# Abstract Algebra

MATH 113

Instructor: James Conway

Kelvin Lee

UC Berkeley

# Contents

# Chapter 1

# Sets and Relations

## 1.1 Sets

**Definition 1.1.1** (Subset). A set $A$ is a **subset** of a set $B$ if $x \in A \implies x \in B$. We write $A \subseteq B$ or $A \subset B$.

**Definition 1.1.2** (Proper subset). A **proper subset** is $A \subseteq B$ but $A \neq B$, i.e., $A \subset B$.

**Remark.** $A = B$ is equivalent to saying that $A \subseteq B$ and $B \subseteq A$.

## 1.2 Set Operations

**Definition 1.2.1** (Union). $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$

**Definition 1.2.2** (Intersection). $A \cap B = \{x \mid x \in A \text{ and } x \in B\}$.

**Definition 1.2.3** (Difference). $A \backslash B = A - B = \{a \in A \mid a \notin B\}$.

**Definition 1.2.4** (Cartesian product). $A \times B = \{(a, b) \mid a \in A, b \in B\}$.

**Remark.** $A \times B \neq B \times A$.

**Definition 1.2.5** (Complement). The **complement** of $A \subseteq U$ is $A^c = \{a \in U \mid a \notin A\}$ where $U$ is the universe.

**Remark.** $A \cup A^c = U$; $A \cap A^c = \varnothing$; $(A^c)^c = A$.

**Theorem 1.2.6** (De Morgan's Laws).

$$(A \cup B)^c = A^c \cap B^c,$$

$$(A \cap B)^c = A^c \cup B^c.$$

## 1.3 Relations

**Definition 1.3.1** (Relations). A **relation** between sets $A$ and $B$ is a subset $\mathcal{R} \subseteq A \times B$. If $(a, b) \in \mathcal{R}$, then $a$ is related to $b$, or $a\mathcal{R}b$, or $a \sim b$.

**Example 1.3.2.** $\mathcal{R} \subseteq \mathbb{R} \times \mathbb{R}$. $\mathcal{R} = \{(x, x) \in \mathbb{R}^2 \mid x \in \mathbb{R}\}$, i.e., $a\mathcal{R}b \iff f(a) = b$, where $f : \mathbb{R} \to \mathbb{R}$ and $f(x) = x$.

**Example 1.3.3.** $\mathcal{R} \subseteq \mathbb{R}^2$, $a\mathcal{R}b \iff b = a^3$, i.e., $\mathcal{R} = \{(x, x^3) \mid x \in \mathbb{R}\}$.

### 1.3.1 Functions

**Definition 1.3.4** (Function)**.** A **function** $f : A \to B$ is a relation $\mathcal{R} \subseteq A \times B$ such that $\forall a \in A, \exists! b \in B$ such that $(a, b) \in \mathcal{R}$.

**Definition 1.3.5** (Binary Operation)**.** A **binary operation** on a set $A$ is a function $f : A \times A \to A$.

**Definition 1.3.6** (Disjoint)**.** $A, B \subseteq U$ are **disjoint** if $A \cap B = \varnothing$.

**Definition 1.3.7** (Partition)**.** A **partition** of $U$ is a collection of disjoint subsets of $U$ whose union is $U$.

**Example 1.3.8.** $U = \mathbb{Z}$ can be partitioned into $\{x \in \mathbb{Z} \mid x < 0\}, \{x \in \mathbb{Z} \mid x > 0\}$.

**Example 1.3.9.** $U = \mathbb{R}$ can be partitioned by the sets $\{x\}$ for each $x \in \mathbb{R}$.

**Definition 1.3.10** (Equivalence Relation)**.** A relation $\mathcal{R} \subseteq A \times A$ is an **equivalence relation** if it is

(i) **reflexive**: $a\mathcal{R}a \quad \forall a \in A$.

(ii) **symmetric**: $a\mathcal{R}b \iff b\mathcal{R}a$.

(iii) **transitive**: $a\mathcal{R}b$ and $b\mathcal{R}c \implies a\mathcal{R}c$.

**Remark.** Equivalence relation "are the same" as partition, i.e., they contain the same information. (Why)?

- If $\mathcal{R}$ is an equivalence relation on $A$, then create partition of $A$: say $a$ and $b$ are in the same subset of the partition $\iff a\mathcal{R}b$. This is a partition of $A$.
- Given a partition of $A$, make a relation $\mathcal{R}$ on $A$ by saying $a\mathcal{R}b \iff a$ and $b$ are in the same subset of the partition. Check $\mathcal{R}$ is an equivalence relation.

**Example 1.3.11.** If $\mathbb{Z}$ are partitioned into $\overline{0}, \overline{1}, \ldots, \overline{n-1}$ for some $n \geqslant 2$, the corresponding equivalence relation is *congruence modulo* $n$. For $a\mathcal{R}b$, write $a \equiv b \pmod{n}$.

## 1.4 Modular Arithmetic

**Notation.**

$$\overline{i} = \{x \in \mathbb{Z} \mid i \text{ is the remainder when } x \text{ is divided by } n\} = \{an + i \mid a \in \mathbb{Z}\}.$$

Define $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$. Goal is to define $+$ and $\times$ on $\mathbb{Z}_n$.

To do so, first, given $x \in \mathbb{Z}$, let $\overline{x} = \{an + x \mid a \in \mathbb{Z}\}$. Then $\overline{x} = \overline{y}$ when $x - y = kn$ for some $k \in \mathbb{Z}$, i.e., $x - y \in \overline{0}$. Now for $+/\times$: define $+ : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ that has the mapping $(\overline{a}, \overline{b}) \to \overline{a+b}$ and define $\times : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ that has the mapping $(\overline{a}, \overline{b}) \to \overline{ab}$.

**Question.** Define $\overline{a} + \overline{b} = \overline{a+b}$. But if $\overline{a} = \overline{x}$ and $\overline{b} = \overline{y}$, then is $\overline{a+b} = \overline{x+y}$?

**Question.** Write out tables of binary operations for $n = 3$.

# Chapter 2

# Groups

## 2.1 Properties of $+$ on $\mathbb{R}$ and $\times$ on $\mathbb{R}\backslash\{0\}$

(i) **Closure**: adding/ multiplying two elements gives another element (built in to definition of a binary operation).

(ii) **Commutativity**:

$$\begin{cases} a+b &= b+a \\ ab &= ba \end{cases} \quad \forall a, b.$$

(iii) **Associativity**

$$\begin{cases} a+(b+c) &= (a+b)+c \\ a(bc) &= (ab)c \end{cases} \quad \forall a, b, c.$$

(iv) **Identity**

$$\begin{cases} a+0 &= 0+a=a \\ a\cdot 1 &= 1\cdot a = a \end{cases} \quad \forall a.$$

(v) **Inverses**

$$\begin{cases} a+(-a) &= 0 \\ a\cdot \frac{1}{a} &= 1 \end{cases} \quad \forall a.$$

**Definition 2.1.1.** We say a binary operation $p : A \times A \to A$ is:

- **commutative** if $p(a,b) = p(b,a) \quad \forall a, b \in A$.
- **associative** if $p(a, p(b,c)) = p(p(a,b), c) \quad \forall a, b, c \in A$.
- **has an identity** if $\exists e \in A$ such that $p(a,e) = p(e,a) = a \quad \forall a \in A$.
- **has inverses** if $\exists$ identity $e \in A$ and $\forall a \in A, \exists b \in A$ such that $p(a,b) = p(b,a) = e$. We denote the inverse as $a^{-1}$.

**Example 2.1.2.** $A = \mathbb{Z}_n, p =$ addition mod $n$, i.e., $p(i,j) = \overline{i} + \overline{j}$.

1. **Associativity:**

$$\begin{aligned}\overline{i} + (\overline{j} + \overline{k}) = \overline{i} + \overline{j+k} &= \overline{i + (j+k)} \\ &= \overline{(i+j)+k} \\ &= \overline{i+j} + \overline{k} \\ &= (\overline{i} + \overline{j}) + \overline{k}.\end{aligned}$$

2. **Identity:** $\overline{0}$.

3. **Inverses:** $\overline{i}$ has inverse $\overline{-i} = \overline{n-i}$. (e.g. $n = 2$: inverse of $\overline{1} = \overline{-1} = \overline{2-1} = \overline{1}$.

4. **Commutativity:**

$$\overline{i} + \overline{j} = \overline{i+j} = \overline{j+i} = \overline{j} + \overline{i}.$$

**Example 2.1.3.** $A = \mathrm{Mat}_n(\mathbb{R})$ = set of $n \times n$ matrices with entries in $\mathbb{R}$. $p : A \times A \to A$ is matrix multiplication. **Associativity:** matrix multiplication is associative. **Identity:** $I_n$ the identity matrix. **Inverses:** No, consider the inverse for the zero matrix. **Commutativity:** $AB \neq BA$ for matrices.

**Example 2.1.4.** $A = GL_n(\mathbb{R})$ General linear group (invertible matrices). **Associativity:** yes. **Identity:** yes. **Inverses:** yes. **Commutativity:** no.

**Example 2.1.5.** $A$ = set of functions $f : \mathbb{R} \to \mathbb{R}, p(f,g) = f \circ g$. **Associativity:** yes. **Identity**: $f(x) = x$. **Inverses**:? **Commutativity:** no, e.g.?

### 2.1.1 Properties

- If $p$ is a binary operation on $A$ with identity $e$, and $ab = ac = e$ and $ba = ca = e$. ($ab$ means $p(a,b)$, $ac$ means $p(a,c)$), then $b = c$. This is the **cancellation law**.

  **Remark.** (Why?) $ab = e \implies cab = ce \implies eb = c \implies b = c$. Hence, inverses are *unique*. That is, if $e, f \in A$ are such that

$$\begin{cases} ea = ae & = a \\ fa = af & = a \end{cases} \quad \forall a \in A,$$

  then $e = f$.
  (Why?) $e = ef = f$ ($f, e$ is identity).

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

**Definition 2.1.6** (Groups)**.** A **group** is a set $G$ with a binary operation $p : G \times G \to G$ that is *associative*, *has an identity* $e$, and *has inverses*. Write this as $(G,p)$ or just $G$ if the binary operation is understood from context.

**Definition 2.1.7** (Abelian)**.** A group $(G,p)$ is **Abelian** or **communitative** if $p$ is commutative.

**Notation:** write $p(a,b)$ as $ab$ or $a+b$ sometimes depending on the context.

**Remark.** Some authors have four properties: with the extra one being **closure**. For us, closure is built in to the definition of $p$.

**Example 2.1.8.** Examples of Abelian group:$(\mathbb{R},+)$,$(\mathbb{R}\backslash\{0\},\times)$, $(\mathbb{Z}_n,+)$.
Examples of non-Abelian group: $(GL_n(\mathbb{R}),\times)$.
Examples of non-group: $(\mathrm{Mat}_n(\mathbb{R}),\times)$, $(\{f:\mathbb{R}\to RR\},\text{commposition})$, $(\mathbb{N},+)$.

**Definition 2.1.9** (Order)**.** The **order** of a group is the cardinality of $G$ as a set.

**Notation:** $|G|$ = order of $G$. $|\mathbb{R}|=\infty, |\mathbb{Z}_n|=n$.

**Theorem 2.1.10** (Cancellation Law)**.** In a group $G$, if $ab=ac$, then $b=c$, i.e., we can cancel $a$.

*Proof.* $a$ has inverse $a^{-1}\in G$. Hence,

$$ab=ac \implies a^{-1}ab=a^{-1}ac \implies eb=ec \implies b=c.$$

□

**Example 2.1.11.**

- $GL_n(\mathbb{R}), GL_n(\mathbb{C}), GL_n(\mathbb{Q})$ under matrix multiplication. (*General linear groups*)
- $SL_n(\mathbb{R}), SL_n(\mathbb{C}), SL_n(\mathbb{Q})$ under matrix multiplication. (*Special linear groups*, i.e. $SL_n(\mathbb{R})=\{A\in GL_n(\mathbb{R}) \mid \det A=1\}$.) Matrix multiplication can be reimagined as a binary operation $SL_n(\mathbb{R})\times SL_n(\mathbb{R})\to SL_n(\mathbb{R})$.
- Given a set $[n]=\{1,2,\dots,n\}$, let $S_n$ = set of bijections $[n]\to[n]$. For example, $f:[3]\to[3]$ $(f(1)=1, f(2)=3, f(2)=3)$ is an element of $S_3$. Define binary operation $p$ on $S_3$ by function composition $fg=f\circ g$, e.g. $(fg)(1)=(f\circ g)(1)=f(g(1))$. This forms a group $(S_n,p)$, called the **symmetric group**, e.g. for $f$ above: $f\circ f$ is $(1\to 1, 2\to 2, 3\to 3)$, which is the identity function.

  **Remark.** It is a group. **Associativity:** function composition is associative. **Identity:** $f(i)=i \quad \forall i$. **Inverse:** every bijection has an inverse bijection (if $f(i)=j$, then define $f^{-1}(j)=i$) and so $f\circ f^{-1}=f^{-1}\circ f=e$. Hence, $S_n$ is a group.
  These bijection can be thought of as permutations of the list $\{1,2,\dots,n\}$, e.g. $f$ above permutes 123 to 132. It also permutes 132 to 123. $f$ takes the second slot to third slot and the third slot to second slot. $f$ permutes: $123 \overset{f}{\rightsquigarrow} 132 \overset{f}{\rightsquigarrow} 123$. There are $n!$ different permutations of $123\cdots n$ and so $|S_n|=n!$.

## 2.2 Subgroups

**Definition 2.2.1** (Subgroup)**.** A **subgroup** is a non-empty subset $H$ of a group $(G,p)$ such that

- $H$ is closed under $p$: $p(a,b)\in H \quad \forall a,b\in H$.
- Identity is in $H$.
- $H$ has inverses: if $a\in H$, then $a^{-1}\in H$.

Under these conditions, we can define a new binary operation: $p_H : H\times H\to H$ defined by $p_H(a,b)=p(a,b)$.

**Proposition 2.2.2.** $(H, p_H)$ is a group.

*Proof.* $p_H$ is a well-defined binary operation since $H$ is closed under $p$. We also have the identity $e \in H$ since given any $a \in H$, we know that $a^{-1} \in H$. Hence, we have $p_H(a, a^{-1}) = p(a, a^{-1}) = e \in H$. The inverse is also given. For associativity, we have $p_H$ is associative because $p$ is associative. □

**Notation:** $H \leqslant G$ means $H$ is a subgroup of $G$.

**Example 2.2.3.** $(\mathbb{Z}, +) \leqslant (\mathbb{Q}, +) \leqslant (\mathbb{R}, +) \leqslant (\mathbb{C}, +)$.

**Example 2.2.4.** $(\mathbb{Q}\backslash\{0\}, \times) \leqslant (\mathbb{R}\backslash\{0\}, \times) \leqslant (\mathbb{C}\backslash\{0\}, \times)$.

**Remark.** Examples of non-subgroups: $(\mathbb{R}\backslash\{0\}, \times) \not\leqslant (\mathbb{R}, +)$, $(\mathbb{R}\backslash\{0\}, +) \not\leqslant (\mathbb{R}, +)$

**Example 2.2.5.** $SL_n(\mathbb{R}) \leqslant GL_n(\mathbb{R})$ (under matrix multiplication).

**Example 2.2.6.** For any group $G$, $\{e\} \leqslant G$, called the **trivial subgroup**.

**Definition 2.2.7** (Proper Subgroup)**.** A subgroup $H \leqslant G$ is a **proper subgroup** if $H \neq G$.

### 2.2.1 Subgroups of $(\mathbb{Z}, +)$

Let $a \in \mathbb{Z}$ and define $a\mathbb{Z} = \{ax \mid x \in \mathbb{Z}\}$ (multiples of $a$).

**Proposition 2.2.8.** $(a\mathbb{Z}, +) \leqslant (\mathbb{Z}, +)$ for any $a \in \mathbb{Z}$.

*Proof.* Non-emptiness: $a \in a\mathbb{Z}$, so $a\mathbb{Z} \neq \varnothing$. Closure: given $ax, ay \in a\mathbb{Z}$, we want to check that $ax + ay \in a\mathbb{Z}$. But $ax + ay = a(x + y) \in a\mathbb{Z}$. Inverses: given $ax \in a\mathbb{Z}$, we know that $a(-x) \in a\mathbb{Z}$ and $ax + a(-x) = ax - ax = 0$, so $a(-x)$ is the inverse of $ax$ and thus $a\mathbb{Z}$ has inverse. □

**Theorem 2.2.9.** If $H \leqslant \mathbb{Z}$, then $H = a\mathbb{Z}$ for some $a \in \mathbb{Z}$.

*Proof.* Since $H \leqslant \mathbb{Z}$, $0 \in H$ (identity). If $H = \{0\}$. then $H = 0\mathbb{Z}$ and we are done. If not, let $a$ be the smallest positive integer in $H$ (see explanation in the following remark). To show that $H = a\mathbb{Z}$, we need to show that $H \subseteq a\mathbb{Z}$ and $a\mathbb{Z} \subseteq H$.
$\underline{(a\mathbb{Z} \subseteq H)}$: given any $ax \in a\mathbb{Z}$, we have

$$ax = \begin{cases} \underbrace{a + \cdots + a}_{x} & \text{if } x > 0, \\ \underbrace{(-a) + \cdots + (-a) + \cdots}_{x} & \text{if } x < 0, \\ 0 & \text{if } x = 0. \end{cases}$$

When $x > 0$, $ax \in H$ since $H$ is closed under addition. When $x < 0$, $ax \in H$ as $-a \in H$ since $H$ has inverse and $H$ is closed under addition. When $x = 0$, $ax \in H$ since $H$ has identity. Hence, since for all cases we have $ax \in H$, this shows that $a\mathbb{Z} \subseteq H$.
$\underline{(H \subseteq a\mathbb{Z})}$ : let $b \in H$, write $b = ax + r$ for some $r, x \in \mathbb{Z}$ with $r \in \{0, 1, \ldots, a - 1\}$. Note that $r = b + a(-x) \in H$ since $b \in H, a(-x) \in a\mathbb{Z} \subseteq H$ and $H$ is closed under addition. If $r \neq 0$, then $r$ is a positive integer in $H$ smaller than $a$. But this contradicts our choice of $a$ as the smallest positive

integer in $H$. Hence, $r = 0$, and $b = ax \in a\mathbb{Z}$. Hence, $H \subseteq a\mathbb{Z}$.
Therefore, we conclude that $H = a\mathbb{Z}$. □

**Remark.** For the second case, $H$ contains a positive integer! (Why?) If not, then $H$ only contains 0 and negative numbers, but then $H$ has no inverses.

Given $a\mathbb{Z}, b\mathbb{Z} \neq \{0\}$, we can define $a\mathbb{Z} + b\mathbb{Z} = \{ax + by \mid x, y \in \mathbb{Z}\}$. As an exercise, show that this is a subgroup of $\mathbb{Z}$. Assuming that we have proved the claim, then by the theorem above, $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ for some $d \in \mathbb{Z}$ and we can take $d > 0$.

**Definition 2.2.10** (Greatest Common Divisor)**.** If $a \neq 0, b \neq 0$, then $d$ is the **greatest common divisor** of $a$ and $b$. We write $d = gcd(a, b)$.

**Proposition 2.2.11.** If $a \neq 0, b \neq 0$, $d = gcd(a, b)$, then:

(i) $d|a$ and $d|b$,

(ii) if $e|a$ and $e|b$, then $e|d$,

(iii) $\exists x, y \in Z$ such that $ax + by = d$.

*Proof.* Recall that $d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$.

