \tau_1 \tau_2 ... \tau_m \text{ with each } \tau_i \text{ a transposition}$$

Think of σ or each τ_i as permuting the standard basis $e_1, e_2, ..., e_n$ for $\mathbb{R}^n$, and write A_σ or A_{τ_i} as the corresponding matrix. Then

$$A_\sigma = A_{\tau_1} A_{\tau_2} ... A_{\tau_m}$$

and

$$\begin{aligned} \det(A_\tau) &= \det\left(A_{\tau_1}\right) \det\left(A_{\tau_2}\right) ... \det\left(A_{\tau_m}\right) \\ &= (-1)^m \end{aligned}$$

Since $\det(A_\tau)$ is a well-defined function on S_n, it follows that any choice is either even or odd.

□

Definition. Let $\sigma \in S_n$ and write $\sigma = \tau_1 \tau_2 ... \tau_m$ where each τ_i is a transposition. If m is even, then σ is called an **even permutation** and if m is odd, then σ is called an **odd permutation**.

Example. $\sigma = (1\ 2\ 3)(4\ 5) = (1\ 2)(2\ 3)(4\ 5)$, σ is odd

Example. id is a product of 0 transpositions, so it is even.

Example. Transpositions are odd.

Example. $\sigma = (1\ 2\ 3\ 4\ 5) = (1\ 2)(2\ 3)(3\ 4)(4\ 5)$

Definition (Alternating Groups)**.** The **alternating group** A_n is the set of all even permutations in S_n

$$A_n := \{\sigma \in S_n \mid \sigma \text{ is even}\}$$

Example. $A_3 = \{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2)\}$

Example. $A_4 = \{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2), (1\ 3\ 4), ...\}$

Proposition. A_n is always a subgroup of S_n with order $\frac{n!}{2}$.

2.5 Cosets and Lagrange's Theorem

Definition (Coset). Fix a group G and $H \leq G$. For $g \in G$, define the left coset H containing g to be

$$g \cdot H := \{gh \mid h \in H\}$$

the right coset H containing g to be

$$H \cdot g := \{hg \mid h \in H\}$$

Example. $G = \langle \mathbb{Z}, + \rangle$ and $H = 4\mathbb{Z} = \langle 4 \rangle$. Find the left coset of H.

$$\begin{aligned} 0 + H &= \{..., -8, -4, 0, 4, 8, ...\} \\ 1 + H &= \{..., -7, -3, 1, 5, 9, ...\} \\ 2 + H &= \{..., -6, -2, 2, 6, 10, ...\} \\ 3 + H &= \{..., -5, -1, 3, 7, 11, ...\} \\ 4 + H &= 0 + H \end{aligned}$$

Example. $G = S_3$ and $H = \langle (1\ 2\ 3) \rangle$,

$$\begin{aligned} H = \operatorname{id} H &= \{\operatorname{id}, (1\ 2\ 3), (1\ 3\ 2)\} \\ (1\ 3)H = (1\ 2)H &= \{(1\ 2), (2\ 3), (1\ 3)\} \end{aligned}$$

Lemma.
1. $aH \neq \varnothing$ for all $a \in G$
2. $aH = bH \iff a^{-1}b \in H$
3. If $aH \cap bH \neq \varnothing$, then $aH = bH$
4. $\bigcup_{a \in G} aH = G$

proof.
1. $e \in H$ since $H \leq G$ and hence

$$a = a \cdot e \in aH$$

thus $aH \neq \varnothing$ for all $a \in G$.

2. $(\Longrightarrow)$ Assume $aH = bH$. Notice that $b = b \cdot e \in bH$ and since $bH = aH$, we have $b \in aH$. By definition of H, there exists $h \in H$ such that

$$b = ah$$

Multiplying both sides a^{-1} yields:

$$\begin{aligned} a^{-1}b &= a^{-1}(ah) \\ &= (a^{-1}a)h \\ &= eh \end{aligned}$$

$$= h$$

Thus, $a^{-1}b = h \in H$

($\Longleftarrow$) Omitted

3. Assume $aH \cap bH \neq \emptyset$, there exists $x \in aH \cap bH$. By definition there exists $h_1, h_2 \in H$ such that

$$x = ah_1 = bh_2$$

Multiplying both sides by a^{-1} gives:

$$h_1 = a^{-1}ah_1 = a^{-1}bh_2$$

Multiplying h_2^{-1} on the right:

$$h_1 h_2^{-1} = a^{-1}b$$

Since $a^{-1}b \in H$, then by 2

$$aH = bH$$

4. We already showed in 1 that $a \in aH$, so $\bigcup_{a \in G} aH = G$

$\square$

Remark. The lemma also holds for right cosets.

Example. $G = (\mathbb{Z}, +)$ and $H = \langle 5 \rangle$,

$$\begin{aligned} 5\mathbb{Z} = H \quad &= \{..., -5, 0, 5, ...\} \\ 1 + 5\mathbb{Z} = 1 + H &= \{..., -4, 1, 6, ...\} \\ 2 + 5\mathbb{Z} = 2 + H &= \{..., -3, 2, 7, ...\} \\ 3 + 5\mathbb{Z} = 3 + H &= \{..., -2, 3, 8, ...\} \\ 4 + 5\mathbb{Z} = 4 + H &= \{..., -1, 4, 9, ...\} \end{aligned}$$

are the distinct left cosets and partition $\mathbb{Z}$.

Definition (Index). The **index** of $H \leq G$ is the number of distinct left cosets of H in G. We write

$$|G : H|$$

Example. $G = \mathbb{Z}$ and $H = \langle 4 \rangle$, $|G : H| = |\mathbb{Z} : \langle 4 \rangle| = 4$

Theorem (Lagrange's Theorem)**.** Let G be a **finite** group and $H \leq G$, then

$$|G| = |H|\ |G : H|$$

in particular, $|H|$ divides $|G|$.

proof. Let $n = |G : H|$, and $a_1 H, \dots, a_n H$ be the distinct left cosets of H. Note by the lemma

$$G = \bigcup_{i=1}^{n} a_i H \text{ with } a_i H \cap a_j H = \varnothing \text{ for } i \neq j$$

then,

$$|G| = \left| \bigcup_{i=1}^{n} a_i H \right| = \sum_{i=1}^{n} |a_i H|$$

Claim. $|a_i H| = |H|$ for all i

proof. Define $f : H \to a_i H$ by $f(h) = a_i h$. f is surjective and if $f(h_1) = f(h_2)$, $a_i h_1 = a_i h_2$ gives $h_1 = h_2$, hence injective. Therefore, f is a bijection and $|a_i H| = |H|$. □

Thus,

$$|G| = \sum_{i=1}^{n} |H| = n|H| = |G : H|\ |H|$$

□

Example. $G = S_4$,

$$\begin{aligned} |G : \langle (1\ \ 2\ \ 3\ \ 4) \rangle| &= \frac{|G|}{|H|} \\ &= \frac{4!}{4} \\ &= 6 \end{aligned}$$

Example. $G = S_n$ and $H = A_n$,

$$\begin{aligned} |G : H| = |S_n : A_n| &= \frac{n!}{|A_n|} \\ &= \frac{n!}{\frac{n!}{2}} \\ &= 2 \end{aligned}$$

therefore there are two distinct left cosets of A_n in S_n.