(i) (1) $a \cdot 1 + b \cdot 0 \in a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$, so $a \in d\mathbb{Z} \implies a$ is a multiple of $d \implies d|a$.
(2) $a \cdot 0 + b \cdot 1 \in d\mathbb{Z}$, so $b \in d\mathbb{Z} \implies b$ is a multiple of $d \implies d|b$.

(ii) if $e|a$ and $e|b$, then $e|ax + by = d$.

(iii) $d \in d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$, so $\exists x, y \in \mathbb{Z}$ such that $d = ax + by \in a\mathbb{Z} + b\mathbb{Z}$.

□

**Remark.** If $ax + by = n$, it is now always the case that $n = gcd(a, b)$. For example, $gcd(2, 4) = 2$, but $2 \cdot 2 + 4 \cdot 1 = 8 \neq gcd(2, 4)$.

**Definition 2.2.12.** $a, b \in \mathbb{Z}$ are **relatively prime** if $gcd(a, b) = 1$.

**Remark.** $gcd(a, b) = 1 \iff \exists x, y \in \mathbb{Z}$ such that $ax + by = 1$.

**Proposition 2.2.13.** If $p \in \mathbb{Z}$ is prime, then $p|ab$ implies $p|a$ or $p|b$.

*Proof.* If $p|ab$, and $p \nmid a$, we want to show $p|b$. Since $p$ has divisors $\pm 1$ and $\pm p$, then $gcd(a, p) = 1$ or $p$. But $p \nmid a$ by assumption, so $gcd(a, p) = 1$. Hence, there exists $x, y \in \mathbb{Z}$ such that $ax + py = 1$. Then multiply both sides by $b$: $abx + pby = b$. Since $p|ab$ and $p|p$, $p|abx + pby = b$ as required. □

### 2.2.2 Cyclic subgroups

**Definition 2.2.14** (Cyclic subgroups)**.** Let $G$ be a group, $a \in G$. Then

$$\langle a \rangle = \{\ldots, a^{-2}, a^{-1}, e, a, a^2, \ldots\} = \{a^n \mid n \in \mathbb{Z}\}.$$

is called the **cyclic subgroup** of $G$ generated by $a$.

**Remark.** $\langle a \rangle$ is the smallest subgroup of $G$ containing $a$, i.e., if $H \leqslant G$ and $a \in H$, then $\langle a \rangle \subseteq H$ by closure and inverses.

**Example 2.2.15.** If $f \in S_1$ is $f = (12)(3)$, then $\langle f \rangle = \{e, f\}$.

**Definition 2.2.16** (Order)**.** If $\langle a \rangle \leqslant G$ is finite, let $n \in \mathbb{N}$ be the smallest positive integer such that $a^n = e$. This $n$ is called the **order** of $a$, written $|a|$. If $|\langle a \rangle| = \infty$, then $|a| = \infty$, and we say that $a$ has **infinite order**.

**Proposition 2.2.17.** Let $|a| = n < \infty$.

(i) $a^\ell = a^m \iff \ell - m \equiv 0 \pmod{n}$. In particular, $a^\ell = e \iff \ell \equiv 0 \pmod{n}$.

(ii) $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$ and $|\langle a \rangle| = n$.

*Proof.*

(i) If $a^\ell = a^m$, then $a^\ell a^{-m} = a^m a^{-m} \implies a^{\ell-m} = e$. Write $\ell - m = nk + r$ for some $r \in \{0, 1, \ldots, n-1\}$. Then $a^r = a^{(\ell-m)-nk} = a^{\ell-m}(a^n)^{-k} = e \cdot e^{-k} = e$. If $r \neq 0$, then $a^r = e$, but $r < n$. This contradicts the definition of $n$ as the order of $a$. Hence, $r = 0$ and $\ell - m = nk \implies \ell - m \equiv 0 \pmod{n}$. Conversely, if $\ell - m \equiv 0 \pmod{n}$, then $\ell - m = nk$ for some $k$, so $a^{\ell-m} = (a^n)^k = e^k = e$.

(ii) Exercise. (See book)

□

**Exercise 2.2.18.** If $|a| = n$, and $\ell \in \{0, \ldots, n-1\}$, then

- $|a^\ell| = 1 \iff \ell = 0$,
- if $d = gcd(n, \ell)$, then $|a^\ell| = \frac{n}{d}$.

**Definition 2.2.19** (Cyclic group)**.** A group $G$ is **cyclic** if $\exists a \in G$ such that $G = \langle a \rangle$. We call $a$ a *generator* of $G$ and say that $G$ is generated by $a$.

**Example 2.2.20.** $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$, called an *infinite cyclic group*. $\mathbb{Z}_n = \langle \overline{1} \rangle$ for any $n$, called a *cyclic group of order n*.

### 2.2.3 Homomorphisms

**Definition 2.2.21** (Homomorphism)**.** Given groups $(G, p)$ and $(G', p')$, a **homomorphism** $\varphi : G \to G'$ is a function such that

$$\varphi(p(a, b)) = p'(\varphi(a), \varphi(b)) \quad \forall a, b \in G.$$

**Remark.** The point of a group homomorphism is to preserve the structure of the group. The idea is that it doesn't matter whether you multiply first then apply the map or apply the map then multiply. This is what we mean when we say it "preserves the structure" of the group.

**Example 2.2.22.** $\varphi : (\mathbb{Z}, +) \to (\mathbb{Z}_n, +)$ and $\varphi(x) = \overline{x}$. To check if this is a homomorphism, we check if $\varphi(x + y) = \varphi(x) + \varphi(y)$, $\forall x, y \in \mathbb{Z}$.

$$\varphi(x + y) = \overline{x + y}$$
$$\varphi(x) + \varphi(y) = \overline{x} + \overline{y}.$$

Since $\overline{x+y} = \overline{x} + \overline{y}$ by definition of $+$ in $\mathbb{Z}_n$, $\varphi$ is a homomorphism.

**Example 2.2.23.** $\varphi_k : \mathbb{Z} \to \mathbb{Z}$, $\varphi_k(x) = kx$.

$$\varphi(x+y) = k(x+y) = kx + ky = \varphi(x) + \varphi(y).$$

Hence, it is a homomorphism.

**Example 2.2.24.** $\exp : (\mathbb{R}, +) \to (\mathbb{R}\backslash\{0\}, \times)$, $\exp(x) = e^x$.

$$\exp(x+y) = e^{x+y} = e^x \cdot e^y = \exp(x) \cdot \exp(y).$$

**Remark.** Non-homomorphism example: $\exp : (\mathbb{Q}, +) \to (\mathbb{Q}\backslash\{0\}, \times)$. This is not well-defined since $e^x$ is generally not rational.

**Example 2.2.25.** $\det : GL_n(\mathbb{R}) \to (\mathbb{R}\backslash\{0\}, \times)$. $\det(AB) = \det(A)\det(B)$.

**Example 2.2.26.** Given any group $G$, and any element $a \in G$, define $\varphi : (\mathbb{Z}, +) \to G$, $\varphi(x) = a^x$. Same as for exp. The image of $\varphi$ is $\langle a \rangle$.

**Example 2.2.27.** Let $G$ and $G'$ be any groups and let $\varphi : G \to G'$ be defined by $a \rightsquigarrow e_{G'}$, $\forall a \in G$. We have $\varphi(ab) = e_{G'}$ and $\varphi(a)\varphi(b) = e_{G'} \cdot e_{G'} = e_{G'}$. This is called the *trivial homomorphism*.

### 2.2.4 Properties of Homomorphism

**Proposition 2.2.28.** If $\varphi : G \to G'$ is a homomorphism, then

(i) $\varphi(a_1, \ldots, a_n) = \varphi(a_1)\varphi(a_2)\cdots\varphi(a_n)$.

(ii) $\varphi(e_G) = e_{G'}$.

(iii) $\varphi(a^{-1}) = \varphi(a)^{-1} \quad \forall a \in G$.

*Proof.*

(i) Induction on definition of homomorphism.

(ii) Since $\varphi(e_G) = \varphi(e_G \cdot e_G) = \varphi(e_G)\varphi(e_G)$, we then multiply both sides by $\varphi(e_G)^{-1}$:

$$\underbrace{\varphi(e_G)^{-1}\varphi(e_G)}_{e_{G'}} = \underbrace{\varphi(e_G)^{-1}\varphi(e_G)}_{e_{G'}}\varphi(e_G) \implies e_{G'} = e_{G'}\varphi(e_G) = \varphi(e_G).$$

(iii) Given $a \in G$. By (ii), we have

$$\varphi(a \cdot a^{-1}) = \varphi(e_G) = e_{G'}.$$

Since $\varphi$ is a homomorphism,

$$\varphi(a \cdot a^{-1}) = \varphi(a)\varphi(a^{-1}) = e_{G'},$$

which implies that $\varphi(a^{-1}) = \varphi(a)^{-1}$.

□

**Remark.**

(1) The image of $\varphi$ is $\varphi(G) = \{\varphi(a) \mid a \in G\} \subseteq G'$. $\varphi(G)$ is a subgroup of $G'$.

(2) The kernel of $\varphi$ is $\ker(\varphi) = \{a \in G \mid \varphi(a) = e_{G'}\} \subseteq G$. $\ker(\varphi)$ is a subgroup of $G$.

*Proof.*

(1) *Closure*: if $\varphi(a), \varphi(b) \in \varphi(G)$, then $\varphi(a)\varphi(b) = \varphi(ab) \in \varphi(G)$. *Inverses*: if $\varphi(a) \in \varphi(G)$, then $\varphi(a)^{-1} = \varphi(a^{-1}) \in \varphi(G)$.

(2) *Closure*: if $a, b \in \ker(\varphi)$, then

$$\varphi(ab) = \varphi(a)\varphi(b) = e_{G'}e_{G'} = e_{G'} \implies ab \in \ker(\varphi).$$

*Inverses*: if $a \in \ker(\varphi)$, then

$$\varphi(a^{-1}) = \varphi(a)^{-1} = e_{G'}^{-1} = e_{G'} \implies a^{-1} \in \ker(\varphi).$$

□

**Example 2.2.29.** $\det : GL_n(\mathbb{R}) \to (\mathbb{R}\backslash\{0\}, \times)$. The identity of $(\mathbb{R}\backslash\{0\}, \times)$ is 1, so

$$\ker(\det) = \{A \in GL_n(\mathbb{R}) \mid \det A = 1\} = SL_n(\mathbb{R}).$$

**Proposition 2.2.30.** If $\varphi : G \to G'$ is a homomorphism, then $\varphi$ is injective if and only if $\ker(\varphi) = \{e_G\}$.

*Proof.* If $\varphi$ is injective, and $a \in \ker(\varphi)$, then $\varphi(a) = e_{G'}$. But also $\varphi(e_G) = e_{G'}$. $\varphi$ being injective implies that $a = e_G$. Hence, $\ker(\varphi) = \{e_G\}$.
Conversely, if $\ker(\varphi) = \{e_G\}$, and $\varphi(a) = \varphi(b)$ for some $a, b \in G$. Multiplying both sides by $\varphi(b)^{-1}$ gives

$$\varphi(a)\varphi(b)^{-1} = \varphi(b)\varphi(b)^{-1} = e_{G'},$$

which implies that $\varphi(a)\varphi(b^{-1}) = e_{G'} \implies \varphi(ab^{-1}) = e_{G'} \implies ab^{-1} \in \ker(\varphi)$. Since $\ker(\varphi) = \{e_{G'}\}$, we know $ab^{-1} = e_G \implies a = b$. Hence, $\varphi$ is injective. □

### 2.2.5 Isomorphisms

**Definition 2.2.31** (Isomorphism)**.** An **isomorphism** $\varphi : G \to G'$ is a bijective homomorphism.

**Example 2.2.32.** $\exp : (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \times)$ is an isomorphism.

**Remark.** If $\varphi : G \to G'$ is an injective homomorphism, then $\varphi : G \to \varphi(G) \leqslant G'$ is an isomorphism.

**Example 2.2.33.** Let $\varphi : (\mathbb{Z}, +) \to \langle a \rangle \leqslant G$ be defined by $x \rightsquigarrow a^x$ for some $a \in G$. $\varphi$ is surjective. $\varphi$ is injective if and only if $a$ has infinite order. If $|a| = n$, then $\varphi : (\mathbb{Z}_n, +) \to \langle a \rangle \leqslant G$ defined by $\overline{x} \rightsquigarrow a^x$ is an isomorphism.

**Example 2.2.34.** Given $A \in GL_n(\mathbb{R})$, the map $f_A : (\mathbb{R}^n, +) \to (\mathbb{R}^n, +)$ defined by $\vec{v} \rightsquigarrow A\vec{v}$ is an isomorphism. *Homomorphism*: $f_A(\vec{v} + \vec{w}) = A(\vec{v} + \vec{w}) = A\vec{v} + A\vec{w} = f_A(\vec{v}) + f_A(\vec{w})$. *Bijection*: Since $A$ is invertible, $\exists$ inverse matrix $A^{-1} \in GL_n(\mathbb{R})$. Then $f_{A^{-1}}$ is the inverse function to $f_A$, i.e., $f_A \circ f_{A^{-1}} = f_{A^{-1}} \circ f_A = id_{\mathbb{R}^n}$. Any invertible function is a bijection.

**Example 2.2.35.** If $a \in G$, then the map $\varphi_a : G \to G$ defined by $b \rightsquigarrow aba^{-1}$ is an isomorphism. This is called *conjugation by* $a$, and $aba^{-1}$ is the conjugate of $b$ by $a$.

**Exercise 2.2.36.** Check $\varphi_a(bc) = \varphi_a(b)\varphi_a(c)$ and check $\varphi_a$ is a bijection. (Hint: find an inverse function)

**Proposition 2.2.37.** If $\varphi : G \to G'$ is an isomorphism, then $\varphi^{-1} : G' \to G$ is also an isomorphism.

*Proof.* $\varphi^{-1}$ exists and is a bijection, as $\varphi$ is a bijection. Now we show that it is a homomorphism by choosing $x, y \in G'$ and show that $\varphi^{-1}(xy) = \varphi^{-1}(x)\varphi^{-1}(y)$. For simplicity, let $\varphi^{-1}(x) = a, \varphi^{-1}(y) = b, \varphi^{-1}(xy) = c$ and we want to show that $c = ab$. Now

$$\begin{aligned} c = ab &\iff \varphi(c) = \varphi(ab) && (\varphi \text{ is a bijection}) \\ &\iff \varphi(c) = \varphi(a)\varphi(b) && (\varphi \text{ is a homomorphism}) \\ &\iff \varphi(\varphi^{-1}(xy)) = \varphi(\varphi^{-1}(x))\varphi(\varphi^{-1}(y)) \\ &\iff xy = xy. \end{aligned}$$

Thus, $c = ab$, which implies that $\varphi^{-1}$ is a homomorphism. Since it's also bijective, it's an isomorphism. □

**Corollary 2.2.38.** The relation $G \sim G' \iff \exists$ isomorphism $G \to G'$ is an equivalence relation.

*Proof. Reflexive:* $G \sim G$, as $\mathrm{id}_G : G \to G$ is an isomorphism. *Symmetric*: if $G \sim G'$ and $\varphi : G \to G'$ is an isomorphism, then $\varphi^{-1} : G' \to G$ is an isomorphism, so $G' \sim G$. *Transitive*: if $G \sim G'$, $G' \sim G''$ and $\varphi : G \to G'$, $\varphi' : G' \to G''$ are isomorphisms, then $\varphi' \circ \varphi : G \to G''$ is an isomorphism, so $G \sim G''$. □

**Definition 2.2.39.** We say $G$ and $G'$ are **isomorphic** if $\exists$ an isomorphism $\varphi : G \to G'$

**Notation:** $G \cong G'$.

**Remark.** There is no such notion of "homomorphic".

## 2.3 Integers mod $n$

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}.$$

The $+$ operation is addition mod $n$, i.e.

$$i + j \equiv k \pmod{n} \implies \overline{i} + \overline{j} = \overline{k}.$$

$(\mathbb{Z}_n, +)$ is an Abelian group.

**Remark.** Recall that the order $|\overline{a}|$ of an element $\overline{a} \in \mathbb{Z}_n$ is the smallest integer $m$ such that

$$\underbrace{\overline{a} + \overline{a} + \cdots + \overline{a}}_{m \text{ times}} = \underbrace{\overline{0}}_{\text{identity}},$$

i.e., the smallest positive integer $m$ such that $am \equiv 0 \pmod{n}$, i.e., the smallest positive $m$ such that $am$ is a multiple of $n$. Then this implies that $am = \mathrm{lcm}(a, n)$, or $m = \frac{\mathrm{lcm}(a,n)}{a} = \frac{\frac{an}{\gcd(a,n)}}{a} = \frac{n}{\gcd(a,n)}$. Hence, $|\overline{a}| = \frac{n}{\gcd(a,n)}$. In particular, $|\overline{a}|$ *is a factor of* $n$ (since $|\overline{a}| \cdot \gcd(a, n) = n$).

**Remark.** If $a$ is such that $\gcd(a,n) = 1$, then $|\overline{a}| = \frac{n}{\gcd(a,n)} = n$, which is the order of $\mathbb{Z}_n$. This implies that $\langle \overline{a} \rangle$ is a subgroup of order $n$, and thus $\langle \overline{a} \rangle = \mathbb{Z}_n$. Hence, $\langle \overline{a} \rangle = \mathbb{Z}_n \iff \gcd(a,n) = 1$.

**Remark.** If $p$ is prime, then $\gcd(a,p) = 1$. $a \neq 0$, $a \in \{1, \dots, p-1\}$ implies that every non-zero element of $\mathbb{Z}_p$ is a generator.

### 2.3.1 Multiplication mod $n$

$\overline{1}$ is the multiplicative identity. $\overline{a} \in \mathbb{Z}_n$ is invertible if there is a $\overline{b} \in \mathbb{Z}_n$ such that

$$\overline{a} \cdot \overline{b} = \overline{1}, \quad \text{i.e., } ab \equiv 1 \pmod{n}.$$

$$\begin{aligned} \exists b \in \mathbb{Z} \text{ s.t. } ab \equiv 1 \pmod{n} &\iff \exists b, k \in \mathbb{Z} \text{ s.t. } ab = 1 + nk \\ &\iff \exists b, k \in \mathbb{Z} \text{ s.t. } a \cdot b + n(-k) = 1 \\ &\iff \gcd(a,n) = 1. \end{aligned}$$

Hence, $\overline{a} \in \mathbb{Z}_n$ has a multiplicative inverse $\iff \gcd(a,n) = 1$.

**Corollary 2.3.1.** $(\mathbb{Z}_n \backslash \{0\}, \times)$ is a group $\iff$ $n$ is prime.

Let $\mathbb{Z}_n^\times = \{\overline{a} \in \mathbb{Z}_n \mid \gcd(a,n) = 1\}$. This is a group under multiplication mod $n$.

$$|\mathbb{Z}_n^\times| = |\{a \in \{1, \dots, n-1\} \mid \gcd(a,n) = 1\}| = \varphi(n),$$

where $\varphi$ is the Euler's totient function.

**Fact.** For prime $p$, $(\mathbb{Z}_p^\times = \mathbb{Z}_p \backslash \{0\}, \times)$ is cyclic, so $(\mathbb{Z}_p^\times, \times) \cong (\mathbb{Z}_{p-1}, +)$.

## 2.4 Roots of Unity

**Definition 2.4.1** (Roots of Unity)**.** The **roots of unity** is the set

$$\mathcal{U}(n) = \{z \in \mathbb{C} \mid z^n = 1\} = \{e^{i\frac{2\pi}{n}k} \mid k = 0, 1, \dots, n-1\},$$

which is a group under complex multiplication.

**Remark.** $\mathcal{U}(n) \cong (\mathbb{Z}_n, +)$ by isomorphism: $f : \underbrace{\mathcal{U}_n \to \mathbb{Z}_n}_{e^{i\frac{2\pi}{n}k} \mapsto \overline{k}}$.

## 2.5 Symmetric Groups

Recall: $S_n$ is the group of bijections $\{1, \dots, n\} \to \{1, \dots, n\}$ under composition and that $|S_n| = n!$.

**Proposition 2.5.1.** The order of an element in $S_n$ is the lcm of the cycle length it contains.

**Example 2.5.2.** $|(12)(34)| = \operatorname{lcm}(2,2) = 2$.

**Example 2.5.3.** $|(1234)(56)(78)| = \operatorname{lcm}(4,2,2) = 4$.

**Remark.** $(12)(34)$ can have two interpretations: $(12)(34) = \underbrace{\sigma_1}_{(12)(3)(4)} \cdot \underbrace{\sigma_2}_{(1)(2)(34)}$, or $(12)(34) = \sigma$.

**Remark.** $(123) = (12)(23)$.

**Definition 2.5.4** (Transposition)**.** A **transposition** is an element $\tau \in S_n$ such that $\tau = (ab)$ for some $a, b \in \{1, \dots, n\}$.

**Remark.** Any element of $S_n$ can be written as a product of transpositions.

**Example 2.5.5.** $(1234)(56) = (12)(23)(34)(56)$.

**Definition 2.5.6** (Even/Odd)**.** $\sigma \in S_n$ is **even/odd** if it can be written as a product of an even/odd number of transpositions.

**Theorem 2.5.7.** No $\sigma \in S_n$ is both odd and even.

*Proof.* The identity $e \in S_n$ has $n$ disjoint cycles. We claim that if $\sigma \in S_n$ has $m$ cycles, then $n - m$ is even/odd if and only $\sigma$ is even/odd. Since $n - m$ cannot be both odd and even, $\sigma$ cannot be both odd and even. □

### 2.5.1 Alternating Groups

$$S_n = \{\text{even } \sigma\} \cup \{\text{odd } \sigma\}$$
$$\{\text{even } \sigma\} \cap \{\text{odd } \sigma\} = \varnothing.$$

There is a homomorphism $\text{sgn} : S_n \to (\{\pm 1\}, \times)$, i.e.,

$$\sigma \mapsto \begin{cases} 1 & \text{if } \sigma \text{ is even,} \\ -1 & \text{if } \sigma \text{ is odd.} \end{cases}$$

Also note that

$$\begin{aligned} \ker(\text{sgn}) &= \{\sigma \in S_n \mid \text{sgn}(\sigma) = 1\} \\ &= \{\sigma \in S_n \mid \sigma \text{ is even}\}. \end{aligned}$$

**Remark.** $\ker(\text{sgn})$ is a subgroup of $S_n$, called the *alternating group* $A_n$ with order $|A_n| = \frac{n!}{2}$.

## 2.6 Symmetry Groups

### 2.6.1 Dihedral Group

**Definition 2.6.1** (Dihedral Group)**.** A **Dihedral group** is the group of symmetries of a regular polygon, which includes rotations and reflections.

**Remark.** Sometimes it is called $D_n$, sometimes $D_{2n}$.

**Fact.** $|D_{2n}| = 2n$ since a symmetry is determined by where a vertex gets sent ($n$ choices) and if it's clockwise or counter-clockwise (2 choices).

For $D_{2n}$, we have elements:

- $x$ = rotation by $\frac{2\pi}{n} = \frac{360^\circ}{n}$ counter-clockwise, and $x^n = e$.
- $y$ = reflection in vertical axis, and $y^2 = e$.
- $yx = x^{n-1}y$.

Then

$$D_{2n} = \{e, x, x^2, \ldots, x^{n-1}, y, xy, \ldots, x^{n-1}y\}.$$

**Remark.** A symmetry in $D_{2n}$ corresponds to a permutation of the vertices. Hence, we can think of $D_{2n}$ as a subgroup of $S_n$, i.e., $D_{2n} \leqslant S_n$ for $n \geqslant 3$. In fact, $D_6 \cong S_3$.

## 2.7 Cosets

**Definition 2.7.1** (Coset)**.** If $H \leqslant G$, and $a \in G$, then the set

$$aH = \{ah \mid h \in H\}$$

is the **left coset** of $H$ associated to $a$. Similarly,

$$Ha = \{ha \mid h \in H\}$$

is the **right coset** of $H$ associated to $a$.

**Remark.** These are *sets*, not subgroups.

**Remark.** If $aH = H$, then $ae \in aH = H$, i.e., $a \in H$. Conversely, if $a \in H$, and $h \in H$, then $a \cdot (a^{-1}h) \in aH \implies h \in aH \implies H \subseteq aH$. Also since $a \in H$, $ah \in H \ \forall h \in H$, so $aH \subseteq H$. Hence, $H = aH$.

**Conclusion.** $aH = H \iff a \in H$. Similarly, $Ha = H \iff a \in H$.

**Proposition 2.7.2.** If $\varphi : G \to G'$ is a group homomorphism, and $K : \ker \varphi \leqslant G$, and $a, b \in G$. Then

$$\varphi(a) = \varphi(b) \iff a^{-1}b \in K \text{ and } b^{-1}a \in K \iff b \in aK \text{ and } a \in bK \iff aK = bK.$$

*Proof.*

$$\begin{aligned}
\varphi(a) = \varphi(b) &\iff e_{G'} = (\varphi(a))^{-1}\varphi(b) \\
&\iff e_{G'} = \varphi(a^{-1})\varphi(b) \\
&\iff e_{G'} = \varphi(a^{-1}b) \\
&\iff a^{-1}b \in K \\
&\iff \exists k \in K \text{ s.t. } a^{-1}b = k \\
&\iff \exists k \in K \text{ s.t. } b = ak. \\
&\iff b \in aK.
\end{aligned}$$

Finally, assuming we have $a \in bK, b \in aK$, $\exists k_1, k_2 \in K$ such that $a = bk_1$ and $b = ak_2$. Given $ak \in aK$, $ak = (bk_1)k = b(k_1k) \in bK \implies aK \subseteq bK$. Similarly, given $bk \in bK, bk = (ak_2)k = a(k_2k) \in aK \implies bK \subseteq aK$. Hence, $aK = bK$.
Conversely, note that $a = ae \in aK$ and $b = be \in bK$. So if $aK = bK$, then $a \in aK = bK$, and $b \in bK = aK$. □

**Corollary 2.7.3.** $\varphi^{-1}(\varphi(a)) = \{b \in G \mid \varphi(b) = \varphi(a)\}$ is equal to $aK$ (or equivalently $Ka$) (since $\varphi(a) = \varphi(b) \iff b \in aK$).

### 2.7.1 Properties of Cosets

Let $G$ be a group, $H \leqslant G$ be a subgroup of $G$. Define relation $\sim$ on $G$ by

$$a \sim b \iff a \in bH.$$

- **Reflexive**: $a \sim a \iff a \in aH$.
- **Symmetric**: if $a \sim b$, then $a \in bH \iff b \in aH$ by proposition. Hence, $b \sim a$.
- **Transitive:** if $a \sim b$, $b \sim c$, then $a \in bH$ and $b \in cH \iff aH = bH$ and $bH = cH$, which implies $aH = bH = cH \iff a \in cH$, i.e., $a \sim c$.

**Conclusion.** Being in each other's coset is an equivalence relation.

**Recall:** {equivalence relations} $\longleftrightarrow$ {partitions}. Here partition subsets are just the cosets.

**Conclusion.** Cosets of $H$ partition $G$.

**Definition 2.7.4** (Index)**.** The number of cosets of $H$ in $G$ is the **index** of $H$ in $G$, denoted by $[G : H]$.

**Lemma 2.7.5.** $|aH| = |H| \, \forall a \in G$.

*Proof.* Set up a bijection by letting $f : H \to aH$ defined by $h \mapsto ah$. *Injective:* if $f(h) = f(h')$, then $ah = ah' \implies h = h'$. *Surjective:* given any $ah \in aH$, then $f(h) = ah$, so $f$ is surjective. Hence, $f$ is a bijection. □

**Example 2.7.6.** $G = S_3, H = \{e, (12)\} = \langle (12) \rangle$. $G = \{e, (12), (13), (23), (123), (132)\}$.

$$eH = \{e, (12)\} = (12)H.$$
$$(13)H = \{(13)e, (31)(12) = (312) = (123)\} = (123)H.$$
$$(23)H = \{(23)e, (23)(12) = (321) = (132)\} = (132)H.$$

**Theorem 2.7.7** (Lagrange's Theorem)**.** If $H \leqslant G$, and $|G|$ is finite, then $|H|$ divides $|G|$.

*Proof.* The cosets of $H$ partition $G$, so

$$|G| = \sum_{\text{cosets of } H \text{ in } G} |\text{coset}|.$$

By the lemma, all cosets have order $|H|$. The number of cosets $= [G : H]$, the index of $H$ in $G$. Hence,

$$|G| = \sum_{i=1}^{[G:H]} |H| = |H| \cdot [G : H].$$

Thus, $|H|$ divides $|G|$. □

**Remark.** $[G : H] = \frac{|G|}{|H|}$.

**Corollary 2.7.8.** If $a \in G$, then $|a|$ divides $|G|$.

*Proof.* $|a| = |\langle a \rangle|$. Since $\langle a \rangle \leqslant G$, by Lagrange, $|\langle a \rangle| = |a|$ divides $|G|$. □

**Corollary 2.7.9.** If $|G| = p$, where $p$ is prime, then $G \cong \mathbb{Z}_p$.

*Proof.* If $a \in G$, then $|a| = 1$ or $|a| = p$ (since $|a|$ divides $|G| = p$). But $|a| = 1 \iff a = a^1 = e$. If $a \neq e$, then $|a| = p \implies |\langle a \rangle| = p = |G| \implies \langle a \rangle = G$, i.e., $G$ is cyclic, generated by $a$. Recall that any cyclic group of order $n$ is isomorphic to $\mathbb{Z}_n$. Hence, $G \cong \mathbb{Z}_p$. □

**Recall:** if $\varphi : G \to G'$ is a homomorphism, $K = \ker \varphi$, then $aK = Ka \ \forall a \in G$.
(Why?) The proposition was that $\varphi^{-1}(\varphi(a)) = aK \ \forall a \in G$. But similarly, with right cosets, $\varphi^{-1}(\varphi(a)) = Ka \ \forall a \in G$, which implies $aK = \varphi^{-1}(\varphi(a)) = Ka \ \forall a \in G$.

## 2.8 Normal Subgroups

**Definition 2.8.1** (Normal subgroup)**.** A subgroup $H \leqslant G$ is called a **normal subgroup** if $aH = Ha \ \forall a \in G$, denoted by $H \trianglelefteq G$. Equivalently, $H$ is a normal subgroup if $aha^{-1} \in H$ for every $h \in H$ and $a \in G$.

**Question.** Why are these equivalent?

**Answer.** If $aH = Ha$, then $ah \in aH = Ha$, so $\exists h' \in H$ such that $ah = h'a \implies aha^{-1} = h' \in H$. Conversely, assume that $aha^{-1} \in H$ for every $a \in G, h \in H$. Choose $a \in G$ and we show that $aH = Ha$. Consider $ah \in aH$. We have $aha^{-1} \in H$, which implies there is $h' \in H$ such that $aha^{-1} = h'$. Thus, $ah = h'a \in Ha \implies aH \subseteq Ha$. Similarly, by considering $a^{-1} \in G$, we have shown that $a^{-1}H \subseteq Ha^{-1}$. Multiply everything in these cosets by $a$ on left and right: so $a(a^{-1}H)a \subseteq a(Ha^{-1})a \implies Ha \subseteq aH$. Hence, $aH = Ha$.

**Example 2.8.2.** The kernel of any homomorphism is normal.

**Example 2.8.3.** $\{\overline{0}, \overline{4}\} \leqslant \mathbb{Z}_8$ is normal.

**Example 2.8.4.** $\{e, (12)\} \leqslant S_3$ is not normal.

**Example 2.8.5.** If $G$ is abelian, then all subgroups are normal, since given $H \leqslant G, a \in G$, then

$$aH = \{ah \mid h \in H\} = \{ha \mid h \in H\} = Ha,$$

so $H \trianglelefteq G$ is a normal subgroup.

**Example 2.8.6.** For any $G$, $\{e\} \trianglelefteq G$ and $G \trianglelefteq G$ since $a\{e\} = \{a\} = \{e\}a$ and $aG = G = Ga$.

**Question.** Why do we care about normal subgroups?

**Answer.** Normal subgroups are perfect for doing algebra with cosets.

If $H \trianglelefteq G$, then

$$\begin{aligned}(aH)(bH) &= \{xy \mid x \in aH, y \in bH\} \\ &= \{a \underbrace{h \cdot b}_{hb=bh"} h' \mid h, h' \in H\} \\ &= \{ab \underbrace{h"h'}_{\text{element in } H} \mid h', h" \in H\} \\ &= abH,\end{aligned}$$

so $(aH)(bH) = abH$ as sets.

## 2.9 Quotient Groups

**Notation.** $\overline{a} = aH$ and $G/H = \{\overline{a} \mid a \in G\}$. Define binary operation on $G/H : \overline{a} \cdot \overline{b} = \overline{ab}$.

**Definition 2.9.1** (Quotient group)**.** If $H \trianglelefteq G$, then $(G/H, \cdot)$ is a group, called the **quotient group** of $G$ by $H$.

**Theorem 2.9.2.** The map $\pi : G \to G/H$ defined by $a \mapsto \overline{a}$ is a group homomorphism with $\ker \pi = H$.

*Proof.* $\pi$ is a homomorphism: $\pi(ab) = \overline{ab} = \overline{a} \cdot \overline{b} = \pi(a) \cdot \pi(b)$. To show $\ker \pi = H$, we have

$$\begin{aligned}\pi(a) = \overline{e} &\iff \overline{a} = \overline{e} \\ &\iff aH = eH = H \\ &\iff a \in H.\end{aligned}$$

Thus, $\ker \pi = H$. □

**Example 2.9.3.** $H = \{\overline{0}, \overline{4}\} \trianglelefteq \mathbb{Z}_8 = G$. $G/H = \{\overline{0} + H, \overline{1} + H, \overline{2} + H, \overline{3} + H\}$.

**Theorem 2.9.4.** Let $H \trianglelefteq G$ be a normal subgroup and $G/H = \{aH \mid a \in G\} = \{\overline{a} \mid a \in G\}$ be the set of left cosets of $H$ and binary operation $G/H \times G/H \to G/H$ defined by $(\overline{a}, \overline{b}) \mapsto \overline{ab}$. Then this is a group, and the map $\pi : G \to G/H$ defined by $a \mapsto \overline{a}$ is a surjective homomorphism with $\ker \pi = H$.

**Remark.** "Identify the quotient group" means "find a familiar group to which the quotient group is isomorphic".

**Example 2.9.5.** Q: "Identify $S_n/A_n$". A: $S_n/A_n \cong \mathbb{Z}_2$.

**Theorem 2.9.6** (First Isomorphism Theorem)**.** If $\varphi : G \to G'$ is a group homomorphism, and $K = \ker \varphi$, then

$$G/K \cong \operatorname{im}(\varphi) = \varphi(G).$$

*Proof.* Assume that $\varphi : G \to G'$ is surjective (if not, replace codomain by image of $\varphi$). Let $K = \ker \varphi$. We want to show that $G/K \cong G'$. Let $\pi : G \to G/K$ be the projection map defined

by $\pi(a) = \overline{a}$. Consider $G \xrightarrow{\pi} G/K \xrightarrow{\overline{\varphi}} G'$ where $\overline{\varphi} : G/K \to G'$ defined by $\overline{\varphi}(\overline{a}) = \varphi(a)$. Then $\varphi = \overline{\varphi} \circ \pi$.
We have to first check that $\overline{\varphi}$ is well-defined, i.e., if $\overline{a} = \overline{b}$ (i.e., $aK = bK$), check that $\overline{\varphi}(\overline{a}) = \overline{\varphi}(\overline{b})$ (i.e.,$\varphi(a) = \varphi(b)$). By the proposition on cosets, we have $\varphi(a) = \varphi(b) \iff aK = bK$ (i.e., $\overline{a} = \overline{b}$). Now check that $\overline{\varphi}$ is an isomorphism. *Homomorphism:* since $\varphi$ is a homomorphism, $\overline{\varphi}(\overline{a} \cdot \overline{b}) = \overline{\varphi}(\overline{ab}) = \varphi(ab) = \varphi(a)\varphi(b) = \overline{\varphi}(\overline{a})\overline{\varphi}(\overline{b})$. *Injective:* we show that $\ker \overline{\varphi} = \{\overline{e}\}$. If $\overline{\varphi}(\overline{a}) = e_{G'}$, then $\varphi(a) = e_{G'}$, which implies that $a \in \ker \varphi = K$ and $a \in K \iff aK = K \iff \overline{a} = \overline{e}$. Thus, $\ker \overline{\varphi} = \{\overline{e}\}$. *Surjective:* if $b \in G'$, then $\exists a \in G$ such that $\varphi(a) = b$ since $\varphi$ is surjective. Then $\overline{\varphi}(\overline{a}) = \varphi(a) = b$. Hence, $\overline{\varphi} : G/K \to G'$ is an isomorphism. □

## 2.10 Group Actions

**Definition 2.10.1.** If $S$ is a set and $G$ is a group, we say $G$ **acts** on $S$ (denoted by $G \curvearrowright S$) if there exists a function $G \times S \to S$ defined by $(g, s) \mapsto g * s$ with the following properties:

- $e * s = s \quad \forall s \in S$
- $(ab) * s = a * (b * s) \quad \forall a, b \in G, \forall s \in S.$

**Remark.** If $G \curvearrowright S$, then given any $g \in G$, we have a function $f_g : S \to S$, where $f_g(s) = g * s \in S$ such that $f_e = \mathrm{id}_S$ (identity function on $S$) and $f_{ab} = f_a \circ f_b \quad \forall a, b \in G$.

**Example 2.10.2.** $G = S_n, S = \{1, \ldots, n\}$ and $\sigma * i = \sigma(i)$.

**Remark.** There may be many different actions of a fixed $G$ on a fixed $S$.

### 2.10.1 Orbits

**Definition 2.10.3** (Orbit)**.** Given a group action $G \curvearrowright S$, and given $s \in S$, the **orbit** of $s$ is $O_s = \{g * s \mid g \in G\}$. That is, $O_s$ is the subset of $S$ consisting of images of $s$ under the action of all elements of $G$, i.e., the image of the function $G \to S$ defined by $g \mapsto g * s$.

**Claim.** If $s' \in O_s$, then $O_{s'} = O_s$.

*Proof.* If $s' \in O_s$, then $\exists g \in G$ such that $g * s = s'$. Now act on both sides by $g^{-1}$:

$$\underbrace{g^{-1} * (g * s)}_{(g^{-1}g)*s=s} = g^{-1} * s' \implies s = g^{-1} * s'.$$

Thus $s \in O_{s'}$.
Given $b * s \in O_s$, then

$$b * s = b * (g^{-1} * s') = (bg^{-1}) * s' \in O_{s'}.$$

Hence, $O_{s'} \subseteq O_s$, which implies $O_s = O_{s'}$. □

**Corollary 2.10.4.** If $O_s \cap O_{s'} \neq \varnothing$, then $O_s = O_{s'}$

*Proof.* If $s'' \in O_s \cap O_{s'}$, then $s'' \in O_s$ and $s'' \in O_{s'}$. By the claim, we have $O_{s''} = O_s$ and $O_{s''} = O_{s'}$, which implies $O_s = O_{s'}$. □

**Fact.** Orbits are either disjoint or equal. Hence, orbits partition $S$. If $S$ is a finite set, then

$$|S| = \sum_{\text{orbits } O} |O|.$$

**Example 2.10.5.** If $G \curvearrowright S$ is the trivial action, then $O_s = \{g * s \mid g \in G\} = \{s\}$.

**Example 2.10.6.** If $G = S_n$, $S = \{1, \dots, n\}$, then $O_1 = S$, since if $(1i) \in S_n$, for $i \in \{2, \dots, n\}$, then $(1i) * 1 = (1i)(1) = i$.