Corollary. If $|G| = p$ is prime, then

$$G \cong \mathbb{Z}_p$$

in particular, G is cyclic.

proof. Let $g \in G$ and $g \neq e$, assume $p = |G| = |\langle g \rangle||G : \langle g \rangle|$. Since $|\langle g \rangle| > 1$ and p is prime, then $|\langle g \rangle| = p$ and $|G : \langle g \rangle| = 1$. Finally, since $|\langle g \rangle| = |g| = p$, by a theorem earlier we have that

$$G \cong \mathbb{Z}_p$$

□

Corollary. If $g \in G$, then $|g|$ divides $|G|$

Example. True of False: There exists a group with 24 elements that contains an element of order 9.

Answer. False! Corollary says 9 would have to divide 24.

2.6 Finitely Generated Abelian Groups

Definition (Direct Product)**.** Given groups $G_1, \ldots, G_n$, there **direct product** is the group

$$G_1 \times \ldots \times G_n := \{(g_1, \ldots, g_n) \mid g_i \in G_i\}$$

and

$$(g_1, \ldots, g_n) \bullet (h_1, \ldots, h_n) := (g_1 \bullet h_1, \ldots, g_n \bullet h_n)$$

Theorem. $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ when $\gcd(m, n) = 1$

Example.

$$\begin{aligned} \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_8 &\cong \mathbb{Z}_{15} \times \mathbb{Z}_8 \\ &\cong \mathbb{Z}_{120} \end{aligned}$$

in particular, $\mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_8$ is cyclic.

Example. Is $\mathbb{Z}_p \times \mathbb{Z}_p \cong \mathbb{Z}_{p^2}$?

Answer. No, $\gcd(p, p) = p$, so the theorem doesn't apply.

Corollary. Let $n = p_1^{t_1} \bullet \ldots \bullet p_k^{t_k}$ be a prime factorization of n, then

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{t_1}} \times \ldots \times \mathbb{Z}_{p_k^{t_k}}$$

Theorem. Let $G_1, ..., G_n$ be groups with $g_i \in G_i$. Set $m_i := |g_i| < \infty$ for each $1 \leq i \leq n$. Then

$$|(g_1, ..., g_n)| = \text{lcm}(m_1, ..., m_n)$$

Proposition. G, H groups, then

$$G \times H \cong H \times G$$

Need to know how to prove this. More generally, if $G_1, ..., G_n$ groups, $\sigma \in S_n$,

$$G_1 \times ... \times G_n \cong G_{\sigma(1)} \times ... \times G_{\sigma(n)}$$

Example.

$$\begin{aligned} \mathbb{Z}_3 \times \mathbb{Z}_{20} \times S_4 &\cong S_4 \times \mathbb{Z}_{20} \times \mathbb{Z}_3 \\ &\cong \mathbb{Z}_{20} \times \mathbb{Z}_3 \times S_4 \end{aligned}$$

Theorem (Fundamental Theorem of Finitely Generated Abelian Groups)**.** Let G be a finitely generated abelian group. Then there exists a unique integer n and unique primes $p_1, ..., p_k$ such that

$$G \cong \mathbb{Z}_{p_1^{r_1}} \times ... \times \mathbb{Z}_{p_k^{r_k}} \times \overbrace{\mathbb{Z} \times ... \times \mathbb{Z}}^{t}$$

where p_i is a prime number (not necessarily distinct) and t, n and the factors are **unique up to isomorphism**.

Remark. if G is a finite abelian group, then

$$G \cong \mathbb{Z}_{p_1^{r_1}} \times ... \times \mathbb{Z}_{p_k^{r_k}}$$

with p_i not necessarily distinct primes and decomposition is unique up to reordering.

Example. $\mathbb{Z}_2$ is the only group up to isomorphism of order 2.

Example. $V_4 = \{I_2, A, B, C\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, and Z_4 is another abelian group of order 4.

Example. How many abelian groups of order 36 are there up to isomorphism?

$36 = 2^2 \cdot 3^2 = 2 \cdot 2 \cdot 3^2$. By FTFGAG, there are 4 groups

1. $\mathbb{Z}_4 \times \mathbb{Z}_9$
2. $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9$
3. $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$
4. $\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3$

In group 1-4, what's the largest order an element has in the group?

- 36 since $G \cong \mathbb{Z}_{36}$

- $|(1\ \ 1\ \ 1)| = \mathrm{lcm}(|1|, |1|, |1|) = 18$
- $|(1\ \ 1\ \ 1\ \ 1)| = 6$
- $|(1\ \ 1\ \ 1)| = 12$

Example . How many abelian groups of order 80 are there up to isomorphism?

- $\mathbb{Z}_{16} \times \mathbb{Z}_5$
- $\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_5$
- $\mathbb{Z}_8 \times \mathbb{Z}_2 \times \mathbb{Z}_5$
- $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5$
- $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_5$

Example . How many abelian groups of order 48 are there up to isomorphism?

$48 = 3 \cdot 2^4$

- $\mathbb{Z}_3 \times \mathbb{Z}_{16}$
- $\mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_4$
- $\mathbb{Z}_3 \times \mathbb{Z}_8 \times \mathbb{Z}_2$
- $\mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$
- $\mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

Lemma . Let $G_1, ..., G_n$ be groups and $H_i \leq G_i$ for each $i = 1, ..., n$. Then $H_1 \times ... \times H_n \leq H_1 \times ... \times g_n$

Theorem . Let G be a finite abelian group. If m divides $|G|$, then there exists $H \leq G$ such that $|H| = m$.

proof. By FTFGAG, $G \cong \prod_{i=1}^{n} \mathbb{Z}_{p_i^{r_i}}$ with p_i prime. Since m devides $|G| = \prod_{i=1}^{n} p_i^{a_i}$ with $a_i \leq r_i$.

$$\begin{aligned} |1^{r_i - a_i}| &= \frac{p_i^{r_i}}{\gcd\left(p_i^{r_i}, p_i^{r_i - a_i}\right)} \\ &= \frac{p_i^{r_i}}{p_i^{r_i - a_i}} \\ &= p_i^{a_i} \end{aligned}$$

So in $\mathbb{Z}_{p_i^{r_i}}$, $|\langle 1^{r_i - a_i} \rangle| = p_i^{a_i}$. Set

$$H_i := \langle \rangle$$

$\square$

2.7 Group Homomorphisms

Definition (Group Homomorphism)**.** Let G, H be groups, A **group homomorphism** is a function $\varphi : G \to H$ such that

$$\varphi(g_1 \cdot g_2) = \varphi(g_1) \cdot \varphi(g_2)$$

for all $g_1, g_2 \in G$.