**Definition 2.10.7** (Transitive)**.** A group action $G \curvearrowright S$ is **transitive** if $\exists$ only one orbit, i.e., $O_s = S \quad \forall s \in S$. Equivalently, for any $s, s' \in S, \exists g \in G$ such that $g * s = s'$.

**Definition 2.10.8** (Stabilizer)**.** If $G \curvearrowright S$ is a group action, and $s \in S$, then the **stabilizer** of $s$ $G_s = \{g \in G \mid g * s = s\}$

**Claim.** $G_s \leqslant G$ is a subgroup of $G$.

*Proof.* $G_s \neq \varnothing$ as $e \in G_s$. If $g, h \in G_s$, then $(gh) * s = g * (h * s) = g * s = s \implies gh \in G_s$ and $G_s$ is closed. If $g \in G_s$, then $g * s = s$. Act on both sides by $g^{-1}$:

$$\begin{aligned} g^{-1} * (g * s) &= g^{-1} * s \\ (g^{-1}g) * s &= g^{-1} * s \\ e * s &= g^{-1} * s \\ s &= g^{-1} * s. \end{aligned}$$

Hence, $g^{-1} \in G_s$ and $G_s$ has inverses. □

**Example 2.10.9.** $S_n \curvearrowright \{1, \dots, n\}$, then if $n \in \{1, \dots, n\}$, $G_n = \{\sigma \in S_n \mid \sigma(n) = n\} \cong S_{n-1}$ since if $n$ is fixed, we can still freely permute $\{1, \dots, n-1\} \subseteq \{1, \dots, n\}$.

**Fact.** $G_i \cong S_{n-1} \quad \forall i \in \{1, \dots, n\}$.

**Proposition 2.10.10.** If $G \curvearrowright S$ and $s \in S$:

(i) if $a, b \in G$, then $a * s = b * s \iff a^{-1}b \in G_s$;

(ii) if $a * s = s'$, then $G_{s'} = aG_sa^{-1} = \{aga^{-1} \mid g \in G_s\}$.

*Proof.*

(i) $a * s = b * s \iff s = a^{-1} * (b * s) = (a^{-1}b) * s \iff a^{-1}b \in G_s$.

(ii) Want to show $aG_sa^{-1} = G_{s'}$. If $aga^{-1} \in aG_sa^{-1}$, then $g \in G_s$, so

$$\begin{aligned} (aga^{-1}) * s' &= a * (g * (a^{-1} * s^{-1})) \\ &= a * (g * s) \\ &= a * s = s'. \end{aligned}$$

So $aga^{-1} \in G_{s'}$ and hence $aG_sa^{-1} \subseteq G_{s'}$. Similarly, we can show that $a^{-1}G_{s'}(a^{-1})^{-1} \subseteq G_s$.

□

**Theorem 2.10.11** (The Orbit-Stabilizer Theorem)**.** If $G \curvearrowright S$ is a group action, and $s \in S$, then there is a bijection $f : \{aG_s \to O_s\}$ defined by $f(aG_s) = a * s$. Then

$$[G : G_s] = |O_s|.$$

*Proof.* We first check that $f$ is well-defined: if $aG_s = bG_s$, we want to check that $a * s = b * s$. From the proposition on cosets, $aG_s = bG_s \iff a^{-1}b \in G_s$. Then by the proposition on action: $a^{-1}b \in G_s \iff a * s = b * s$.
Now we check that $f$ is a bijection. *Injective*: if $f(aG_s) = f(bG_s)$, then

$$a * s = b * s \iff aG_s = bG_s \implies f \text{ is injective.}$$

*Surjective:* if $s' \in O_s$, we want $aG_s$ such that $f(aG_s) = s'$. But

$$s' \in O_s \implies \exists a \in G \text{ s.t. } a * s = s',$$

so $f(aG_s) = a * s = s'$. Hence, $f$ is surjective. Thus, $f$ is a bijection.

□

Recall from the Lagrange's theorem that for $H \leqslant G$:

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

Here we have $G_s \leqslant G$, so

$$|G| = |G_s| \cdot [G : G_s] = |G_s| \cdot |O_s|.$$

Hence,

$$\boxed{|G| = |G_s| \cdot |O_s| \quad \forall s \in S.}$$

**Example 2.10.12** (Rubik's Cube)**.** $G$ = rotational symmetries of a cube, $S$ = cube. Let $s$ = vertex $\in S$. Then $O_s = \{\text{vertices in } S\} \implies |O_s| = 8$ and $|G_s| = 3$. Then by O-S Theorem, we have $|G| = |G_s| \cdot |O_s| = 3 \cdot 8 = 24$.

### 2.10.2 Permutation Representations

**Definition 2.10.13** (Permutation representation)**.** A **permutation representation** of a group $G$ is a homomorphism $\varphi : G \to \text{Perm}(S)$ for some set $S$, where $\text{Perm}(S)$ is the **permutation group** of the set $S$, i.e., the set of bijections $S \to S$ with composition of functions being the binary operation.

**Theorem 2.10.14.** Given group $G$ and set $S$. There is a bijection

$$\{\text{actions of } G \text{ on } S\} \iff \{\text{permutation representations } G \to \text{Perm(S)}\}$$

*Proof.* If we have an action $G \curvearrowright S$, then we want a corresponding homomorphism $G \to \text{Perm}(S)$. Given $a \in G$, recall that we have a function $f_a : S \to S$ given by $f_a(s) = a * s$.

**Claim.** $f_a$ is a bijection, i.e., $f_a \in \text{Perm}(S)$.

*Proof of claim.* $f_a$ has an inverse $f_{a^{-1}} : S \to S$ since

$$\begin{aligned}(f_{a^{-1}} \circ f_a)(s) &= f_{a^{-1}}(f_a(s)) \\ &= a^{-1} * (a * s) \\ &= (a^{-1}a) * s = e * s = s.\end{aligned}$$

Similarly, $(f_a \circ f_{a^{-1}})(s) = s$. □

So given a group action $G \curvearrowright S$, define $\varphi : G \to \mathrm{Perm}(S)$ defined by $\varphi(a) = f_a$. We check that $\varphi$ is a homomorphism:

$$\begin{aligned}f_{ab}(s) &= (ab) * s \\ &= a * (b * s) \\ &= f_a(f_b(s)) \\ &= (f_a \circ f_b)(s).\end{aligned}$$

So we have a function $\{G \curvearrowright S\} \to \{\text{homomorphisms } G \to \mathrm{Perm}(S)\}$ defined by action $\mapsto (\varphi : G \to \mathrm{Perm}(S) \text{ s.t. } \varphi(a) = f_a)$. Now given a permutation representation $\varphi : G \to \mathrm{Perm}(S)$, we want to define an action $G \curvearrowright S$. Define $a * s = [\underbrace{\varphi(a)}_{\in \mathrm{Perm}(S)}](s)$. Now we check that this satisfies group action properties: (1) $e * s = [\varphi(e)](s) = \mathrm{id}_S(s) = s \quad \forall s \in S$. (2) $a * (b * s) = [\varphi(a)]([\varphi(b)](s)) = (\varphi(a) \circ \varphi(b))(s) = (\varphi(ab))(s) = (ab) * s \forall a, b \in G, \forall s \in S$. So this is indeed a group action $G \curvearrowright S$. Hence, we get the desired function. □

### 2.10.3 Faithful Representation

**Definition 2.10.15** (Faithful representation)**.** An injective permutation representation $\varphi : G \to \mathrm{Perm}(S)$ is called a **faithful representation**. The corresponding action $G \curvearrowright S$ is called a **faithful action**.

**Remark.** A faithful representation preserves the maximal amount of information about the original group.

> **Theorem 2.10.16** (Cayley's Theorem)**.** Every group is isomorphic to a subgroup of a permutation group.

*Proof.* We are looking for a faithful representation $G \to \mathrm{Perm}(S)$ for some $S$. Equivalently, we need to find a faithful action $G \curvearrowright S$ for some $S$.
Let $S = G$ (as a set) and $a * s = as$ (group multiplication). If $a * s = s$, then $as = s \implies a = e$. So our action $G \curvearrowright S$ is faithful, which implies that the homomorphism representation $G \to \mathrm{Perm}(S)$ is faithful, and so $G \cong \mathrm{im}(\varphi) \leqslant \mathrm{Perm}(S) = \mathrm{Perm}(G)$. □

**Remark.** If $|G| = n$, then $G \cong$ subgroup of $S_n$. Why? $\mathrm{Perm}(G) \cong S_n$.

### 2.10.4 Conjugation and the Class Equation

Recall the conjugation action $G \curvearrowright G$ defined by $g * a = gag^{-1}$.

**Definition 2.10.17** (Centralizer)**.** The stabilizer of $a \in G$ is called the **centralizer** of $a$, written

$$\begin{aligned} Z(a) &= \{g \in G \mid gag^{-1} = a\} \\ &= \{g \in G \mid ga = ag\}. \end{aligned}$$

The orbit of $a \in G$ is called the **conjugacy class** of $a$, written

$$C(a) = \{gag^{-1} \mid g \in G\}.$$

**Definition 2.10.18** (Center)**.** The **center** of a group $G$ is

$$Z(G) = \{g \in G \mid ga = ag \quad \forall a \in G\}.$$

**Remark.**

- $Z(G), Z(a) \leqslant G$.
- $Z(G) = \bigcap_{a \in G} Z(a)$, so $Z(a) \leqslant Z(G)$.
- $Z(a)$ contains $Z(G)$ and $\langle a \rangle$.
- If $b \in Z(a)$, then $\langle b \rangle \leqslant Z(a)$.
- The O-S Theorem implies that $|G| = |C(a)||Z(a)| \quad \forall a \in G$.
- $a \in Z(G) \iff Z(a) = G \iff C(a) = \{a\}$.
- $Z(G) = G \iff G$ is Abelian.
- $a \in C(a) \quad \forall a \in G$, as $eae^{-1} = a$.

Recall that the orbits of an action $G \curvearrowright S$ partition $S$, which implies that the conjugacy classes partition $G$.

If $G$ is finite, then there are finitely many conjugacy classes, call them $C_1, C_2, \ldots, C_k$.

**Definition 2.10.19** (Class Equation)**.** The equation:

$$|G| = |C_1| + |C_2| + \cdots + |C_k|$$

is called the **class equation**.

**Remark.**

- Since $e \in Z(G)$, $C(e) = \{e\}$ assume $C_1 = C(e)$, so $|C_1| = 1$. In fact every element in $Z(G)$ corresponds to a $+1$ in class equation (as $a \in Z(G) \iff C(a) = \{a\}$).
- By O-S theorem, each $|C_i|$ divides $|G|$.

**Example 2.10.20.** If $G$ is Abelian, $Z(G) = G$, so class equation is $|G| = \underbrace{1 + 1 + \ldots + 1}_{|G| \text{ times}}$.

**Example 2.10.21.** $G = S_3 = \{e, (12), (13), (23), (123), (132)\}$. $C(e) = \{e\}$. By O-S, $|C((123))| = \frac{|S_3|}{|Z((123))|}$. We know that $\langle (123) \rangle \leqslant Z((123))$ with order 3. By Lagrange, $|Z((123))|$ divides $|S_3| = 6$. Hence, $|Z((123))| = 3$ or 6. If it's 6, then $(123) \in Z(S_3)$. But $(12)(123)(12)^{-1} = (12)(12)(23)(12) = (32)(21) = (321) = (132) \neq (123)$. Hence $|Z((123))| = 3 \implies |C((123))| = 6/3 = 2$.

**Fact.** $|a| = |gag^{-1}| \quad \forall a, g \in G$.

$|C((12))| = 1, 2$, or 3, as we only have 3 unused elements in $S_3$. It's not 1 as (12) is not in the center. If it's 2, then $|C((23))|$ or $|C((13))|$ must be 1 as conjugacy classes partition $G$. But neither (13) nor (23) is in $Z(S_3)$, so $\neq 2$. Hence, it's 3. Thus,

$$|S_3| = 6 = \underbrace{1}_{C(e)=\{e\}} + \underbrace{2}_{C((123))} + \underbrace{3}_{C((12))}.$$

The class equation is then $6 = 1 + 2 + 3$!

**Techniques:**

- $|C(a)| = \frac{|G|}{|Z(a)|}$.
- of 1s $\leftrightarrow |Z(G)|$.
- $\langle a \rangle \leqslant Z(a)$ and $Z(G) \leqslant Z(a)$. Thus by Lagrange, $|a|$ and $|Z(G)|$ divide $|Z(a)|$.
- $|C(a)|$ and $|Z(a)|$ divide $|G|$.

#### 2.10.4.1 Normal Subgroups and Class Equations

**Proposition 2.10.22.** If $H \trianglelefteq G$ is a normal subgroup, and $a \in H$, then $C(a) \subseteq H$. And $H$ is a union of conjugacy classes.

*Proof.* If $a \in H$, then $gag^{-1} \in H \quad \forall g \in G$. But $\{gag^{-1} \mid g \in G\} = C(a) \implies C(a) \subseteq H$. Since every $a \in H$ is contained in some conjugacy class $C(a)$, we see $H = \bigcup_{a \in H} C(a)$. □

**Corollary 2.10.23.** $A_5$ is a simple group, i.e., it has no proper non-trivial normal subgroups.

*Proof.* We can work out the class equation for $A_5$ to be:

$$60 = 1 + 12 + 12 + 15 + 20.$$

IF $H \trianglelefteq A_5$, then $|H|$ divides $|A_5| = 60$, and $H = C(e) \bigcup \cdots$, so $|H| = 1 + \underbrace{\cdots}_{\text{combination of 12,15,20}}$. No combination divides 60 except $|H| = 1, |H| = 60$. □

#### 2.10.4.2 p-Groups

**Definition 2.10.24** (p-group)**.** A **p-group** is a group $G$ with $|G| = p^k$, for some prime $p$, integer $k \geqslant 1$.

**Proposition 2.10.25.** If $G$ is a p-group, then $|Z(G)| > 1$.

*Proof.* Class equation for $G$:

$$p^k = 1 + \cdots.$$

If $|Z(G)| = 1$, then every other term in class equation is larger than 1. Since they all divide $|G| = p^k$ and $p$ is prime, they are all powers of $p$. Thus,

$$p^k = 1 + p^{r_1} + p_{r_2} + \cdots + p^{r_n} \qquad (r_i \geqslant 1 \forall i),$$

which implies that

$$1 = p^k - p^{r_1} - p^{r_2} - \cdots - p^{r_n}.$$

The RHS is divisible by $p$, but LHS is not. Hence, a contradiction. Thus $|Z(G)| > 1$. □

**Proposition 2.10.26.** If $|G| = p^2$, then $G$ is Abelian.

*Proof.* $G$ Abelian $\iff Z(G) = G \iff |Z(G)| = p^2$. If $G$ is not Abelian, then $|Z(G)| = p$ as it's at least 1 (by proposition) and it's not $p^2$. Choose $a \notin Z(G)$. Then $Z(a)$ contains $Z(G)$ and $a$, which implies $|Z(a)| \geqslant p + 1$. But $|Z(a)|$ divides $p^2$, which means that $|Z(a)| = p^2$. Hence, $Z(a) = G$ and so $a \in Z(G)$, which contradicts $a \notin Z(G)$. Therefore, $|Z(G)| = p^2$, and $G$ is Abelian. □

## 2.11 Product Groups

Let $(G, p), (G', p')$ be two groups. We can construct the set $G \times G'$. Define binary operation $p \times p'$ :

$$p \times p'((a, a'), (b, b')) = (p(a, b), p'(a', b')).$$

This makes $G \times G'$ into a group, where the identity is $(e_G, e_{G'})$ and the inverse is $(a, a')^{-1} = (a^{-1}, a'^{-1})$.

**Definition 2.11.1** (Product group)**.** The group $(G \times G', p \times p')$ is called the **product group** of $(G, p)$ and $(G', p')$

**Remark.** $|G \times G'| = |G| \cdot |G'|$.

**Inclusion maps**

$$\begin{aligned} \iota_G : G &\to G \times G' \\ a &\mapsto (a, e) \end{aligned} \qquad \begin{aligned} \iota_{G'} : G' &\to G \times G' \\ a' &\mapsto (e, a') \end{aligned}$$

**Projection maps**

$$\begin{aligned} \pi_G : G \times G' &\to G \\ (a, a') &\mapsto a \end{aligned} \qquad \begin{aligned} \pi_{G'} : G \times G' &\to G' \\ (a, a') &\mapsto a' \end{aligned}$$

For the kernel, we have

$$\begin{aligned} \ker \pi_G &= \{(a, a') \in G \times G' \mid \pi_G(a, a') = e_G\} \\ &= \{(e_G, a') \in G \times G' \mid a' \in G'\} \\ &\cong G' \qquad \text{(isom. is } \iota_G : G \to \operatorname{im}(\iota_G) \leqslant G \times G'). \end{aligned}$$

Similarly, $\ker \pi_{G'} \cong G$. Then by the First Isomorphism Theorem, $G \times G'/\ker \pi_G \cong G'$ and $G \times G'/\ker \pi_{G'} \cong G'$.

Let $|a| = n$ in $G$ and $|a'| = m$ in $G'$. Note that $(a, a')^k = (e_G, e_{G'})$ in $G \times G'$. So if $(a, a')^k = (e_G, e_{G'})$, then $k$ must be a multiple of $n$ and $m$. Hence,

$$|(a, a')| = \operatorname{lcm}(n, m).$$

**Example 2.11.2.** In $\mathbb{Z}_2 \times \mathbb{Z}_3$,

$$\begin{aligned} |(\overline{1}, \overline{2})| &= \operatorname{lcm}(|\overline{1}|, |\overline{2}|) \\ &= \operatorname{lcm}(2, 3) \\ &= 6, \end{aligned}$$

$\implies \langle(\overline{1}, \overline{2})\rangle$ is cyclic, which implies $\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$.

**Proposition 2.11.3.** If $m, n$ are relatively prime, then $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$.

*Proof.* Consider $(\overline{1}, \overline{1}) \in \mathbb{Z}_m \times \mathbb{Z}_n$.

$$\begin{aligned} |(\overline{1}, \overline{1})| &= \operatorname{lcm}(|\overline{1}|, |\overline{1}|) \\ &= \operatorname{lcm}(m, n) = mn. \end{aligned}$$

Thus, $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic, which then implies it's $\cong \mathbb{Z}_{mn}$. □

**Proposition 2.11.4.** If $\gcd(m, n) \neq 1$, then $\mathbb{Z}_m \times \mathbb{Z}_n \ncong \mathbb{Z}_{mn}$.

*Proof.* $\mathbb{Z}_{mn}$ has an element of order $mn$. If $(\overline{a}, \overline{b}) \in \mathbb{Z}_m \times \mathbb{Z}_n$, then

$$\begin{aligned} |(\overline{a}, \overline{b})| &= \operatorname{lcm}(|\overline{a}|, |\overline{b}|) \\ &\leqslant \operatorname{lcm}(m, n) \\ &= \frac{mn}{\gcd(m, n)} < mn. \end{aligned}$$

So $\mathbb{Z}_m \times \mathbb{Z}_n$ has no element of $mn$. □

**Remark.** $\mathbb{Z}_2 \times \mathbb{Z}_2 \ncong \mathbb{Z}_4$. But $\mathbb{Z}_2 \times \mathbb{Z}_2$ has a subgroup $\{(\overline{0}, \overline{0}), (\overline{1}, \overline{0})\} \cong \mathbb{Z}_2$.