Remark. Every isomorphism is a homomorphism.

Note. A bijective homomorphism is an isomorphism.

Example. $SL_2(\mathbb{R})$ is the special linear group of 2×2 metrices.

$$G = SL_2(\mathbb{R}) := \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{R}, ad - bc \neq 0 \right\}$$

define

$$\begin{aligned} \det : G &\longrightarrow \mathbb{R} \setminus \{0\} \\ A &\longmapsto \det(A) \end{aligned}$$

also, $\mathbb{R} \setminus \{0\}$ is a group with multiplication. From linear algebra, if $A, B \in G$,

$$\det(AB) = \det(A) \cdot \det(B)$$

hence $\det$ is a group homomorphism but not an isomorphism.

Example. Let

$$\varphi : Z \longrightarrow Z_2$$
$$\varphi(n) = \begin{cases} 0 & \text{if } n \text{ is even} \\ 1 & \text{if } n \text{ is odd} \end{cases}$$

This is a group homomorphism. Let $m, n \in \mathbb{Z}$,

Case 1. m, n both even, then $\varphi(m+n) = 0 = 0 + 0 = \varphi(m) + \varphi(n)$
Case 2. m even, n odd, then $\varphi(m+n) = 1 = 0 + 1 = \varphi(m) + \varphi(n)$
Case 3. m, n both odd, then $\varphi(m+n) = 0 = 1 + 1 = \varphi(m) + \varphi(n)$

Therefore , φ is a group homomorphism. Also, φ is not an isomorphism.

Example. Define

$$\begin{aligned} \varphi : \mathbb{Z}_3 &\longrightarrow S_3 \text{ by} \\ 0 &\longmapsto \text{id} \\ 1 &\longmapsto (1\ 2\ 3) \\ 2 &\longmapsto (1\ 3\ 2) \end{aligned}$$

This is a group homomorphism.

Example. $\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}$, $\varphi(n) = 8n$ is a group homomorphism.

Example (Trivial Homomorphism)**.** Let G, H be groups, then the **trivial homomorphism** is the function $\varphi : G \to H$ defined by $\varphi(g) = e_H$ for all $g \in G$.

Definition. Let $\varphi : G \to H$ be a group homomorphism.

The **image** of φ is the set

$$\operatorname{im}(\varphi) := \{\varphi(g) \mid g \in G\}$$

The **kernel** of φ is the set

$$\ker(\varphi) := \{g \in G \mid \varphi(g) = e_H\}$$

Theorem. If $\varphi : G \to H$ is a group homomorphism, then $\varphi(e_G) = e_H$. In particular, $e_G \in \ker(\varphi)$ and $e_H \in \operatorname{im}(\varphi)$.

proof. Consider

$$\begin{aligned} \varphi(e_G) \cdot e_H &= \varphi(e_G) \\ &= \varphi(e_G \cdot e_G) \\ &= \varphi(e_G) \cdot \varphi(e_G) \\ \Rightarrow \varphi(e_G) &= e_H \end{aligned}$$

□

Proposition. Let $\varphi : G \to H$ be a group homomorphism. Then $\operatorname{im}(\varphi) \leq H$ and $\ker(\varphi) \leq G$.

proof. We'll prove $\ker(\varphi) \leq G$. Let $a, b \in \ker(\varphi)$. WTS:

$$\begin{aligned} e_G &\in \ker(\varphi) \\ \forall a, b \in \ker(\varphi).\ ab^{-1} &\in \ker(\varphi) \end{aligned}$$

For first one, $\varphi(e_G) = e_H$, so by definition, $e_G \in \ker(\varphi)$. For second one, let $a, b \in \ker(\varphi)$, then $\varphi(a) = \varphi(b) = e_H$. Thus,

$$\begin{aligned} \varphi(ab^{-1}) &= \varphi(a) \cdot \varphi(b^{-1}) \\ &= e_H \cdot \varphi(b)^{-1} \\ &= e_H \cdot e_H^{-1} \\ &= e_H \end{aligned}$$

Therefore, $ab^{-1} \in \ker(\varphi)$ and so $\ker(\varphi) \leq G$. The proof for $\operatorname{im}(\varphi) \leq H$ is similar. □

Example. Define $\varphi : \mathbb{Z} \to S_4$ given by $\varphi(n) = (1\ 2\ 4)^n$. Check if φ is a group homomorphism:

$$\varphi(m + n) = (1\ 2\ 4)^{m+n}$$

$$\begin{aligned} &= (1\ 2\ 4)^m(1\ 2\ 4)^n \\ &= \varphi(m)\varphi(n) \\ \operatorname{im}(\varphi) &= \langle(1\ 2\ 4)\rangle \\ \ker(\varphi) &= 3\mathbb{Z} = \langle 3\rangle \end{aligned}$$

Example. Fix $n \geq 2$, define $\varphi : S_n \to \mathbb{Z}_2$ given by

$$\varphi(\sigma) = \begin{cases} 0 & \text{if } \sigma \text{ is even} \\ 1 & \text{if } \sigma \text{ is odd} \end{cases}$$

For example, $\varphi((1\ 2)) = 1$, $\varphi((1\ 2\ 3)(1\ 4)(3\ 4)) = 0$.

$$\begin{aligned} \operatorname{im}(\varphi) &= \mathbb{Z}_2 \\ \ker(\varphi) &= A_n \end{aligned}$$

Proposition. A group homomorphism $\varphi : G \to H$ is injective iff

$$\ker(\varphi) = \{e_G\}$$

proof.
($\Longrightarrow$) Assume φ is injective. $e_G \in \ker(\varphi)$ by theorem. If $g \neq e_G$, then $\varphi(g) \neq \varphi(e_G) = e_H$. Thus, $\ker(\varphi) = \{e_G\}$.

($\Longleftarrow$) Assume $\ker(\varphi = \{e_G\})$. WTS: φ injective. Let $\varphi(a) = \varphi(b)$, then

$$\begin{aligned} \varphi(a)^{-1}\varphi(a) &= \varphi(a)^{-1}\varphi(b) \\ \varphi(a)^{-1}\varphi(b) &= e_H \\ \varphi(a^{-1}b) &= e_H \\ a^{-1}b &= e_G \\ a &= b \end{aligned}$$

hence φ is injective. $\square$

Example. $G = (\mathbb{R}^2, +)$ and define

$$\begin{aligned} \varphi : G &\longrightarrow G \\ \begin{bmatrix} a \\ b \end{bmatrix} &\longmapsto \begin{bmatrix} 1 & 1 \\ 2 & 2 \end{bmatrix}\begin{bmatrix} a \\ b \end{bmatrix} \end{aligned}$$

is φ injective? Equivalently, is $\operatorname{null}\left(\begin{bmatrix} 1 & 1 \\ 2 & 2 \end{bmatrix}\right) = \left\{\vec{0}\right\}$?

No, $\begin{bmatrix} 1 & 1 \\ 2 & 2 \end{bmatrix}\begin{bmatrix} 1 \\ -1 \end{bmatrix} = \vec{0}$.

Definition. Let $N \leq G$. We say N is **normal** if $gN = Ng$ for all $g \in G$. In this case, we write $N \trianglelefteq G$.

Example. If G is abelian, then every subgroup $N \leq G$ is normal.

Example. $N \trianglelefteq G$ when $|G : N| = 2$. For example, $\langle(1\ 2\ 3)\rangle = N \leq S_3$, $|S_3 : N| = 2$, so $N \trianglelefteq S_3 = G$. More generally, $|S_n : A_n| = \frac{n!}{\frac{n!}{2}} = 2$ so $A_n \trianglelefteq S_n$.

Example. $H = \langle(1\ 2)\rangle$ is not a normal subgroup of S_3.

$$\begin{aligned}(1\ 3)H &= \{(1\ 3), (1\ 3)(1\ 2)\} \\ &= \{(1\ 3), (1\ 2\ 3)\} \\ H(1\ 3) &= \{(1\ 3), (1\ 2)(1\ 3)\} \\ &= \{(1\ 3), (1\ 3\ 2)\}\end{aligned}$$

so $(1\ 3)H \neq H(1\ 3)$ and H is not normal.

Proposition. If $\varphi : G \longrightarrow H$ is a group homomorphism, then

$$\ker(\varphi) \trianglelefteq G$$

proof. Set $N := \ker(\varphi)$. Let $g \in G$. WTS: $gN = Ng$.

Claim (1). $gN = \{x \in G \mid \varphi(x) = \varphi(g)\} = e^{-1}(\{g\})$

proof. Let $P = \{x \in G \mid \varphi(x) = \varphi(g)\}$. Let $x \in P$, by definition $\varphi(x) = \varphi(g)$, then

$$\begin{aligned}\varphi(g)^{-1}\varphi(x) &= e_H \\ \varphi(g^{-1}x) &= e_H \\ g^{-1}x &\in N \\ x &= (g \cdot g^{-1})x \\ &= g \cdot (g^{-1}x) \in gN \\ \implies P &\subseteq gN\end{aligned}$$

Let $x \in gN$, then

$$\exists y \in N.\ x = gy$$
$$\varphi(x) = \varphi(gy) = \varphi(g)\varphi(y) = \varphi(g)$$

then $x \in P$ and so $gN = P$. $\square$

Claim (2). $Ng = \{x \in G \mid \varphi(x) = \varphi(g)\} = e^{-1}(\{g\})$

proof. Similar to claim (1), leave as exercise. $\square$

By claim (1) and (2), $gN = Ng$ and so $N \trianglelefteq G$. $\square$

Proposition (Quotient Group). Let $N \trianglelefteq G$, then define

$$\frac{G}{N} := \{gN \mid g \in G\}$$

with multiplication given by

$$aN \cdot bN := (ab)N$$

then

1. $\frac{G}{N}$ with multiplication is a group (callled the factor/quotient group).
2. If $\pi : G \longrightarrow \frac{G}{N}$ is given by $\pi(g) = gN$, then π is a onto group homomorphism with $\ker(\pi) = N$. In particular, every normal subgroup is the kernel of some group homomorphism.

proof. First, we'll show the multiplication is well-defined. Let $aN = a'N$ and $bN = b'N$, then

$$a^{-1}a' \in N \text{ and } b^{-1}b' \in N$$

WTS: $(ab)^{-1}a'b' \in N$. Observe that

$$(ab)^{-1}a'b' = b^{-1}a^{-1}a'b'$$

but $a^{-1}a \in N$ and N normal, $b^{-1}N = Nb^{-1}$, then

$$\begin{aligned} b^{-1}(a^{-1}a)b' &= nb^{-1}b' \text{ for some } n \in N \\ &\in N \text{ since } b^{-1}b' \in N \end{aligned}$$

1. Now, check $\frac{G}{N}$ is a group:
   - Associative: let $aN, bN, cN \in \frac{G}{N}$,

$$\begin{aligned} (aN \cdot bN) \cdot cN &= abN \cdot cN \\ &= (ab)cN \\ &= a(bc)N \\ &= aN \cdot (bc)N \\ &= aN \cdot (bN \cdot cN) \end{aligned}$$

   - Identity: $N = eN$ is the identity since $eN \cdot aN = aN \cdot eN = aN$ for all $aN \in \frac{G}{N}$.
   - Inverse: Let $aN \in \frac{G}{N}$, then $a^{-1}N$ is the inverse since $aN \cdot a^{-1}N = a^{-1}N \cdot aN = N$.
2. Let $a, b \in G$ and observe that

$$\begin{aligned} \pi(ab) &= (ab)N \\ &= aN \cdot bN \\ &= \pi(a)\pi(b) \end{aligned}$$

   so π s a group homomorphism. Clearly, π is surjective. Let $aN \in \ker(\pi)$, $\pi(a) = e_{\frac{G}{N}} = N$ iff $a \in N$. Hence $\ker(\pi) = N$.

$\square$

Example. $G = \mathbb{Z}, N = \langle 6 \rangle \trianglelefteq G$. Note that $\frac{G}{N} = \frac{\mathbb{Z}}{\langle 6 \rangle}$ is a group with 6 elements:

$$\begin{gathered} \langle 6 \rangle = 6\mathbb{Z} \\ 1 + 6Z \\ \vdots \\ 5 + 6Z \end{gathered}$$

Here $\frac{\mathbb{Z}}{6\mathbb{Z}}$ is an abelian group with 6 elements. By FTFGAG,

$$\frac{\mathbb{Z}}{6\mathbb{Z}} \cong \mathbb{Z}^6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$$

Example. $G = S_3, N = \langle (1\ \ 2\ \ 3) \rangle$,

$$\frac{G}{N} = \frac{S_3}{\langle (1\ \ 2\ \ 3) \rangle}$$

$$\left| \frac{G}{N} \right| = |G : N| = \frac{|G|}{|N|} = \frac{6}{3} = 2$$

by fact from class, $\frac{G}{N}$ is isomorphic to $\mathbb{Z}_2$.