**Proposition 2.11.5.** If $|G| = p^2$, then $G \cong \mathbb{Z}_{p^2}$ or $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

*Proof.* Given $a \neq e$ in $G$, by Lagrange we have $|a| = p$ or $p^2$. If $\exists a \in G$ with $|a| = p^2$, then $G$ is cyclic and $G \cong \mathbb{Z}_{p^2}$. If not, then pick $a \in G$ with $|a| = p$, and pick $b \in G$ such that $b \notin \langle a \rangle$.

**Claim.** $\langle a \rangle \cap \langle b \rangle = \{e\}$.

*Proof.* Intersection $I$ is a subgroup as well, so $I \leqslant \langle a \rangle$, $I \leqslant \langle b \rangle$. $|I|$ divides $|\langle a \rangle| = |\langle b \rangle| = p$, which implies $|I| = 1$ or $p$. If it's $p$, then $\langle a \rangle = I = \langle b \rangle$. But $b \notin \langle a \rangle$. Hence, $|I| = 1$ and so $I = \{e\}$. □

**Claim.** $\{a^i b^j \mid 0 \leqslant i, j \leqslant p - 1\}$ is a set of order $p^2$.

*Proof.* If $a^i b^j = a^{i'} b^{j'}$ for some $i, i', j, j'$, $a^{i-i'} = b^{j'-j}$. But $\langle a \rangle \cap \langle b \rangle = \{e\}$. Then $a^{i-i'} = b^{j'-j} = e$, so $i = i', j = j'$. Thus, $G = \{a^i b^j\}$ since $|G| = p^2$. □

Now write down a function $\varphi : \mathbb{Z}_p \times \mathbb{Z}_p \to G$ defined by $\varphi((\overline{i}, \overline{j})) = a^i b^j$. $\varphi$ is a bijection and $\varphi(\overline{i} + \overline{i'}, \overline{j} + \overline{j'}) = a^{i+i'} b^{j+j'} = a^i a^{i'} b^j b^{j'} = a^i b^j a^{i'} b^{j'} = \varphi((\overline{i}, \overline{j}))\varphi((\overline{i'}, \overline{j'}))$, so $\varphi$ is an isomorphism. □

# Chapter 3

# Symmetry

## 3.1 Isometries

**Definition 3.1.1** (Isometry)**.** An **isometry** of $\mathbb{R}^n$ is a *rigid motion*, i.e., a bijection $f : \mathbb{R}^n \to \mathbb{R}^n$ that preserves distance:

$$\|\vec{x} - \vec{y}\| = \|f(\vec{x}) - f(\vec{y})\| \quad \forall \vec{x}, \vec{y} \in \mathbb{R}^n.$$

**Definition 3.1.2** (Symmetry)**.** If $A \subseteq \mathbb{R}^n$, then a **symmetry** of $A$ is an isometry $f : \mathbb{R}^n \to \mathbb{R}^n$ such that $f(A) = A$ (as sets), i.e., $f(\vec{a}) \in A \quad \forall \vec{a} \in A$ (and if $f(\vec{x}) \in A$, $\vec{x} \in A$).

**Example 3.1.3** (Translation)**.** Translation is an isometry: $f_{\vec{v}}(\vec{x}) = \vec{x} + \vec{v}$ for a fixed $\vec{v} \in \mathbb{R}^n$.

**Example 3.1.4** (Orthogonal linear maps)**.** Define $O(n) = \{A \in GL_n(\mathbb{R}) \mid A^\intercal = A^{-1}\}$, which is the *orthogonal group*. Given $A \in O(n)$, define $f_A : \mathbb{R}^n \to \mathbb{R}^n$ defined by $f_A(\vec{x}) = A\vec{x}$.

**Claim.** $f_A$ is an isometry.

*Proof.* $\|\vec{x}\| = \sqrt{\vec{x} \cdot \vec{x}}$. Given $\vec{x}, \vec{y} \in \mathbb{R}^n$, we show that $\|A\vec{x} - A\vec{y}\| = \|\vec{x} - \vec{y}\|$. But $\|A\vec{x} - A\vec{y}\| = \|A(\vec{x} - \vec{y})\|$. Since $A\vec{x} \cdot A\vec{y} = (A\vec{x})^\intercal(A\vec{y}) = \vec{x}^\intercal(A^\intercal A)\vec{y} = \vec{x}^\intercal\vec{y} = \vec{x} \cdot \vec{y}$, $\|A(\vec{x} - \vec{y})\| = \|\vec{x} - \vec{y}\|$. □

**Theorem 3.1.5.** If $f : \mathbb{R}^n \to \mathbb{R}^n$ is an isometry that fixes the origin (*i.e.*, $f(\vec{0}) = \vec{0}$), then $f = f_A$, for some $A \in O(n)$.

*Proof.* Given $f : \mathbb{R}^n \to \mathbb{R}^n$ such that $f(\vec{0}) = \vec{0}$. We want to show: (1) $f$ is linear $\iff$ $f(\vec{x}) = A\vec{x}$ for some $A \in GL_n(\mathbb{R})$, (2) $f$ preserves dot products ($\implies$ $A \in O(n)$).
We prove (2) by choosing $\vec{x}, \vec{y} \in \mathbb{R}^n$,

$$\begin{aligned}\|f(\vec{x}) - f(\vec{y})\| &= \sqrt{(f(\vec{x}) - f(\vec{y})) \cdot (f(\vec{x}) - f(\vec{y}))} \\ &= \sqrt{(\vec{x} - \vec{y}) \cdot (\vec{x} - \vec{y})}.\end{aligned}$$

Pick $\vec{y} = \vec{0} \implies f(\vec{y}) = f(\vec{0}) = \vec{0}$. Expanding $(\vec{x} - \vec{y}) \cdot (\vec{x} - \vec{y}) = (f(\vec{x}) - f(\vec{y})) \cdot (f(\vec{x}) - f(\vec{y}))$, we get $\vec{x} \cdot \vec{y} = f(\vec{x}) \cdot f(\vec{y})$. Hence, $f$ preserves the dot product.
(1) is left as an exercise. □

**Corollary 3.1.6.** Every isometry of $\mathbb{R}^n$ is $f(\vec{x}) = A\vec{x} + \vec{v}$, where $\vec{v} \in \mathbb{R}^n$ and $A \in O(n)$.

*Proof.* If $f(\vec{0}) = \vec{v}$, then let $T(\vec{x}) = \vec{x} - \vec{v}$. Then

$$\begin{aligned}(T \circ f)(\vec{0}) &= T(f(\vec{0})) \\ &= T(\vec{v}) = \vec{0}.\end{aligned}$$

So $T \circ f$ is an isometry that fixes $\vec{0}$. Then by the theorem, $T \circ f = f_A$ for some $A \in O(n) \implies f = T^{-1} \circ f_A$, i.e., $f(\vec{x}) = T^{-1}(f_A(\vec{x})) = T^{-1}(A\vec{x}) = A\vec{x} + \vec{v}$. □

**Remark.** This uses the fact that set of isometries is closed under composition. In fact, it's a group, called $\mathrm{Isom}(\mathbb{R}^n)$ or $E(n)$.

### 3.1.1 Orientation

**Claim.** The determinant of $A \in O(n)$ is $\pm 1$.

*Proof.* $(\det A)^2 = \det A \cdot \det A^\intercal = \det AA^\intercal = \det AA^{-1} = \det I = 1 \implies \det A = \pm 1$. □

**Definition 3.1.7.** If $\det A = 1$, $f_A$ is called **orientation preserving**. If $\det A = -1$, $f_A$ is called **orientation reversing**.

We have a homomorphism $\varphi : O(n) \to (\{\pm 1\}, \times)$ and $\ker \varphi = \{A \in O(n) \mid \det A = 1\}$, which is called the **special orthogonal group** $SO(n)$.

**Dimension 2**

**Theorem 3.1.8.** If $A \in O(2)$, then $f_A$ is a rotation about $\vec{0}$ or a reflection $\circ$ rotation.

*Proof.* Let $\vec{v} = f_A((1,0))$. Let $\ell$ be the line which contains $\vec{v}$ and $\ell'$ be the line perpendicular to $\ell$. Then $f_A((0,1))$ is a unit vector on $\ell'$ ($\vec{w}$ or $-\vec{w}$). If $f_A((0,1)) = \vec{w}$, then $f_A$ rotates $(1,0)$ and $(0,1)$ by a fixed angle $\theta$. Since $f_A$ is linear and $(x,y) = x(1,0) + y(0,1)$, $f_A(x,y) = x\vec{v} + y\vec{w}$, so $f_A$ is rotation by $\theta$. If $f_A((0,1)) = -\vec{w}$, then let $R$ = reflection in $\ell$, then $(R \circ f_A)((1,0)) = R(\vec{v}) = \vec{v}$ and $(R \circ f_A)((0,1)) = R(-\vec{w}) = \vec{w}$. Hence $R \circ f_A$ is a rotation, as above, which implies that $f_A = R^{-1} \circ$ rot. = refl. $\circ$ rot.. □

**Corollary 3.1.9.** If $f : \mathbb{R}^2 \to \mathbb{R}^2$ is any isometry, then $f$ is one of identity, translation, rotation, reflection, glide reflection (refl $\circ$ trans).

*Proof.* Exercise. □

**Fact.** Any isometry of $\mathbb{R}^2$ fixes ($f(\vec{x}) = \vec{x}$) $0, 1$ or infinitely many points.

**Dimension 3**

**Theorem 3.1.10.** If $A \in SO(3)$, then $f_A$ is a rotation about an axis through the origin.

**Corollary 3.1.11.** If $A \in O(3)$ has $\det A = -1$, then $f_A =$ refl$\circ$ rot..

# Chapter 4

# More Group Theory

## 4.1 The Sylow Theorems

Recall that $if H \leqslant G$ is a subgroup, then by Lagrange, $|H|$ divides $|G|$. But the converse is false.

**Definition 4.1.1.** If $G$ is a group, $|G| = p^e m$, where $p$ is prime, $e > 0$. and $p \nmid m$. Then a subgroup $H \leqslant G$ with $|H| = p^e$ is called a **Sylow p-subgroup** of $G$. Equivalently, $H$ is a p-group, and $p \nmid [G : H] = \frac{|G|}{|H|}$.

**Theorem 4.1.2** (First Sylow Theorem)**.** If $p \mid |G|$, then $G$ has a Sylow p-subgroup.

**Theorem 4.1.3** (Cauchy's Theorem)**.** If $p \mid |G|$, then $G$ contains an element of order $p$.

*Proof.* If $p \mid |G|$, then the first Sylow theorem implies that there exists $H \leqslant G$ with $|H| = p^e$. If $a \in H, a \neq e$, then $|a| \,||H| = p^e$, and $|a| \neq 1$, which implies $|a| = p^k$ for some $k$. Then $|a^{p^{k-1}}| = p$. □

**Definition 4.1.4.** $\mathrm{Syl}_p(G)$ = set of Sylow $p-$subgroups of $G$.

**Theorem 4.1.5** (Second Sylow Theorem)**.** Let $p \mid |G|$ be primte.

(i) All Sylow $p-$subgroups are *conjugate*, i.e., if $H, H' \in \mathrm{Syl}_p(G)$, then $\exists a \in G$ such that $aHa^{-1} = H'$.

(ii) Every $p-$subgroup ($H \leqslant G, |H| = p^\ell$ for some $\ell$) is contained in some Sylow $p-$subgroup.

**Corollary 4.1.6.** If $H \in \mathrm{Syl}_p(G)$, then

$$\mathrm{Syl}_p(G) = \{H\} \iff H \trianglelefteq G \text{ is normal.}$$

*Proof.* If $a \in G$, $aHa^{-1} \leqslant G$, and $|aHa^{-1}| = |H|$, $aHa^{-1} \in \mathrm{Syl}_p(G)$. $H \trianglelefteq G$ is normal $\iff$ $aHa^{-1} = H \quad \forall a \in G \iff \mathrm{Syl}_p(G) = \{H\}$ since any $H' \in \mathrm{Syl}_p(G)$ is $H' = aHa^{-1}$, for some $a \in G$. □

**Theorem 4.1.7** (Third Sylow Theorem)**.** Let $p \mid |G| = p^e m$ be prime, and let $n_p = |\mathrm{Syl}_p(G)|$. Then

- $n_p \mid m$.
- $n_p \equiv 1 \pmod{p}$.
- $n_p = [G : N_G(H)]$ for any $H \in \mathrm{Syl}_p(G)$ where $N_G(G)$ is the **normalizer** of $H$ in G:

$$N_G(H) = \{a \in G \mid aHa^{-1} = H\}.$$

$$H \trianglelefteq G \iff N_G(H) = G \iff [G : N_G(H)] = 1.$$

### 4.1.1 Applications

#### 4.1.1.1 Wilson's Theorem

**Theorem 4.1.8** (Wilson's Theorem)**.** A number $p \in \mathbb{N}$ is prime $\iff (p-1)! \equiv -1 \pmod{p}$.

*Proof.* If $n \in \mathbb{N}$ is composite, then $\exists$ prime $q < n$ such that $q \mid n$. Then if $(n-1)! \equiv -1 \pmod{n}$, then $(n-1)! = -1 + nk$ for some $k$. But $n = q\ell$ for some $\ell$, so $(n-1)! = -1 + q(\ell k) \implies (n-1)! \equiv -1 \pmod{q}$. Since $q \leqslant n-1$, $(n-1)! = (n-1)\cdots(q+1)q(q-1)\cdots 2 \cdot 1$. so $(n-1)!$ is a multiple of $q$, and so $(n-1)! \equiv 0 \pmod{q}$, so we have a contradiction and thus $(n-1)! \not\equiv -1 \pmod{n}$.

If $p \in \mathbb{N}$ is prime, consider $S_p$, the symmetric group. $|S_p| = p!$. Since $p \mid p!$ and $p^2 \nmid p!$, any $H \in \mathrm{Syl}_p(S_p)$ has order $p$, generated by a $p$-cycle in $S_p$. There are $(p-1)!$ $p$-cycles in $S_p$ because any $p$-cycle can be written as $(1 i_2 i_3 \dots i_p)$, where $\{i_2, \dots, i_p\} = \{2, \dots, p\}$ and there are $(p-1)!$ ways of choosing $i_2, \dots, i_p$. If $H, H' \in \mathrm{Syl}_p(S_p)$, and $H \neq H'$, then $H \cap H' = \{e\}$ (since $H \cap H' \leqslant H$ and $\leqslant H'$ and so its order is 1 or $p$. But its not $p$, as $H \neq H'$, so it's 1). Hence $n_p = |\mathrm{Syl}_p(S_p)| = \frac{(p-1)!}{p-1} = (p-2)!$. By Third Sylow theorem, $n_p \equiv 1 \pmod{p}$. Hence, $(p-2)! \equiv 1 \pmod{p}$ so $(p-1)(p-2)! \equiv p-1 \pmod{p}$, i.e., $(p-1)! \equiv -1 \pmod{p}$. □

**Lemma 4.1.9.** If $H, K \trianglelefteq G$, and $H \cap K = \{e\}$, and $|G| = |H||K|$, then $G \cong H \times K$.

**Theorem 4.1.10.** If $|G| = 15$, then $G \cong \mathbb{Z}_{15}$.

*Proof.* If $|G| = 15 = 5 \cdot 3$. Let $H \in \mathrm{Syl}_3(G), K \in \mathrm{Syl}_5(G)$. Then $n_3 \mid 5, n_3 \equiv 1 \pmod{3} \implies n_3 = 1$, so $H \trianglelefteq G$, and $n_5 \mid 3$, $n_5 \equiv 1 \pmod{5} \implies$ □

**Proposition 4.1.11.** If $|G| = 300$, then $G$ is not *simple*, i.e., $G$ has a non-trivial proper normal subgroup.

**Theorem 4.1.12** (Fundamental Theorem of Finitely Generated Abelian Groups)**.** Any finitely generated abelian group is isomorphic to $\underbrace{\mathbb{Z} \times \cdots \mathbb{Z}}_{m \geqslant 0} \times \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$ where $k \geqslant 0, n_i \geqslant 2$.

# Chapter 5

# Rings

**Definition 5.0.1** (Ring)**.** A **ring** is a set $R$ with binary operations $+$ and $\times$ satisfying:

(i) $(R, +)$ is an Abelian group where the identity is denoted by 0 and the inverse of $a \in R$ by $-a$.

(ii) $(R, \times)$ is a group possibly without inverses, or *monoid*, i.e. it's associative, has identity.

(iii) $+$ and $\times$ satisfy *distributivity* properties: $\begin{cases} a(b+c) & = ab + ac \\ (b+c)a & = ba + ca. \end{cases}$

**Definition 5.0.2** (Commutative ring)**.** A **commutative ring** is a ring where the multiplication is commutative.

**Remark.** Unless otherwise stated, all rings will be commutative. "Ring" = "commutative ring".

**Example 5.0.3** (Communative rings)**.** $(\mathbb{Z}, +, \times), (\mathbb{Q}, +, \times), (\mathbb{R}, +, \times), (\mathbb{C}, +, \times)$.

**Example 5.0.4.** $(\mathbb{Z}_n, +, \times)$ where $+, \times$ are mod $n$, additive identity $= \overline{0}$ and multiplicative identity $= \overline{1}$.

Note that from now on all rings are commutative.

**Example 5.0.5** (Gaussian Integers)**.** $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$.

**Remark.** Although every $\mathbb{C}$ number has a multiplicative inverse in $\mathbb{C}$, that inverse might not be in $\mathbb{Z}[i]$.

**Example 5.0.6.** $2^{-1} = \frac{1}{2} \in \mathbb{C}$, but $\frac{1}{2} \notin \mathbb{Z}[i]$.

**Example 5.0.7.** $\mathbb{Z}\left[\frac{1}{2}\right] = \{a + b \cdot \frac{1}{2} \mid a, b \in \mathbb{Z}\}$. Not good! Multiplication isn't closed! $\frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4} \notin \mathbb{Z}\left[\frac{1}{2}\right]$. Fix: $\mathbb{Z}\left[\frac{1}{2}\right] = \left\{a_0 + a_1 \cdot \frac{1}{2} + a_2 \cdot \frac{1}{4} + \cdots + a_n \cdot \frac{1}{2^n} \mid n \geqslant 0, a_i \in \mathbb{Z}\right\}$.

**Remark.** For $\mathbb{Z}[i]$, we don't need more than $a+bi$ since powers of $i$ are simple: $a_0 + a_1 i + a_2 i^2 + a_3 i^3 = (a_0 - a_2) + (a_1 - a_3)i$.

**Definition 5.0.8** (Subring)**.** A **subring** of $(R, +, \times)$ is a subset $S \subseteq R$ that is closed under $+, \times$, has additive inverses, and contains 1, i.e., $(S, +) \leqslant (R, +)$ and $S$ is closed under $\times$ and $1 \in S$.

**Example 5.0.9.** $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ are subrings.

**Example 5.0.10.** $\mathbb{Z} \subseteq Z[i] \subseteq \mathbb{C}$. $\mathbb{Z} \subseteq \mathbb{Z}\left[\frac{1}{2}\right] \subseteq \mathbb{Q}$.