Example. If $n \geq 2$, show $A_n \trianglelefteq S_n$ and

$$\frac{S_n}{A_n} \cong \mathbb{Z}_2$$

proof. First, $|S_n : A_n| = |S_n \mid A_n| = 2$. By HW4, $\sigma A_n = A_n \sigma$ for all $\sigma \in S_n$, so by def, $A_n \trianglelefteq S_n$ and

$$\left| \frac{S_n}{A_n} \right| = |S_n : A_n| = 2$$

so $\frac{S_n}{A_n}$ is a group with 2 elements, thus isomorphic to $\mathbb{Z}_2$. $\square$

Chapter 3

Rings and Fields

3.1 Rings and Fields

Definition (Ring)**.** A **ring** R is a set with two associative binary operations, addition $(+)$ and multiplication $(\cdot)$ such that:

1. $(R, +)$ is an abelian group
2. (Distributivity) For $a, b, c \in R$, we have

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

   when multiplication is commutative $(\forall a, b \in R.\ a \cdot b = b \cdot a)$, we say R is **commutative**.

Notation:
- ab will be written for $a \cdot b$
- The additive identity of R is called "zero" and is denoted 0, so

$$\forall r \in R.\ 0 + r = r + 0 = r$$

Example .

1. $\mathbb{Z}$ with usual $+$ and $\cdot$ is a commutative ring.
2. Same thing for $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$
3. $M_2(\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{R} \right\}$ is a ring with matrix addition and matrix multiplication, and is not commutative.
4. More generally, $M_n(\mathbb{R})$ is a non-commutative ring when $n \geq 2$.
5. $$\varphi(\mathbb{R}) = \{f : \mathbb{R} \to \mathbb{R} \mid f \text{ continuous}\}$$
$$\varphi^\infty(\mathbb{R}) = \{f : \mathbb{R} \to \mathbb{R} \mid f \text{ diff}\}$$

   these are commutative rings where addition and multiplication are defined pointwise.
6. $\mathbb{Z}_m$ is a commutative ring. The addition and multiplication are modular arithmetic:

$$a + b = r \text{ where } a + b = qm + r \text{ with } 0 \leq r < m$$

$$a \cdot b = r' \text{ where } a \cdot b = q'm + r' \text{ with } 0 \leq r' < m$$

7. If R, S are rings, then $R \times S$ is a ring.
8. If R is a commutative ring, then

$$R[x] = \{a_n x^n + \ldots + a_1 x + a_0 \mid a_i \in R\}$$

is the polynomial with variable x and coefficients in R, then $R[x]$ is a commutative ring.

Proposition. If R is a ring, then every $x \in R$ has a unique additive inverse $-x$ and additive Cancellation holds:

$$x + y = x + z \in R \longrightarrow y = z \in R$$

Proposition. If R is a ring, then the following hold for any $a, b \in R$:

1. $0a = 0$
2. $a \cdot (-b) = (-a) \cdot b$
3. $(-a) \cdot (-b) = ab$

proof.

1. On classwork 8
2. WTS:

$$ab + a(-b) = 0$$
$$ab + (-a)b = 0$$

first, observe that

$$\begin{aligned} ab + a(-b) &= a(b + (-b)) \\ &= a \cdot 0 \\ &= 0 \end{aligned}$$

next,

$$\begin{aligned} ab + (-a)b &= (a + (-a))b \\ &= 0 \cdot b \\ &= 0 \end{aligned}$$

3. $$\begin{aligned} (-a) \cdot (-b) &= -(a \cdot (-b)) \\ &= -(-(a \cdot b)) \\ &= a \cdot b \end{aligned}$$

□

Definition (Ring homomorphism). A function $\varphi : R \to S$ is a **ring homomorphism** if R and S are rings and for all $r_1, r_2 \in R$,

$$\varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2) \qquad \varphi(r_1 \cdot r_2) = \varphi(r_1) \cdot \varphi(r_2)$$

If φ is bijective, then φ is a **ring isomorphism**.

Example. define $\varphi : \mathbb{Z} \to \mathbb{Z}_2$ by

$$\varphi(n) = \begin{cases} 0 \text{ if } n \text{ is even} \\ 1 \text{ if } n \text{ is odd} \end{cases}$$

Definition (Identity)**.** Let R be a ring. We say R has **identity/unity element**, denoted $1 \in R$ if

$$\forall a \in R.\ 1 \cdot a = a \cdot 1 = a$$

that is, 1 is an identity element with respect to multiplication.

Note. $1 \in R$, if exists, is unique.

Example.
- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ have identity elements 1.
- $\mathbb{Z}_m$, 1 is the identity element.
- $M_n(\mathbb{R})$ has identity element I_n.
- $\mathbb{Z}[x]$ has an identity element 1.
- For $m \geq 2$, Consider $R = m \cdot \mathbb{Z}$, R is a ring.

Definition (Unit)**.** Let R be a ring with $1 \in R$. We say $a \in R$ is a **unit** if there exists $b \in R$ such that $ab = ba = 1$. In this case, b is called the **inverse** of a and is denoted a^{-1}, and

$$R^X := \{a \in R \mid a \text{ is a unit}\}$$

Example.

- $\mathbb{Z}^X = \{1, -1\}$
- $\mathbb{Q}^X = \mathbb{Q} \setminus \{0\}, \mathbb{R}^X = \mathbb{R} \setminus \{0\}, \mathbb{C}^X = \mathbb{C} \setminus \{0\}$
- $M_n(\mathbb{R})^X = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid ad - bc \neq 0 \right\}$
- $\mathbb{R} = \mathbb{Z}_4[x]$, $f = 2x + 1 \in R$, $f \cdot f = 1$, so $f \in R^X$

Definition (Zero Divisor)**.** Let R be a commutative ring. We say that $a \in R$ is a **zero-divisor** if there exists $0 \neq b \in R$ such that $ab = 0$

Example.

- The only zero-divisor in $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ is 0
- $R = \mathbb{Z}_4$, $2 \cdot 2 = 4 = 0$, so 2 is a zero-divisor in $\mathbb{Z}_4$

- $R = \mathbb{Z}_6$, $2 \cdot 3 = 6 = 0$, $4 \cdot 3 = 12 = 0$, so 2, 3, and 4 are zero-divisors in $\mathbb{Z}_6$
- $R = M_2(\mathbb{R})$,

$$\underbrace{\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}}_{A} \underbrace{\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}}_{B} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

  then A, B are zero-divisors in $M_2(\mathbb{R})$
- $R = \mathbb{Z}_4[x]$, $f = 2x + 2$, $f \cdot f = 0$, f is a zero-divisor in $\mathbb{Z}_4[x]$
- $R = \mathbb{Z}_9$, zero divisors are $\{0, 3, 6\}$
- $R = \mathbb{Z}_7$, zero divisors are $\{0\}$

Definition (Domain and Field)**.** Let R be commutative ring with $1 \in R$ and $1 \neq 0$. We say that R is a(n) (**integral**) **domain** if the only zero-divisor is 0. We say that R is a **field** if

$$R^X = R \setminus \{0\}$$

that is, every non-zero element has an inverse in a field.