**Remark.** $\mathbb{Z}\left[\frac{1}{2}\right]$ is the smallest subring of $\mathbb{Q}$ containing $\mathbb{Z}$ and $\frac{1}{2}$, i.e., if $S \subseteq \mathbb{Q}$ is a subring, and $\mathbb{Z} \subseteq S$ and $\frac{1}{2} \in S$, then $\mathbb{Z}\left[\frac{1}{2}\right] \subseteq S$. Similarly, $\mathbb{Z}[i]$ is the smallest subring of $\mathbb{C}$ containing both $\mathbb{Z}$ and $i$.

**Remark.** If $S \subseteq \mathbb{C}$ is a subring, then $\mathbb{Z} \subseteq S$. Why? All subrings contain 1, have additive inverses, and are closed under addition.

- $1+1, 1+1+1, \ldots \in S$
- $-1, -1+(-1), \ldots \in S$
- $0 \in S$, as $(S,+) \leqslant (R,+)$.

Similarly for subrings of $\mathbb{Q}, \mathbb{R}$, etc. Hence $\mathbb{Z}\left[\frac{1}{2}\right]$ is the smallest subring of $\mathbb{Q}$ containing $\frac{1}{2}$ and $\mathbb{Z}[i]$ is the smallest subring of $\mathbb{C}$ containing $i$.

**Example 5.0.11.** Choose $\alpha \in \mathbb{C}$. $\mathbb{Z}[\alpha]$ is the subring of $\mathbb{C}$ *generated by* $\alpha$, or $\mathbb{Z}$ *adjoin* $\alpha$, is the smallest subring of $\mathbb{C}$ containing $\alpha$. In particular, $\mathbb{Z}[\alpha] = \left\{\sum_{i=0}^{n} a_i \alpha^i \mid n \geqslant 0, a_i \in \mathbb{Z}\right\} = \{f(\alpha) \mid f(x) \text{ is an integer polynomial}\}$. For example, $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ (since $\sqrt{2}^2 = 2, \sqrt{2}^3 = 2\sqrt{2}, \sqrt{2}^4 = 4, \ldots$, so higher powers aren't needed). $\mathbb{Z}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Z}\}$.

**Example 5.0.12.** Similar definition for $\mathbb{Q}[\alpha]$ and $\mathbb{R}[\alpha]$ : smallest subrings of $\mathbb{C}$ containing $\mathbb{Q}$ (or $\mathbb{R}$) and $\alpha$: $\left\{\sum_{i=0}^{n} a_i \alpha^i \mid n \geqslant 0, a_i \in \mathbb{Q} (\text{or } a_i \in \mathbb{R})\right\}$.

## 5.1 Polynomial Rings

**Definition 5.1.1** (Polynomial ring)**.** If $x$ is a variable (not a specific element of $\mathbb{C}$), then $\mathbb{Z}[x]$ is the **polynomial ring** in variable $x$ with $\mathbb{Z}$ coefficients, i.e. if $f \in \mathbb{Z}[x]$, then $f(x) = a_0 + a_1 x + \cdots + a_n x^n$, for some $n \geqslant 0$, $a_i \in \mathbb{Z}$. Similarly, if $R$ is any ring, then $R[x]$ is the polynomial ring in variable $x$ with coefficients in $R$.

**Example 5.1.2.** In $\mathbb{Z}_4[x]$, we have elements $\overline{2}_x + \overline{1} = \overline{2}x^2 + x + \overline{3}$ and $(\overline{2}x + \overline{1}) + (\overline{2}x^2 + x + \overline{3}) = \overline{2}x^2 + (\overline{2} + \overline{1})x + (\overline{1} + \overline{3}) = \overline{2}x^2 + \overline{3}x$ and $(\overline{2}x + \overline{1})(\overline{2}x^2 + x + \overline{3}) = (\overline{2}\cdot\overline{2})x^3 + (\overline{1}\cdot\overline{2} + \cdot\overline{2}\cdot\overline{1})x^2 + (\overline{2}\cdot\overline{3} + \overline{1}\cdot\overline{1})x + (\overline{1}\cdot\overline{3}) = \overline{3}x + \overline{3}$.

**Example 5.1.3.** $(R[x])[y]$: polynomials in $y$ with coefficients in $R[x]$ (polynomials in $x$ with coefficients in $R$). For example, $y^2 + (1+x)y + (-x^3) \in (R[x])[y]$. After expanding, we get polynomials in variable $x$ and $y$ with $\mathbb{Z}$ coefficients: $-x^3 + y^2 + xy + y$ or can group $x$: $-x^3 + yx + (y^2 + y) \in (R[y])[x]$. Instead of distinguishing all these rings, we just write $R[x, y]$. In general, consider the ring $R[x_1, \ldots, x_n]$ of polynomials in variables $x_1, \ldots, x_n$ with coefficients in $R$.

There is a subring of $R[x]$ that can be identified with the ring $R$. $r \in R \iff f(x) = r \in R[x]$. We often write $R \subseteq R[x]$ is a subring.

**Example 5.1.4.** Ring of *Laurent polynomials*: $R[x, x^{-1}]$ is the ring

$$\left\{ \sum_{-n_1}^{n_2} a_i x^i \mid n_1 \geqslant 0, n_2 \geqslant 0, a_i \in R \right\}.$$

### 5.1.1 Division of Polynomials with Remainder

If $R$ is a ring, $f, g \in R[x]$ and $f$ is monic, then there exist unique polynomials $q, r \in R[x]$ such that $g(x) = f(x)q(x) + r(x)$ and $r(x) = 0$ or $\deg r < \deg f$.

*Proof.* Polynomial long division. □

**Corollary 5.1.5.** If $f(x) \in R[x]$, and $\alpha \in R$, then the remainder of dividing $f$ by $x - \alpha$ is $f(\alpha) \in R \subseteq R[x]$.

*Proof.* $x - \alpha \in R[x]$ is monic, so write $f(x) = (x - \alpha)q(x) + r(x)$, where $r = 0$ or $\deg r < \deg(x - \alpha) = 1$. Either way, $r$ is constant. So plug in $x = \alpha$ : $f(\alpha) = (\alpha - \alpha)q(\alpha) + r(\alpha) \implies r(\alpha) = f(\alpha)$. But $r$ is constant, so $r = f(\alpha)$. □

**Corollary 5.1.6.** If $f \in R[x]$ and $\alpha \in R$, then $f(\alpha) = 0 \iff f$ is divisible by $x - \alpha$.

*Proof.* $\implies$ : By corollary above. Conversely, if $f = (x-\alpha)g$ for some $g$, then $f(\alpha) = (\alpha-\alpha)g(\alpha) = 0$. □

**Definition 5.1.7** (Characteristic)**.** The **characteristic** of a ring $R$ is the smallest positive integer $n$ such that $\underbrace{1 + 1 + \cdots + 1}_{n \text{ times}} = 0$ (i.e. order of 1 in $(R, +)$).

**Notation.** $\text{char}R = n$. If no such $n$ exists, we say $\text{char}R = 0$.

**Example 5.1.8.** $\text{char}\mathbb{Z} = 0$, $\text{char}\mathbb{Z}_n = n$. $\text{char}R[x] = \text{char}R$. If $R = \{0\}$, then $R$ is the *zero ring*, in which $1 = 0$, then $\text{char}R = 1$.

**Exercise 5.1.9.** If $R$ is a ring in which $1 = 0$, then $R = \{0\}$.

**Definition 5.1.10** (Unit)**.** A **unit** in a ring $R$ is an element $a \in R$ that has a multiplicative inverse, i.e. $\exists b \in R$ such that $ab = 1 = ba$.

**Example 5.1.11.** In $\mathbb{Z}$, units are $\pm 1$. In $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, units are any $a \neq 0$. In $\mathbb{Z}_n$, units are any $\overline{a}$ with $\gcd(a, n) = 1$. In $\mathbb{Z}[i]$, units are $\pm 1, \pm i$.

## 5.2 Fields

**Definition 5.2.1** (Field)**.** A **field** is a ring where every non-zero element is a unit.

**Example 5.2.2.** $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$, not $\mathbb{Z}, \mathbb{Z}[i], \mathbb{Z}_n$.

If $f, g \in R[x]$, and leading coefficients of $f$ is any unit $u \in R$, then we can do division:

$$g/f = g/uu^{-1}f = (u^{-1}g)/(\underbrace{u^{-1}f}_{\text{monic}})$$

so write $f = u \cdot \overline{f}$, where $\overline{f}$ is monic (i.e. factor out $u$). Then divide $g = \overline{f}q + r$. Then $g = u^{-1}u\overline{f}q + r = f(u^{-1}q) + r$. In particular, we can do division for any $fg \in R[x]$, when $R$ is a field.

## 5.3 Ring Homomorphisms

**Definition 5.3.1** (Ring homomorphism)**.** $\varphi : R \to R'$ is a **ring homomorphism** if

- $\varphi(a + b) = \varphi(a) + \varphi(b)$ ($\varphi : (R, +) \to (R', +')$ is a group homomorphism)
- $\varphi(ab) = \varphi(a)\varphi(b)$

- $\varphi(1_R) = 1_{R'}$, where $1_R$ is the multiplicative identity in $R$ and $1_{R'}$ is the multiplicative identity in $R'$.

$\varphi$ is a **ring isomorphism** if it's a ring homomorphism and is bijective.

**Example 5.3.2.** $\varphi_k : \mathbb{Z} \to \mathbb{Z}$ defined by $\varphi_k(n) = kn$. $\varphi_k$ is a ring homomorphism $\iff k = 1$ as we need $\varphi(1) = 1$. We also need $\underbrace{\varphi(n)\varphi(m)}_{=(kn)(km)} = \varphi(nm) = knm \implies k^2mn = knm \implies k = 0$, or 1. But $k = 0$ doesn't work.

**Example 5.3.3.** $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ defined by $\varphi(x) = \overline{x}$ is a ring homomorphism.

**Example 5.3.4.** If $R$ is any ring, there is a unique ring homomorphism $\varphi : \mathbb{Z} \to R$, where $\varphi(0) = 0_R, \varphi(1) = 1_R, \varphi(-1) = -1_R$ and $\varphi(n > 0) = 1_R + \cdots + 1_R$ and $\varphi(n < 0) = (-1_R) + \cdots + (-1_R)$. Why unique? As a group, $\mathbb{Z}$ is cyclic generated by 1, so $\varphi(1)$ determines entire homomorphism and we need $\varphi(1) = 1_R$.

**Example 5.3.5.** If $R$ is any ring of characterisitc $n$, then there's a unique ring homomorphism $\varphi : \mathbb{Z}_n \to R$ sending $\overline{1} \mapsto 1_R$.

**Example 5.3.6.** If $R$ is any ring, and $r \in R$ is any element, then $\varphi_r : R[x] \to R$ defined by $\varphi(f(x)) = f(r)$ is a ring homomorphism. $(f + g)(r) = f(r) + g(r)$ and $(fg)(r) = f(r)g(r)$. Multiplicative identity in $R[x]$ is $f(x) = 1_R \mapsto f(r) = 1_R$.

**Example 5.3.7.** If $\varphi : R \to R'$ is any ring homomorphism, then we can write a ring homomorphism: $\varphi : R[x] \to R'[x]$ that maps $\sum a_i x^i \mapsto \sum \varphi(a_i)x^i$.

**Definition 5.3.8.** If $\varphi : R \to R'$ is a ring homomorphism, then the **kernel** of $\varphi$ is

$$\ker \varphi = \{r \in R \mid \varphi(r) = 0_{R'}\}$$

Note that $\varphi$ is also a group homomorphism $(R, +) \to (R', +')$, and its kernel as a group homomorphis = kernel as a ring homomorphism.

**Remark.** $\ker \varphi$ is *NOT* a subring of $R$ since $\varphi(1_R) = 1_{R'} \neq 0_{R'}$ (unless $R' = \{0\}$).

**Remark.** If $s \in \ker \varphi$, and $r \in R$, then $\varphi(rs) = \varphi(r)\varphi(s) = \varphi(r) \cdot 0_{R'} = 0_{R'} \implies rs \in \ker \varphi$. Similarly, $sr \in \ker \varphi$, but $sr = rs$.

### 5.3.1 Ideals

**Definition 5.3.9** (Ideal)**.** An **ideal** $I$ of a ring $R$ is a non-empty subset $I \subseteq R$ satisfying:

- $(I, +)$ is a subgroup of $(R, +)$
- If $s \in I$, $r \in R$, then $rs \in I$ (i.e. $I$ is closed under scaling by elements of $R$)
- Equivalently, $I \subseteq R$ is a non-empty subset such that whenever $s_1, \ldots, s_n \in I$, $r_1, \ldots, r_n \in R$, then $r_1s_1 + \cdots + r_ns_n \in I$ (i.e. linear combinations of elements of $I$ with coefficients in $R$ is still in $I$)

**Example 5.3.10.** The *principal ideal* generated by $a \in R$ is

$$(a) = \{ra \mid r \in R\}.$$

Also denoted $aR$ or $Ra$. *Closed under +:* $ra + r'a = (r + r')a \in (a)$; *Additive inverse:* $(-r)a = -ra \in (a)$; *Closed under scaling by elements of R:* $r'(ra) = (r'r)a \in (a)$. *Non-empty:* $(a) \neq \varnothing$, as $1 \cdot a = a \in (a)$. Hence, $(a)$ is an ideal.

**Definition 5.3.11** (Unit/zero ideal)**.** The **unit ideal** is $(1) = R$. The **zero ideal** is $(0) = \{0\}$.

**Definition 5.3.12** (Proper ideal)**.** A **proper ideal** is any $I \subset R$.

**Proposition 5.3.13.** $(a) = R \iff a$ is a unit.

*Proof.* If $(a) = R$, then $1 \in (a) \implies \exists b \in R$ such that $ba = 1$. This $b$ is the multiplicative inverse to $a$. Hence, $a$ is a unit.
Conversely, if $a$ is a unit, let $a^{-1}$ be its multiplicative inverse. Then given any $r \in R$, $r = (ra^{-1})a \in (a) \implies r \in (a)$. Hence, $R \subseteq (a)$. But of course $(a) \subseteq R$. Hence, $R = (a)$. □

**Remark.** A proper ideal is *never* a subring. Ideals are *almost* subrings except a subring must contain 1. Subrings are generally not ideals, as they are not required to be closed under scaling by $R$.

**Example 5.3.14.** $\mathbb{Z} \subseteq \mathbb{Q}, 2 \in \mathbb{Z}, \frac{1}{4} \in \mathbb{Q}$ but $\frac{1}{4} \cdot 2 = \frac{1}{2} \notin \mathbb{Z}$. Hence, $\mathbb{Z}$ is not an ideal but it is a subring.

**Remark.** What stops an ideal from being a subring is containing the multiplicative identity, whereas what stops a subring from being ideal is being closed under scaling by any element of $R$.

**Example 5.3.15.** $\varphi_r : R[x] \to R$ defined by $\varphi_r(f(x)) = f(r)$. The kernel is

$$\begin{aligned}\ker(\varphi_r) &= \{f \in R[x] \mid f(r) = 0\} \\ &= \{f \in R[x] \mid x - r \mid f\} \\ &= \{(x-r)g(x) \mid g \in R[x]\} \\ &= \underbrace{(x-r)}_{\text{principal ideal generated by } x-r \in R[x]}.\end{aligned}$$

**Example 5.3.16.** $\varphi : \mathbb{Z}[x] \to \mathbb{C}$ defined by $\varphi(f(x)) = f(i)$.

$$\begin{aligned}\ker\varphi &= \{f \in \mathbb{Z}[x] \mid f(i) = 0\} \\ &= \{f \in \mathbb{Z}[x] \subseteq \mathbb{C}[x] \mid f(i) = 0\} \\ &= \{f \in \mathbb{Z}[x] \subseteq \mathbb{C}[x] \mid x - i \mid f(i)\}.\end{aligned}$$

But $(x-i) \subseteq \mathbb{C}[x]$ but $(x-i) \nsubseteq \mathbb{Z}[x]$. In fact, we are looking for $(x-i) \cap \mathbb{Z}[x]$.
If $(x-i) \mid f \in \mathbb{Z}[x] \subseteq \mathbb{C}[x]$, then $f = (x-i)g(x)$ where $g(x)$ is from $\mathbb{C}[x]$. Take complex conjugates:

$$\overline{f(x)} = \overline{(x-i)} \cdot \overline{g(x)}.$$

Since $f$ has real coefficients, so $f(x) = \overline{f(x)} = \overline{(x-i)} \cdot \overline{g(x)} = (x+i)\overline{g(x)}$, which implies $(x+i) \mid f$. Hence, $(x-i)$ and $(x+i)$ are factors of $f$, which implies $(x-i)(x+i) \mid f$, i.e. $x^2+1 \mid f$. Hence, $\ker\varphi \subseteq (x^2+1)$. But if $(x^2+1)g(x) \in (x^2+1)$, then plug in $x = i$ : $(i^2+1)g(i) = 0 \implies (x^2+1)g(x) \in \ker\varphi$. Hence, $(x^2+1) \subseteq \ker\varphi$, and so $\ker\varphi = (x^2+1)$.

**Definition 5.3.17.** The ideal generated by $a_1, \ldots, a_n \in R$ is

$$(a_1, \ldots, a_n) = \{r_1a_1 + \cdots + r_na_n \mid r_i \in R\}.$$

**Example 5.3.18.** $(2, x) \subseteq \mathbb{Z}[x]$ contains all polynomials with an even constant term. $(2) \subseteq \mathbb{Z}[x]$ contains all polynomials with even coefficients. $(x) \subseteq \mathbb{Z}[x]$ contains all polynomials with 0 constant term.

**Claim.** $(2, x)$ is not a principal ideal.

*Proof.* If it is principal, $(2, x) = (f)$ for some $f \in \mathbb{Z}[x]$. Then $x \in (f)$ and $2 \in (f)$, so $2 = fg$ for some $g \implies f$ is constant ($\deg fg = \deg f + \deg g$) and in fact $f = \pm 1$ or $\pm 2$ as $f \mid 2$. If $f = \pm 1$, then $f$ is a unit, so $(f) = \mathbb{Z}[x]$. But $(2, x) \neq \mathbb{Z}[x]$, as $(2, x)$ only contains polynomials with even constant term. If $f = \pm 2$, then $f \mid x$, so $x = \pm 2g$ for some $g$. But no solution for $g$ as $\pm\frac{1}{2}x \notin \mathbb{Z}[x]$. Hence, no such $f$ exists, and $(2, x)$ is not principal. □

**Example 5.3.19.** If $\varphi : \mathbb{Z}[x] \to \mathbb{Z}_n$ is defined by $\varphi(f(x)) = \overline{f(0)}$, what is $\ker \varphi$? Certainly $\varphi(n) = 0$ and $\varphi(x) = 0$. This implies that $(n, x) \subseteq \ker \varphi$. $\varphi(fn + gx) = \varphi(f)\varphi(n) + \varphi(g)\varphi(x) = \overline{0}$ for any $f, g \in \mathbb{Z}[x]$. Also if $f(x) = a_m x^m + \cdots + a_1 x + a_0 \in \ker \varphi$, then $f(0) = a_0 \equiv 0 \pmod{n} \implies a_0 = nk$ for some $k \implies f(x) = x(a_m x^{m-1} + \cdots + a_1) + nk \in (n, x)$. Hence, $\ker \varphi \subseteq (n, x)$ and hence $\ker \varphi = (n, x)$.

Recall that a *field* is a ring in which all non-zero elements have multiplicative inverses.

**Theorem 5.3.20.** A ring is a field $\iff$ the only ideals of $R$ are $R$ and $(0)$.

*Proof.* If $R$ is a field, take $I \subseteq R$ such that $I \neq (0)$. Consider $a \in I$, $a \neq 0$. Then $R$ is a field, so $a$ is a unit. For any $r \in R, ra \in (a)$ and $ra \in I \implies (a) \subseteq I$. But $a$ is a unit $\implies (a) = R$. Hence, $I = R$.
Conversely, take $a \in R, a \neq 0$. Then $(a) \neq (0)$ as $a \in (a)$ but $a \notin (0) \implies (a) = R \implies a$ is a unit. □

**Corollary 5.3.21.** If $\varphi : F \to R$ is a ring homomorphism, where $F$ is a field, then $\varphi$ is injective (or $R = \{0\}$).

*Proof.* $\ker \varphi$ is an ideal of $F$. If $R \neq \{0\}$, then $\varphi(1_F) = 1_R \neq 0_R$, so $\ker \varphi \neq F$. Then by the theorem above, $\ker \varphi = (0)$. Hence, $\varphi$ is injective (proved for groups, but also holds here). □

**Remark.** There isn't always a ring homomorphism from $R \to R'$ for rings $R, R'$ (unlike the case for groups).

**Proposition 5.3.22.** If $F$ is a field, then every ideal in $F[x]$ is a principal ideal, i.e. if $I \subseteq F[x]$ is an ideal, then $I = (f)$ for some $f \in F[x]$.

*Proof.* The idea is to emulate the proof that subgroups of $\mathbb{Z}$ are $\langle a \rangle$ for some $a$. Let $I \subseteq F[x]$ be an ideal, $I \neq (0)$. Choose $f \in I$ of smallest degree. We want to show $I = (f)$. If $g \in (f)$, then $g = fh$ for some $h \in F[x]$. Since $f \in I, h \in F[x], fh \in I$. Hence, $g \in I$ and so $(f) \subseteq I$.
If $g \in I$, use division algorithm to write $g = fq + r$ for some $q, r \in F[x]$, where $r = 0$ or $\deg r < \deg f$ (this uses "$F$ is a field", so leading coefficient of $f$ is always a unit). If $r = 0$, then $g = fq \in (f)$. If $r \neq 0$, then $r = \underbrace{g}_{\in I} - \underbrace{f}_{\in I}\underbrace{g}_{\in F[x]} \in I$. But now $r \in I$ and $\deg r < \deg f$, which contradicts to the choice of $f$ as having the smallest degree in $I$. So can't have $r \neq 0$, so $r = 0$ and $g \in (f) \implies I \subseteq (f)$. Hence, $I = (f)$. □

**Definition 5.3.23** (gcd). If $F$ is a field, $f, g \in F[x]$ not both 0, then the **greatest common divisor** of $f, g$ is $\gcd(f, g) = d \in F[x]$, where $(f, g) = (d)$ and $d$ is monic.

## 5.4 Quotient Rings

Recall that an ideal $I \subseteq R$ in a ring is:

- $(I,+) \leqslant (R,+)$ is a subgroup. Since $R$ is abelian, $(I,+) \trianglelefteq (R,+)$.
- For any $s \in I, r \in R$, we have $rs \in I$.
- Ideals are to rings what normal subgroups are to groups.

**Definition 5.4.1** (Quotient Rings)**.** Let $R$ be a ring, $I \subseteq R$ an ideal. Then $(R,+)/(I,+)$ is a quotient group. The cosets of $I : a + I$, for $a \in I$.
**Notation:** $\overline{a} = a + I = \{a + s \mid s \in I\}$.

$R/I$ has an Abelian group structure and it is a ring.

**Remark.** $\pi : R \to R/I$ defined by $\pi(a) = \overline{a}$ is a surjective ring homomorphism and $\ker \pi = I$.

**Theorem 5.4.2** (First Isomorphism Theorem)**.** If $\varphi : R \to R'$ is a ring homomorphism $I = \ker \varphi$, then $R/I \cong \mathrm{im}(\varphi)$.

**Example 5.4.3.** If $I = (0) = \{0\}$, then $R/I \cong R$. Why? $\varphi : R \to R$ is an isomorphism, so $\ker \varphi = (0)$, $\varphi$ is surjective. By the theorem, $R/(0) \cong R$.

**Example 5.4.4.** $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ defined by $\varphi(k) = \overline{k}$. $\ker \varphi = \{k \in \mathbb{Z} \mid \overline{k} = \overline{0}\} = \{k \in \mathbb{Z} \mid k \equiv 0 \pmod n\} = \{kn \mid k \in \mathbb{Z}\} = (n)$. 1st Isomorphism Theorem $\implies \mathbb{Z}/(n) \cong \mathbb{Z}_n$.

**Claim.** $\mathbb{Z}[x]/(x-2) \cong \mathbb{Z}$.

*Proof.* $\varphi_2 : \mathbb{Z}[x] \to \mathbb{Z}$ defined by $\varphi_2(f(x)) = f(2)$. $\varphi_2$ is surjective and $\ker \varphi_2 = (x-2)$. By 1st Isomorphism Theorem, $\mathbb{Z}[x]/(x-2) \cong \mathbb{Z}$. □

**Takeaways:**

- $(\mathbb{Z}[x]/(f))/(\overline{g}) \cong \mathbb{Z}[x]/(f,g) \cong (\mathbb{Z}[x]/(g))/(\overline{f})$.
- $\mathbb{Z}[x]/(x-a) \cong \mathbb{Z} \quad \forall a \in \mathbb{Z}$ via 1st Isomorphism Theorem on $\varphi_a : \mathbb{Z}[x] \to \mathbb{Z}$ defined by $\varphi_a(f(x)) = f(a)$.
- If $\varphi : R \to R'$ is an isomorphism, then $R/(a) \cong R'/(\varphi(a))$.

**Example 5.4.5.** Identify $R = \mathbb{Z}[x]/(x^2-3, 2x+4)$. Let's understand and simplify $I = (x^2-3, 2x+4)$, i.e. find a simpler set of generators for $I$. Note that $2(x^2-3) + (2-x)(2x+4) \in I$, i.e. $2x^2 - 6 + 4x + 8 - 2x^2 - 4x = 2 \in I$.

**Claim.** $\underbrace{(x^2-3, 2x+4)}_{I} = \underbrace{(x^2-3, 2)}_{I'}$.

*Proof.* Need to show $x^2-3, 2 \in I$ and $x^2-3, 2x+4 \in I'$. $x^2-3 \in I$ and $\in I'$ as it's a generator. We already showed $2 \in I$. $2x+4 = 0 \cdot (x^2-3) + (x+2) \cdot 2 \in I'$. Hence, $I \subseteq I', I' \subseteq I \implies I = I'$. □

*Alternative proof:* Since $2 \in I$, we can write $(x^2-3, 2x+4) = (x^2-3, 2x+4, 2) = (x^2-3, 2)$. □

So $R \cong \mathbb{Z}[x]/I \cong \mathbb{Z}[x]/(2, x^2-3) \cong (\mathbb{Z}[x]/(2))/(\overline{x^2-3})$ and $\mathbb{Z}[x]/(2) \cong \mathbb{Z}_2[x]$ (since $\varphi : \mathbb{Z}[x] \to \mathbb{Z}_2[x]$ defined by $\varphi(\sum a_i x^i) = \sum \overline{a_i} x^i$ is surjective and ker = {polynomials with even coefficients} = (2)). Then $R \cong \mathbb{Z}_2[x]/(x^2+\overline{1})$ (since in $\mathbb{Z}_2[x]$, $\overline{x^2-3} = x^2+\overline{1}$). Elements of $R$ are $\overline{f}$ for $f \in \mathbb{Z}_2[x]$. Say $f = a_0 + a_1 x + \cdots + a_n x^n$ where $a_i \in \{\overline{0}, \overline{1}\}$ for each $i$. In $R$, $\overline{x^2+\overline{1}} = \overline{0}$, since we're quotienting by $(x^2+\overline{1}) \implies \overline{x^2} = \overline{\overline{-1}} = \overline{\overline{1}}$ (identity in $R$)

$$\begin{aligned}
\overline{f} &= \overline{a_0} + \overline{a_1 x} + \cdots + \overline{a_n}\overline{x^n} \\
&= \overline{a_0} + \overline{a_1 x} + \overline{a_2} + \overline{a_3 x} + \cdots \\
&= \left(\sum_{i \text{ even}} \overline{a_i}\right) + \left(\sum_{i \text{ odd}} \overline{a_i}\right)\overline{x} \\
&= \underbrace{\overline{\left(\sum_{i \text{ even}} a_i\right)}}_{\in \mathbb{Z}_2} + \underbrace{\overline{\left(\sum_{i \text{ odd}} a_i\right)}}_{\in \mathbb{Z}_2}.\overline{x}
\end{aligned}$$

Hence, $R = \{\overline{\overline{0}}, \overline{\overline{1}}, \overline{x}, \overline{x+\overline{1}}\}$.

## 5.5 Product Rings

**Definition 5.5.1** (Product rings)**.** Given rings $R$ and $R'$, the **product ring** $R \times R'$ has underlying set $R \times R'$ and binary operations:

- $(a, a') + (b, b') = (a + b, a' + b')$
- $(a, a') \cdot (b, b') = (ab, a'b')$.
- identities for addition $(0_R, 0_{R'})$ and $(1_R, 1_{R'})$ for multiplication.

**Question.** Given a ring, can I determine whether it's isomorphic to a product ring?

### 5.5.1 Idempotents

**Definition 5.5.2** (Idempotent element)**.** An **idempotent element** is $e \in R$ such that $e^2 = e$.

**Example 5.5.3.** $0^2 = 0, 1^2 = 1$ are always idempotents. $\mathbb{Z}_2 \times \mathbb{Z}_2$ has non-trivial idempotents: $(\overline{0}, \overline{1}), (\overline{1}, \overline{0})$.

**Remark.**

- If $e$ is idempotent, then so is $e' = 1 - e$. Check: $(e')^2 = (1-e)^2 = 1 - 2e + e^2 = 1 - 2e + e = 1 - e = e'$. $ee' = 0$.
- $ee' = 0$. Check: $ee' = e(1-e) = e - e^2 = e - e = 0$.
- The principal ideal $(e)$ generated by $e$ is itself a ring with multiplicative identity $e$. (not a subring of $R$). Check: every ideal is a ring except that it's missing a multiplicative identity, so check that $e$ is a multiplicative identity for elements of $(e)$: given $b \in (e), b = ae$ for some $a \in R$. Then $eb = e(ae) = ae^2 = ae = b$.

**Theorem 5.5.4.** If $e \in R$ is idempotent, then $R \cong (e) \times (e')$.

*Proof.* Define $\varphi : R \to (e) \times (e')$ defined by $\varphi(a) = (ae, ae')$. $\varphi$ is a homomorphism: $\varphi(a+b) = ((a+b)e, (a+b)e') = (ae+be, ae'+be') = (ae, ae') + (be, be') = \varphi(a) + \varphi(b)$. $\varphi(ab) = (abe, abe') = (abe^2, ab(e')^2) = ((ae)(be), (ae'(be')) = (ae, ae')(be, be') = \varphi(a)\varphi(b)$. $\varphi(1) = (1e, 1e') = (e, e')$, multiplicative identity in $(e) \times (e')$. $\varphi$ is injective: if $\varphi(a) = (0,0)$, then $ae = 0$ and $ae' = 0 \implies 0 = ae + ae' = a(e+e') = a(e + (1-e)) = a \implies a = 0$. Hence, $\ker \varphi = (0)$ and so $\varphi$ is injective. $\varphi$ is surjective: if $(ae, be') \in (e) \times (e')$, then let $c = ae + be'$. Then

$$\begin{aligned}\varphi(c) &= ((ae+be')e, (ae+be')e') \\ &= (ae^2 + bee', aee' + b(e')^2) \\ &= (ae, be').\end{aligned}$$

Hence, $\varphi$ is bijective, and hence an isomorphism. □

**Remark.** If $e = 1$, then $e' = 0$ (or vice versa), so by the theorem, $R \cong (1) \times (0) = R \times \{0\}$ (isomorphism is $r \mapsto (r, 0)$).

How to think about this? If $R \cong R_1 \times R_2$, then we have idempotents $e = (1,0)$ and $e' = (0,1)$ and any element $(a,b)$ of $R_1 \times R_2$ can be written as $ae + be'$. Hence, $R$ can be written as a non-trivial product $\iff \exists$ non-trivial idempotents in $R$.

**Example 5.5.5.** $R = \mathbb{Z}_6$. $e = \overline{3}$ is idempotent, as $\overline{3^2} = \overline{9} = \overline{3}$. Thus, $e' = \overline{1} - \overline{3} = \overline{-2} = \overline{4}$ is also idempotent and by the theorem, $\mathbb{Z}_6 \cong (\overline{3}) \times (\overline{4}) \cong \mathbb{Z}_2 \times \mathbb{Z}_3$. Similarly, $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$ when $\gcd(m,n) = 1$ as rings.

## 5.6 Adjoining Elements

**Example 5.6.1.** Say we have $\mathbb{Z}$ and we want to "enlarge" $\mathbb{Z}$ to a larger ring that contains a multiplicative inverse to 2.

**Idea:** A multiplicative inverse $\alpha$ to 2 satisfies $2\alpha = 1$, i.e. $2\alpha - 1 = 0$, i.e. $\alpha$ is a root of $2x - 1$. Consider $\mathbb{Z}[x]$, let $R = \mathbb{Z}[x]/(2x-1)$. Let $\alpha = \overline{x} = x + (2x-1)$ (coset associated to $x$). Then $\overline{2x-1} = \overline{0} \implies \overline{2} \cdot \overline{x} - \overline{1} = \overline{0}$, i.e. $\overline{2}\alpha = \overline{1}$ in $R$.

**Remark.** $R \cong \mathbb{Z}\left[\frac{1}{2}\right]$.

In general, if $R$ is a ring, and $\alpha$ is a solution to $f_1(x) = 0, f_2(x) = 0, \ldots, f_n(x) = 0$ (where $f_i \in R[x]$). Then $R' = R[x]/(f_1, f_2, \ldots, f_n)$ is called a **ring extension** of $R$ by *adjoining* $\alpha$ to $R$. We write $R' = R[\alpha]$.

**Example 5.6.2.** Want a ring extension of $\mathbb{Z}$ by an element $\alpha$ satisfying $2\alpha = 6, 6\alpha = 15$, i.e. $2\alpha - 6 = 0, 6\alpha - 15 = 0$. So ring extension is $R = \mathbb{Z}[x]/(2x-6, 6x-15)$. Then $\alpha = \overline{x} \in R$ is the desired element. For example, if we have $\overline{6}\alpha - \overline{2}\alpha - \overline{2}\alpha = \overline{15} - \overline{6} - \overline{6}$. Then $\overline{2}\alpha = \overline{3}$, but we also have $\overline{2}\alpha = \overline{6} \implies \overline{3} = \overline{6}$ in $R \implies \overline{3} = \overline{0}$ in $R$.

**Example 5.6.3.** Ring extension of $\mathbb{Z}$ by $\alpha$ satisfying $2\alpha = 0$, i.e. $R = \mathbb{Z}[x]/(2x)$. However, $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$. But in $R$, $\overline{x} \neq \overline{0}$, but $\overline{2}\overline{x} = \overline{0}$.

**Example 5.6.4.** If $R$ is an extension of $\mathbb{R}$ by $\alpha$ satisfying $\alpha^2 = 1$, then $R \cong \mathbb{R} \times \mathbb{R}$. As an exercise, check $R[x]/(x^2-1) \cong \mathbb{R} \times \mathbb{R}$.

Hence, it's important to understand $R[x]/(f)$ for $f \in R[x]$. If $f$ is monic, i.e. $f = x^n + a_{n-1}x^{n-1} + \cdots + a_0$. Let $\alpha$ denote a root of $f$, i.e. $\alpha = \overline{x} \in R[x]/(f)$. Denote $R[x]/(f) \cong R[\alpha]$. Then $R[\alpha]$ has a *basis* $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ over $R$. Why? if $g = \sum_k a_k x^k \in R[x]$, then $\overline{g} = \sum_k \overline{a_k x}^k$, then $\overline{g} = \sum_k \overline{a_k}\overline{x}^k$. If $k \geqslant n$, then $\overline{x}^k = \overline{x}^n \cdot \overline{x}^{k-n} = \alpha^n \alpha^{k-n} = (-\overline{a_{n-1}}\alpha^{n-1} - \cdots - \overline{a_1}\alpha - \overline{a_0})\alpha^{k-n}$ since $\overline{f} = \overline{0} \implies \overline{x^n + a_{n-1}x^{n-1} + \cdots + a_0} = \overline{0} \implies \alpha^n + \overline{a_{n-1}}\alpha^{n-1} + \cdots + \overline{a_0} = \overline{0}$ solve for $\alpha^n$. Repeat until $\overline{g}$ has no powers of $\alpha$ larger than $n-1$. (also need to check linear independence)

**Question.** If $\overline{g}, \overline{h} \in R[\alpha]$, what is $\overline{g} \cdot \overline{h}$?

**Answer.** Write $gh = fq + r$, for some $q, r \in R[\alpha]$ where $r = 0$ or $\deg r < \deg f$. Then $\overline{g}\overline{h} = \overline{f}\overline{q} + \overline{r} = \overline{r}$.

**Example 5.6.5.** Consider $\mathbb{Z}_5$, and adjoin a square root of $\overline{3}$. $R = \mathbb{Z}_5[\sqrt{\overline{3}}] \cong \mathbb{Z}_5[x]/(x^2 - \overline{3})$. Let $\alpha = \overline{x} \in R$. Then by above, $x^3 - \overline{3}$ monic $\implies$ $\{\overline{1}, \alpha\}$ is a basis for $R \implies$ elements of $R$ are $\{A + B\alpha \mid A, B \in \mathbb{Z}_5\}$ and where $\alpha^2 = \overline{3}$.

**Claim.** $R$ is a field of order 25.

*Proof.* $\overline{A} + \overline{0}\overline{\alpha} = \overline{A}$ is a unit for all $\overline{A} \neq \overline{0}$, since $\mathbb{Z}_5$ is a field. So assume $\overline{B} \neq \overline{0}$. Then $(\overline{A} + \overline{B}\alpha)(\overline{A} - \overline{B}\alpha) = \overline{A}^2 - \overline{B}^2\alpha^2 = \overline{A}^2 - \overline{3}\overline{B}^2$. We can think of this as being in $\mathbb{Z}_5$, and it's invertible if $\neq \overline{0}$. If $\overline{A}^2 - \overline{3}\overline{B}^2 = \overline{0}$ in $\mathbb{Z}_5$, then $\overline{3} = \overline{A}^2(\overline{B}^{-1})^2 = (\overline{A}\overline{B}^{-1})^2$. But $\overline{3}$ is not a square in $\mathbb{Z}_5$, so $\overline{A}^2 - \overline{3}\overline{B}^2 \neq \overline{0} \implies (\overline{A} + \overline{B}\alpha)(\overline{A} - \overline{B}\alpha)(\overline{A} - \overline{3}\overline{B}^2)^{-1} = \overline{1} \implies \overline{A} + \overline{B}\alpha$ is a unit in $R \implies R$ is a field. □

## 5.7 Fractions

**Definition 5.7.1** (Fraction)**.** Given a ring $R$, a **fraction** is $\frac{a}{b}$, for $a, b \in R, b \neq 0$. Consider $\frac{a}{1}$ as $a$. Let $\frac{a}{b} \sim \frac{c}{d} \iff ad = bc$. Define $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$, $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$.
**Problem:** What if $b, d \neq 0$, but $bd = 0$? For example in $\mathbb{Z}_4$, $\overline{2} \cdot \overline{2} = \overline{0}$, but $\overline{2} \neq \overline{0}$.