Proposition . In a commutative ring, the units and zero-divisors are disjoint sets.

proof. On homework. □

Corollary . If R is a field, then R is a domain.

Example .
- Not every domain is a field. For example, $\mathbb{Z}$ is a domain but not a field.
- $\mathbb{R}, \mathbb{Q}, \mathbb{C}$ are all fields
- $\mathbb{Z}_7$ is a field
- $\mathbb{Z}_6$ is not a domain (nor a field!)
- $\mathbb{R}[x]$ is a domain but not a field: $f = 1 - x$ does not have an inverse in $\mathbb{R}[x]$

$$f^{-1} = \frac{1}{1 - x} = \sum_{n=0}^{\infty} x^n \notin \mathbb{R}[x]$$

  and $\mathbb{R}[x]^X = \mathbb{R} \setminus \{0\}$

Proposition . If R is a domain and $ab = ac$ with $a \neq 0$, then $b = c$.

proof. Consider

$$\begin{aligned} a(b - c) &= ab - ac \\ &= ab - ab \end{aligned}$$

$$= 0$$

since R is a domain and $a \neq 0$, this forces $b - c = 0$, so $b = c$. □

Proposition. if $m > 0$ is composite, then $\mathbb{Z}_m$ is **not** a domain. If p is a prime, then $\mathbb{Z}_p$ is a field and hence a domain.

proof. Assume m is composite, there exists $a, b \in \mathbb{Z}$ with $m = ab$ and $1 < a < m, 1 < b < m$. Therefore, $a, b \in \mathbb{Z}_m$ and $a, b \neq 0$. But $ab = m = 0$ in $\mathbb{Z}_m$, they are zero-divisors and $\mathbb{Z}_m$ is not a domain.

Now assume p is a prime and let $a \in \mathbb{Z}_p$ with $a \neq 0$. We know that $\gcd(a, p) = 1$. By the Euclidean Algorithm there exists $s, t \in \mathbb{Z}$ with

$$1 = \gcd(a, p) = as + pt$$

use the Division Algorithm to write

$$s = qp + r$$

with $0 < r < p$. Now $r \in \mathbb{Z}_p$ and want to show $ar = 1 \in \mathbb{Z}_p$:

$$\begin{aligned} ar &= ar + aqp \\ &= a(r + qp) \\ &= as \\ &= as + pt \\ &= 1 \end{aligned}$$

hence $r = a^{-1}$ in $\mathbb{Z}_p$. Since a is arbitrary, every non-zero element in $\mathbb{Z}_p$ has an inverse and $\mathbb{Z}_p$ is a field. □

Definition (Characteristic)**.** Let R be a commutative ring and $1 \neq 0$. The **characteristic** of R, denoted $\mathrm{char}(R)$ is the smallest positive interger n such that

$$\underbrace{1 + 1 + \ldots + 1}_{n} = 0$$

if no such n exists, then $\mathrm{char}(R) = 0$.

Example.
- $\mathrm{char}(\mathbb{Z}) = 0$
- $\mathrm{char}(\mathbb{Z}_m) = m$
- $\mathrm{char}(\mathbb{Z}_2 \times \mathbb{Z}_2) = 2$

Proposition. If R is a commutative ring with $1 \neq 0$ and $\mathrm{char}(R) = n > 0$, then

$$\forall a \in R.\ \underbrace{a + a + \ldots + a}_{n} = 0$$

proof. Let $a \in R$ and consider

$$\begin{aligned} \underbrace{a + a + \ldots + a}_{n} &= a \cdot 1 + \ldots + a \cdot 1 \\ &= a \cdot (1 + \ldots + 1) \\ &= a \cdot 0 \\ &= 0 \end{aligned}$$

□

3.2 Fermat's and Euler's Theorems

Definition. Fix $m > 0$. Given $a, b \in \mathbb{Z}$, we write $a \equiv b \bmod m$ "a is equiv. to b mod m" if

$$a + m\mathbb{Z} = b + m\mathbb{Z}$$

equivalently,

$$a \equiv b \bmod m \iff a - b \in m\mathbb{Z}$$

Example.

$$\begin{aligned} 50 &\equiv 2 \bmod 4 \\ &\equiv -2 \bmod 4 \\ &\equiv -6 \bmod 4 \end{aligned}$$

Example. The equation $2x \equiv 1 \bmod 7$ has integer solutions of the form

$$\forall n \in \mathbb{Z}.\ x = 4 + 7n$$

Example. $2x \equiv 0 \bmod 6$,

$$\begin{aligned} x &= 3 + 6n \text{ where } n \in \mathbb{Z} \\ x &= 6n \text{ where } n \in \mathbb{Z} \end{aligned}$$

Remark. If R is a commutative ring with $1 \neq 0$, then R^X is anabelian group with multiplication and identify element 1. In particular, if $\mathbb{F}$ is a field, then

$$\mathbb{F}^X = \mathbb{F} \setminus \{0\} = \{a \in \mathbb{F} : a \neq 0\}$$

is an abelian group.

Theorem (Fermat's Little Theorem)**.** If p is a prime number and $a \in \mathbb{Z}$ with $p \nmid a$ then

$$a^{p-1} \equiv 1 \bmod p$$

proof. Since p is prime, $\frac{\mathbb{Z}}{p\mathbb{Z}}$ is a field. In particular, $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^X$ is an abelian group with $p - 1$ elements. By Lagrange's Theorem,

$$(a + p\mathbb{Z})^{p-1} = 1 + p\mathbb{Z}$$

therefore

$$a^{p-1} \equiv 1 \bmod p$$

□

Corollary. If p is prime and $a \in \mathbb{Z}$ then $a^p \equiv a \bmod p$

proof.
- Case 1: $a \equiv 0 \bmod p$, then $a^p \equiv 0^p \equiv 0 \equiv a \bmod p$
- Case 2: $a \not\equiv 0 \bmod p$. In this case, FLT says $a^{p-1} \equiv 1 \bmod p$. Multiplying both sides by a yields:

$$a^p \equiv a \bmod p$$

□

Example. Find $x \in \mathbb{Z}_{13}$ such that $x \equiv 8^{103} \bmod 13$

Answer.

$$\begin{aligned} 8^{103} &= 8^{96}8^7 \\ &\equiv 8^7 \bmod 13 \\ &= 8^6 \cdot 8 \\ &\equiv (-5)^6 \cdot 8 \bmod 13 \\ &= \left((-5)^2\right)^3 \cdot 8 \\ &\equiv (-1)^3 \cdot 8 \bmod 13 \\ &= -8 \end{aligned}$$

so $x = 5$.

Example. Show $2^{11,213} - 1$ is not divisible by 11.

proof.

$$\begin{aligned} 2^{11,213} &= 2^{11,210} \cdot 2^3 \\ &\equiv 1 \cdot 8 \bmod 11 \\ &= 8 \end{aligned}$$

so $2^{11,213} - 1$ is not divisible by 11. □

Example. Prove that $n^{33} - n$ is divisible by 15 for every $n \in \mathbb{Z}$.

proof. Let's show $n^{33} \equiv n \bmod 3$ and $n^{33} \equiv n \bmod 5$.

For 3:
- Case 1: $n \equiv 0 \bmod 3$, $n^{33} \equiv 0 \equiv n \bmod 3$
- Case 2: $n \not\equiv 0 \bmod 3$,

$$\begin{aligned} n^{33} &= n^{32} \cdot n \\ &\equiv 1 \cdot n \bmod 3 \\ &= n \end{aligned}$$

For 5:

- Case 1: $n \equiv 0 \bmod 5$, $n^{33} \equiv 0 \equiv n \bmod 5$
- Case 2: $n \not\equiv 0 \bmod 5$,

$$\begin{aligned} n^{33} &= n^{32} \cdot n \\ &= \left(n^4\right)^8 \cdot n \\ &\equiv 1 \cdot n \bmod 5 \\ &= n \end{aligned}$$

Therefore, $n^{33} - n$ is divisible by 15. □

Example. Solve for x in $\frac{\mathbb{Z}}{31\mathbb{Z}}$, or $\mathbb{Z}_{31}$:

$$x^{62} - 16 = 0 \text{ in } \mathbb{Z}_{31}$$

use the solution to find all integer solutions to

$$x^{62} - 16 \equiv 0 \bmod 31$$

Answer.

$$\begin{aligned} x^{32} - 16 &\equiv x^2 - 16 \bmod 31 \\ &\equiv (x-4)(x+4) \bmod 31 \\ &\equiv 0 \bmod 31 \end{aligned}$$

since $\frac{\mathbb{Z}}{31\mathbb{Z}}$ is a field,

$$\begin{aligned} x - 4 &\equiv 0 \bmod 31 \\ x + 4 &\equiv 0 \bmod 31 \end{aligned}$$

Recall. Fix $m > 0$, then

$$\begin{aligned} \varphi(m) &= \text{number of positive integers } n < m \text{ with} \gcd(m, n) = 1 \\ &= |\{n \in Z_m : \gcd(n, m = 1)\}| \end{aligned}$$

Example. $\varphi(8) = 4$

Example. p prime, $\varphi(p) = p - 1$

Proposition. Fox $m > 0$ and $a \in \mathbb{Z}_m$, then

- If $\gcd(a, m) \neq 1$, then a is a zero-divisor in $\mathbb{Z}_m$
- If $\gcd(a, m) = 1$, then a is a unit in $\mathbb{Z}_m$

Corollary.

$$\left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right)^X$$

is an abelian group with $\varphi(m)$ elements, the elements are those $a + m\mathbb{Z}$ with $\gcd(a, m) = 1$.

Theorem (Euler's Theorem). If $m > 0$ and $a \in \mathbb{Z}$ with $\gcd(a, m) = 1$, then

$$a^{\varphi(m)} \equiv 1 \bmod m$$

Remark. If m is prime in Euler's Theorem, then on recovers FLT.

Example. $5^{64} \equiv 1 \bmod 8$ by Euler's Theorem since $\varphi(8) = 4$.

Example. find all integers solutions to

$$5x^{31} \equiv 1 \bmod 18$$

here $m = 18$, $\varphi(18) = 6$. Any solution x has $\gcd(x, 18) = 1$. So by Euler's Theorem,

$$x^{\varphi(18)} = x^6 \equiv 1 \bmod 18$$

so

$$5x^{31} \equiv 5x \bmod 18$$

to find x, lets use the Division Algorithm

$$\begin{aligned} 18 &= 3 \cdot 5 + 3 \\ 5 &= 1 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

now run in reverse

$$\begin{aligned} 1 &= 3 - 1 \cdot 2 \\ &= 3 - 1 \cdot (5 - 3) \\ &= 2 \cdot 3 - 1 \cdot 5 \\ &= 2 \cdot (18 - 3 \cdot 5) - 1 \cdot 5 \\ &= 2 \cdot 18 - 7 \cdot 5 \\ 1 &\equiv (-7) \cdot 5 \bmod 18 \end{aligned}$$

all integer solutions are of the form

$$x = -7 + 18n \text{ where } n \in \mathbb{Z}$$

Example. Is 7 a perfect square in the following rings?

1. $\mathbb{Z}_{23}$
2. $\mathbb{Z}_{31}$

Answer.

1. Suppose it is. That is, there exists $x \in \mathbb{Z}$ such that $x^2 \equiv 7 \bmod 23$. By FLT, $x^{22} \equiv 1 \bmod 23$, so we would have

$$\begin{aligned} 1 &\equiv x^{22} \bmod 23 \\ &\equiv \left(x^2\right)^{11} \\ &\equiv 7^{11} \end{aligned}$$

$$\begin{aligned}
&\equiv 7 \cdot (49)^5 \\
&\equiv 7 \cdot 3^5 \\
&\equiv 7 \cdot 27 \cdot 9 \\
&\equiv 7 \cdot 4 \cdot 9 \\
&\equiv 5 \cdot 9 \\
&\equiv -1 \\
&\equiv 22 \bmod 23
\end{aligned}$$

Contradiction. So 7 is not a perfect square in $\mathbb{Z}_{23}$.

2. Yes it is a perfect square in $\mathbb{Z}_{31}$.

$$\begin{aligned}
x^2 &\equiv 7 \bmod 31 \\
&\equiv 7 + 3 \cdot 31 \bmod 31 \\
&\equiv 100 \bmod 31 \\
x &\equiv \pm 10 \bmod 31
\end{aligned}$$

so $x = 10$ or $x = 21$.

Example. Find $x \in \mathbb{Z}_{15}$ such that $2^{90} = x \bmod 15$.

Answer. By Eular's Theorem, $2^8 \equiv 1 \bmod 15$. So

$$\begin{aligned}
2^{90} &\equiv 2^{88} \cdot 2^2 \bmod 15 \\
&\equiv 1 \cdot 4 \bmod 15 \\
&\equiv 4 \bmod 15
\end{aligned}$$

so $x = 4$.

3.3 The Field of Fractions

Definition (The field of fractions)**.** Let R be a domain. The **field of fractions** is

$$\begin{aligned}
Q &:= \frac{R \times (R \setminus \{0\})}{\sim} \\
&= \frac{\{(a, b) \in R \times R \mid b \neq 0\}}{\sim}
\end{aligned}$$

where

$$(a, b) \sim (c, d) \iff ad = bc$$

we'll write $\frac{a}{b}$ as the equivalence class of $(a, b) \in Q$.

Example. $\mathbb{Z}$ is a domain and its field of fractions is $\mathbb{Q}$.

Example. $\mathbb{C}$ is a domain and its field of fractions is $\mathbb{C}$.

Example. More generally, if $\mathbb{F}$ is a field, then it is its own field of fraction.

Definition (Degree). Let R be a ring with $1 \neq 0$. The degree of $f \in R[x]$ with $f \neq 0$ is $\deg(f) = n$ where

$$f = a_n x^n + \dots + a_1 x + a_0$$

with $a_n \neq 0$

Example.
- $f = x^2 + 1$, $\deg(f) = 2$
- $f = 5x^4 + 2x^3$, $\deg(f) = 4$

Theorem. R is a domain iff $R[x]$ is a domain

proof.
- ($\Longrightarrow$) Assume R is a domain. Let $f, g \in R[x]$ with $f \neq 0$ and $g \neq 0$. WTS: $f \cdot g \neq 0$, or

$$\deg(f \cdot g) = \deg(f) + \deg(g)$$

Remark. Does **not** hold when R is not a domain. E.g., $\mathbb{Z}_4[x]$,

$$\begin{aligned} f &= 2x \qquad & \deg(f) &= 1 \\ g &= 2x^3 + x & \deg(g) &= 3 \\ f \cdot g &= 2x^2 \deg(f \cdot g) = 2 \end{aligned}$$

Write

$$f = a_n x^n + \dots + a_1 x + a_0$$

with $a_n \neq 0$, then $\deg(f) = n$, and

$$g = b_m x^m + \dots + b_1 x + b_0$$

with $b_m \neq 0$, then $\deg(g) = m$. Then

$$f \cdot g = a_n b_m x^{n+m} + \dots + a_1 b_1 x + a_0 b_0$$

since $a_n \neq 0$, $b_n \neq 0$ and R is domain, $a_n b_m \neq 0$, so

$$\deg(f \cdot g) = n + m = \deg(f) + \deg(g)$$

in particular, $R[x]$ is a domain.
- ($\Longleftarrow$) $R \subseteq R[x]$ and $R[x]$ is a domain so it follows that R must also be a domain.

$\square$

Example. $\mathbb{Z}[x]$ is a domain. Its field of fractions is

$$\left\{ \frac{f}{h} \;\middle|\; f, g \in \mathbb{Z}[x], g \neq 0 \right\} = \frac{\{(f, g) \in \mathbb{Z}[x] \times \mathbb{Z}[x] \mid g \neq 0\}}{\sim}$$

that is, the field of fractions of $\mathbb{Z}[x]$ is the set of rational functions with integer coefficients:

$$\frac{1}{1-x^2}, \frac{7x^4+2x^5}{10x^7+2x+1} \in \text{field of fractions}$$

Theorem. If R is a domain with field of fractions Q, then Q is a field where

$$\frac{a}{c}+\frac{c}{d} := \frac{ad+bc}{bd}$$
$$\frac{a}{c}\cdot\frac{b}{d} := \frac{ab}{cd}$$

proof. First check $+$ is well defined. Let $\frac{a}{b}=\frac{a'}{b'}$, WTS:

$$\frac{a}{b}+\frac{c}{d}=\frac{a'}{b'}+\frac{c}{d}$$

that is, WTS:

$$\frac{ad+bc}{bd}=\frac{a'd+b'c}{b'd} \underset{\text{definition}}{\iff} (ad+bc)b'd = bd(a'd+b'c)$$

Since

$$\frac{a}{b}=\frac{a'}{b'} \implies ab'=ba'$$

then

$$\begin{aligned}(ad+bc)b'd &= (ad)(b'd)+(bc)(b'd) \\ &= ab'd^2+bdcb' && \text{since } R \text{ commutative} \\ &= ba'd^2+bdcb' \\ &= (bd)(a'd)+(bd)(b'c) && \text{since } R \text{ commutative} \\ &= (bd)(a'd+b'c) && \text{by distribution}\end{aligned}$$

therefore $+$ is well-defined.

Exercise. Show multiplication is well-defined.

Since R is a commutative ring, $+$ and $\cdot$ are commutative binary operations on Q,

Claim. $\frac{0}{1}$ is the additive identity.

$$\frac{a}{b}+\frac{0}{1}=\frac{a\cdot 1+b\cdot 0}{b\cdot 1}=\frac{a}{b}$$

Claim. $\frac{1}{1}$ is the multiplicative identity.

$$\frac{a}{b}\cdot\frac{1}{1}=\frac{a\cdot 1}{b\cdot 1}=\frac{a}{b}$$

Claim.

$$-\left(\frac{a}{b}\right) = \frac{-a}{b} \in Q$$
$$\frac{a}{b} + \frac{-a}{b} = \frac{ab - ba}{b^2} = \frac{0}{b^2} = \frac{0}{1}$$

Exercise. Show $+$ and $\cdot$ are associative.

Claim. If $\frac{a}{b} \neq 0$, then

$$\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$$

Finally, we show Distributivity holds:

$$\begin{aligned}
\frac{a}{b} \cdot \left(\frac{c}{d} + \frac{e}{f}\right) &= \frac{a}{b} \cdot \left(\frac{cf + de}{df}\right) \\
&= \frac{a(cf) + a(de)}{b(df)} \\
&= \frac{ab(cf) + ab(de)}{b^2(df)} \\
&= \frac{ac(bf) + (bd)ae}{b^2(df)} \\
&= \frac{ac}{bd} + \frac{ae}{bf}
\end{aligned}$$

□

Proposition. If R is a domain with field of fractions Q, then the function

$$\begin{aligned}
\iota : R &\longrightarrow Q \\
a &\longmapsto \frac{a}{1}
\end{aligned}$$

is a injective ring homomorphism.

proof. Let $a, b \in R$

1.

$$\iota(a + b) = \frac{a + b}{1} = \frac{a}{1} + \frac{b}{1} = \iota(a) + \iota(b)$$

2. $\iota(a \cdot b) = \iota(a) \cdot \iota(b)$ Omitted
3. ι is injective: Assume $\iota(a) = \iota(b)$, then definition of ι gives

$$\frac{a}{1} = \frac{b}{1} \iff a \cdot 1 = b \cdot 1 \iff a = b$$

□

Remark. Previous propositions says we can view $R \subseteq Q$. In fact, Q is the smallest field containing R.

Theorem. If R is a domain and Q is its field of fractions with $\iota : R \longrightarrow Q$ from the previous proposition, then for any injective ring homomorphism $\varphi : R \longrightarrow F$ with F a field, there exists a unique injective field homomorphism $\tilde{\varphi} : Q \longrightarrow F$

$$\begin{tikzcd} R \arrow[r, hook, "\varphi"] \arrow[d, hook, "\pi"'] & F \\ Q \arrow[ur, hook, dashed, "\exists!\tilde{\varphi}"] & \end{tikzcd}$$