**Definition 5.7.2** (Zero-divisor)**.** A **zero-divisor** is $a \in R$ such that $ab = 0$ for some $b \neq 0$.

**Remark.** 0 is always a zero-divisor unless $R = \{0\}$.

**Definition 5.7.3** (Integral Domain)**.** An **integral domain** or **ID**, is a ring $R$ with no non-trivial zero-divisors, i.e. $ab = 0 \implies a = 0$ or $b = 0$.

### 5.7.1 Properties of Integral Domains

- IDs have cancellation law: if $a \neq 0, ab = ac$, then $b = c$. (since $ab - ac = 0 \implies a(b-c) = 0 \implies b - c = 0 \implies b = c$).
- If $R$ is an ID, then if $f, g \in R[x]$, then $\deg(fg) = \deg f + \deg g$.

**Theorem 5.7.4.** If $R$ is an integral domain, and $F$ is the set of equivalence classes of fraction in $R$, then $F$ is a field with fractions addition/multiplication as given above, called the *field of fractions* of $R$ (or *field of quotients*).

**Example 5.7.5.** If $R$ is an ID, then $R[x]$ is an integral domain. The field of fractions of $R[x]$ is written $R(x) = \{f/g \mid f, g \in R[x], g \neq 0\}/\sim$ called the *ring of rational function over R*.

**Example 5.7.6.** Any field is an ID. If $ab = 0, a \neq 0$, then $a^{-1}ab = a^{-1}0 \implies b = 0$.

**Example 5.7.7.** Any subfield of an ID is an ID: $\mathbb{Q}[\alpha] \subseteq \mathbb{C}$ is an ID, as $\mathbb{C}$ is a field, its field of fractions is written $\mathbb{Q}(\alpha)$.

**Example 5.7.8.** $\mathbb{Z}_p$ is an ID when $p$ is prime (also a field) but $\mathbb{Z}_n$ is not an ID if $n$ is composite.

## 5.8 Maximal Ideals

**Question.** If $R$ is any ring, and $I \subseteq R$ is an ideal, under what condition is $R/I$ an ID/field?

**Definition 5.8.1** (Maximal Ideal)**.** An ideal $I \subseteq R$ is a **maximal ideal** if $I \neq R$ and if $I \subseteq J$, then $J = I$ or $J = R$.

**Example 5.8.2.** $I = (x) \subseteq \mathbb{Z}[x]$ is not maximal since $(x) \subset (2, x) \subset \mathbb{Z}[x]$.

**Exercise 5.8.3.** $(2, x)$ is maximal in $\mathbb{Z}[x]$.

**Example 5.8.4.** $I = (x) \subseteq \mathbb{Q}[x]$ is maximal. Why? If $(x) \subseteq J \subseteq \mathbb{Q}[x]$, then $J$ is an ideal in $[x]$, and $\mathbb{Q}$ is a field, by the proposition, we have $J = (f)$ for some $f \in \mathbb{Q}[x]$. Notice that $x \in (x) \subseteq J \implies x \in (f) \implies \exists g \in \mathbb{Q}[x]$ such that $x = fg$. Then $\deg f = 0, \deg g = 1$ or $\deg f = 1, \deg = 0$. If $\deg f = 0$, then $f = c \neq 0 =$ unit $\implies J = (f) = \mathbb{Q}[x]$. If $\deg f = 1$, then $f = ax + b$ for some $a, b, c \in \mathbb{Q}$ and $g = c$, which implies that $1 \cdot x + 0 = (ax + b)c = acx + bc \implies ac = 1, bc = 0 \implies b = 0, ac = 1$. Hence, $f = ax \implies f \in (x) \implies (f) \subseteq (x)$. Therefore, $J \subseteq I \implies I = J$.

**Proposition 5.8.5.** $R/I$ is a field $\iff$ $I$ is a maximal ideal of $R$ (or $I = R$).

*Proof.* $R/I = \{0\} \iff I = R$. So assume $R/I \neq \{0\}$. Consider homomorphism $\pi : R \to R/I$ defined by $\pi(a) = \overline{a}$. We know that $R/I$ is a field $\iff$ only proper ideal of $R/I$ is $(0)$.

**Claim.** If $J \subseteq R/I$ is an ideal, then $\pi^{-1}(J) = \{s \in R \mid \pi(s) \in J\}$ is an ideal of $R$ that contains $I = \ker \pi$.

*Proof of claim.* If $s, t \in \pi^{-1}(J)$, then $\pi(s + t) = \pi(s) + \pi(t) \in J \implies s + t \in \pi^{-1}(J)$. If $s \in \pi^{-1}(J)$, then $\pi(-s) = -\pi(s) \in J \implies -s \in \pi^{-1}(J)$. If $s \in \pi^{-1}(J), r \in R$, then $\pi(rs) = \pi(r)\pi(s) \in J \implies rs \in \pi^{-1}(J)$. Since $\overline{0} \in J, \ker \pi = \pi^{-1}(\overline{0}) \subseteq \pi^{-1}(J)$. But $\ker \pi = I$, so $I \subseteq \pi^{-1}(J)$. □

So if $J \subseteq R/I$ is an ideal, then $\pi^{-1}(J)$ is an ideal such that $I \subseteq \pi^{-1}(J) \subseteq R$. $\pi$ is surjective $\implies \pi(\pi^{-1}(J)) = J$.

If $I$ is maximal, then $\pi^{-1}(J)$ is $I$ or $R$. If $\pi^{-1}(J) = I$, then $J = \pi(I) = (\overline{0}$. If $\pi^{-1}(J) = R$, then $J = \pi(R) = R/I$. So $R/I$ has only $(\overline{0})$ and $R/I$ as ideals, then $R/I$ is a field.

Conversely, if $R/I$ is a field, then consider $I \subset J \subseteq R$, then $\pi(J) \neq (\overline{0})$, and it's an ideal in $R \implies \pi(J) = R/I$ (since $R/I$ is a field). Then $J = \pi^{-1}(\pi(J)) = R$. Hence, $I$ is maximal. □

**Example 5.8.6.** $(0) \subseteq F$ is a maximal ideal, when $F$ is a field.

## 5.9 Prime Ideals

**Definition 5.9.1** (Prime ideal)**.** An ideal $I \subseteq R$ is a **prime ideal** if $ab \in I \implies a \in I$ or $b \in I$.

**Proposition 5.9.2.** $R/I$ is an integral domain $\iff$ $I$ is a prime ideal in $R$.

*Proof.* If $I$ is prime, consider $\overline{a}, \overline{b} \in R/I$ such that $\overline{a}\overline{b} = \overline{0} \implies \overline{ab} = \overline{0} \implies ab \in I$. Why? $ab \in \ker(\pi : R \to R/I) = I$. $I$ is prime implies that $a \in I$ or $b \in I$. Then $\overline{a} = \overline{0}$ or $\overline{b} = \overline{0}$. Hence, $R/I$ is an ID.
Conversely, if $R/I$ is an ID, consider $a, b \in R$ such that $ab \in I \implies \overline{ab} = \overline{0}$ in $R/I$, i.e. $\overline{a}\overline{b} = \overline{0}$. Then $R/I$ is an ID implies that $\overline{a} = \overline{0}$ or $\overline{b} = \overline{0}$, which means that $a \in I$ or $b \in I$. Hence, $I$ is a prime ideal. □

**Question.** When are principal ideals prime/maximal?

**Definition 5.9.3** (Prime)**.** An element $p \in R$ is **prime** if $p$ is not a unit or 0 and if $p \mid ab$, then $p \mid a$ or $p \mid b$.

**Definition 5.9.4** (Irreducible)**.** An element $a \in R$ is **irreducible** if $a$ is not a unit or 0 and if $a = bc$, then one of $b, c$ is a unit, i.e. there is no non-trivial factorization of $a$ where trivial means that $a = u(u^{-1}a)$ where $u$ is a unit).

**Remark.** What we normally call "prime" for integers is actually "irreducible."

**Proposition 5.9.5.** If $R$ is a ring, $I = (a), a \neq 0$ is a unit, then $I$ is a prime ideal $\iff$ $a$ is a prime element.

*Proof.* Consider $b, c \in R$ such that $a \mid bc \implies bc = (a)$. $(a)$ is prime implies that $b \in (a)$ or $c \in (a)$, which means that $a \mid b$ or $a \mid c$, which tells us that $a$ is prime.

Conversely, consider $b, c \in R$ such that $bc \in (a) \implies a \mid bc$. Then $a$ being a prime means that $a \mid b$ or $a \mid c$, which implies that $b \in (a)$ or $c \in (a)$. Then $(a)$ is a prime ideal. □

**Proposition 5.9.6.** If $R$ is an integral domain, $I = (a)$ for some unit $a \neq 0$, then $I$ being maximal $\implies$ $a$ is irreducible.

*Proof.* If $I$ is maximal, $I = (a)$, then let $a = bc$ for some $b, c \in R$. Assume that $b$ is not a unit, we show that $c$ is a unit. $a$ is a multiple of $b \implies a \in (b) \implies (a) \subseteq (b) \implies (a) \subseteq (b) \subseteq R$. $b$ not being a unit $\implies (b) \neq R$. Then $(a)$ being maximal $\implies (a) = (b)$. Hence, $b \in (a)$ and $b = ad$ for some $d \in R$. So $a = bc = adc \implies a - adc = 0 \implies a(1 - dc) = 0$. $R$ begin ID and $a \neq 0 \implies 1 - dc = 0 \implies 1 = dc$, i.e. $c$ is a unit. □

**Remark.** The converse is false. Consider $R = \mathbb{Z}[x]$ and $a = 2$. Then 2 is irreducible in $\mathbb{Z}[x]$. If $2 = fg$, then $f, g$ are both constant and one of them is a unit. But (2) is not maximal as $(2) \subset (2, x) \subset \mathbb{Z}[x]$.

**Exercise 5.9.7.** If all ideals in $R$ are principal, then $a$ being irreducible $\implies (a)$ is maximal.

### 5.9.1 Irreducible and Prime Elements

**Example 5.9.8.** $R = \mathbb{Z}[\sqrt{-5}] \cong \mathbb{Z}[x]/(x^2 + 5) = \{A + B\sqrt{-5} \mid A, B \in \mathbb{Z}\}$. $R$ is an ID since $R \subseteq \mathbb{C}(x^2 + 5) \subseteq \mathbb{Z}[x]$ is a prime ideal, which implies that $x^2 + 5$ is a prime element of $\mathbb{Z}[x]$.

**Claim.** $6 \in R$ is not irreducible.

*Proof.* $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ and $2, 3, 1 \pm \sqrt{-5}$ are irreducible and hence not units. Why? We find all units in $R$: note that $|z|^2 = z\overline{z}$. In $R = \mathbb{Z}[\sqrt{-5}]$, $|a + b\sqrt{-5}|^2 = a^2 + 5b^2 \in \mathbb{Z}$.
Units in $R$: if $a \in R$ is a unit, $\exists b \in R$ such that $ab = 1 \implies |ab|^2 = |1|^2 = 1 \implies |a|^2|b|^2 = 1 \implies |a|^2 = |b|^2 = 1$. Conversely, if $|a|^2 = 1$, then $a \cdot \overline{a} = 1$. If $a = x + y\sqrt{-5}$, then $\overline{a} = x - y\sqrt{-5} \in R \implies a$ is a unit. So $a \in R$ is a unit $\iff |a|^2 = 1$.
In $R = \mathbb{Z}[\sqrt{-5}]$, $|a|^2 = 1 \implies x^2 + 5y^2 = 1$ where $x, y \in \mathbb{Z}$, so $y = 0$ and $x = \pm 1$. So the only units in $R$ are $\pm 1$. □

**Claim.** 2 is irreducible.

*Proof.* If $2 = ab$ for some $a, b \in R$, we want to show that $a$ is a unit or $b$ is a unit. But $2 = ab \iff |2|^2 = |ab|^2 \iff 4 = |a|^2|b|^2 \implies \{|a|^2, |b|^2\} = \{1, 4\}$ or $\{2, 2\}$. For the first case, one of them must be a unit. The second case is impossible since it has no solution for $x, y \in \mathbb{Z}$. Hence, 2 is irreducible. □

**Claim.** 3 is irreducible.

*Proof.* Same proof as above. □

**Claim.** $1 \pm \sqrt{-5}$ are irreducible.

*Proof.* If $1 \pm \sqrt{-5} = ab$, then $6 = |1 \pm \sqrt{-5}|^2 = |a|^2|b|^2$, we know $|a|^2, |b|^2 \neq 2, 3$, so $|a|^2, |b|^2 = 1, 6$ or $6, 1$. Hence, one must be a unit and so $1 \pm \sqrt{-5}$ are irreducible. □

**Claim.** $2, 3, 1 \pm \sqrt{-5}$ are not prime in $R$.

*Proof.* $2 \mid 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ but $2 \nmid 1 \pm \sqrt{5}$. Why? If $1 \pm \sqrt{-5} = 2a$ for some $a \in R$, then $6 = |1 \pm \sqrt{-5}|^2 = |2a|^2 = 4|a|^2$. But $6 = 4|a|^2$ has no solution for $|a|^2 \in \mathbb{Z}$. Similarly, $3 \nmid 1 \pm \sqrt{-5}$, but $3 \mid (1 + \sqrt{-5})(1 - \sqrt{-5}) = 6$. □

**Remark.** Irreducible does not imply prime, even in an integral domain.

**Example 5.9.9.** $R = \mathbb{Z}_4$. $\overline{2}$ is prime. Why? $\overline{2} \mid \overline{0}$ and $\overline{2} \mid \overline{2}$. The only products giving $\overline{2}$ or $\overline{0}$ involve a $\overline{2}$ or $\overline{0}$. But $\overline{2}$ is not irreducible. Why? $\overline{2} = \overline{2} \cdot \overline{4}$ and $\overline{2}, \overline{4}$ are not units or 0.

**Remark.** Prime does not imply irreducible in general.

**Proposition 5.9.10.** In an integral domain, prime $\implies$ irreducible.

*Proof.* If $p \in R$ is prime, and $R$ is an ID, let $p = ab$. Then $p \mid ab$. $p$ being a prime $\implies p \mid a$ or $p \mid b$. WLOG, say $p \mid a$ so $a = px$ for some $x \in Rp = ab = pxb \implies p(1 - xb) = 0$. Since $p \neq 0$, $R$ is an ID $\implies 1 - xb = 0 \implies xb = 1 \implies b$ is a unit. Hence, $p$ is irreducible. □

# Chapter 6

# Factoring

## 6.1 Unique Factorization Domains

### 6.1.1 Euclidean Domains

**Definition 6.1.1** (Size function)**.** Given a ring $R$, a **size function** is a function $\sigma : R\backslash\{0\} \to \mathbb{N}_{\geqslant 0}$.

**Definition 6.1.2** (Euclidean domain)**.** A **Euclidean domain** is an integral domain $R$ with a size function $\sigma$ such that the division algorithm works, i.e. if $a, b \in R, b \neq 0$, then $\exists q, r \in R$ such that $a = bq + r$ and either $r = 0$ or $\sigma(r) < \sigma(b)$.

**Example 6.1.3.** $R = \mathbb{Z}[\sqrt{-5}]$ with $\sigma(x + y\sqrt{-5}) = x^2 + 5y^2$ is NOT a Euclidean domain.

*Proof.* Suppose for contradiction that $(R, \sigma)$ is a ED. Let $a = 1 + \sqrt{-5}, b = 2$. If $1 + \sqrt{-5} = 2q + r$, we know that $2 \nmid 1 + \sqrt{-5}$, so $r \neq 0 \implies \sigma(r) < \sigma(2) = 4$. $\sigma(r) = 2, 3$ are impossible and so $\sigma(r) = 1$, i.e. $r$ is a unit and so $r = \pm 1$. Then $1 + \sqrt{-5} = 2q \pm 1$. But neither $\sqrt{-5}$ nor $2 + \sqrt{-5}$ is divisible by 2: $\sigma(2q) = 4|q|^2$ but $\sigma(\sqrt{-5}) = 5, \sigma(2 + \sqrt{-5}) = 9$ and $4 \nmid 5, 4 \nmid 9$. Hence no such $q$ exists and so $(R, \sigma)$ cannot be a ED. □

### 6.1.2 Principal Ideal Domain

**Definition 6.1.4** (Principal ideal domain)**.** A **principal ideal domain** (PID) is an integral domain in which all ideals are principal.

**Theorem 6.1.5.** A Euclidean domain is a PID.

**Theorem 6.1.6.** In a PID, irreducible $\implies$ prime.

**Corollary 6.1.7.** $\mathbb{Z}[\sqrt{-5}]$ is not a ED with any size function $\sigma$.

**Definition 6.1.8** (Associate)**.** An **associate** of an element $a \in R$ is $b \in R$ such that $b = au$ for some unit $u \in R$. $a \mid b$ and $b \mid a \implies a, b$ are associates.

**Remark.** Not all PIDs are EDs.

### 6.1.3 Unique Factorization Domain

**Definition 6.1.9** (Unique factorization domain)**.** An integral domain $R$ is a **unique factorization domain** if

- every $a \in R$ can be written as a finite product of irreducibles.
- $a_1 a_2 \cdots a_n = b_1 b_2 \cdots b_m$, where each $a_i$ and $b_j$ are irreducible, then $n = m$, and after reordering, $a_i = u_i b_i$ for some unit $u_i \in R$ for each $i = 1, \ldots, n$.

**Example 6.1.10.** $\mathbb{Z}[\sqrt{-5}]$ is NOT a UFD, since $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ and $2 \neq u(1 \pm \sqrt{-5})$ for any unit $u \in R$.

**Theorem 6.1.11.** Every PID $R$ is also a UFD.

**Theorem 6.1.12.** In a UFD, irreducible $\implies$ prime.

### 6.1.4 Types of Rings

$$\text{Fields} \subset \text{EDs} \subset \text{PIDs} \subset \text{UFDs} \subset \text{ID} \subset \text{Ring}.$$

**Example 6.1.13.** $\mathbb{Z}[x]$ is a UFD that's not a PID since $(2, x) \subseteq \mathbb{Z}[x]$ is not principal.

**Example 6.1.14.** $\mathbb{Q}$ is a field, so $\mathbb{Q}[x]$ is a ED, and thus a UFD.

**Example 6.1.15.** $\mathbb{Z}_p$ is a field, so $\mathbb{Z}_p[x]$ is a UFD.

**Definition 6.1.16** (Primitive)**.** $f(x) = \sum_{k=0}^{n} a_k x^k \in \mathbb{Z}[x]$ is **primitive** if

- $\deg f > 0$, i.e. not constant
- $\gcd(a_1, \ldots, a_n) = 1$
- $a_n > 0$

**Remark.** If $\deg f > 0$, $a_n > 0$, then $f$ is primitive $\iff$ $p \nmid f$ for any prime integer $p$ $\iff$ $\Psi_p(f) \neq \overline{0}$ for any prime $p$, where $\Psi_p : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ is defined by $\sum a_k x^k \mapsto \sum \overline{a_k \pmod p} x^k$.

**Proposition 6.1.17.**

(i) $n \in \mathbb{Z}[x]$ is prime in $\mathbb{Z}[x]$ $\iff$ $n \in \mathbb{Z}$ is prime.

(ii) $f, g$ are primitive $\implies$ $fg$ primitive.

**Lemma 6.1.18.** Every non-constant $f \in \mathbb{Q}[x]$ can be written uniquely as $f = c_f f_0$ where $c_f \in \mathbb{Q}$ and $f_0 \in \mathbb{Z}[x] \subseteq \mathbb{Q}[x]$ is primitive.

**Theorem 6.1.19.** If $f, g \in \mathbb{Z}[x] \subseteq \mathbb{Q}[x]$ and $f, g$ have a common non-constant factor in $\mathbb{Q}[x]$, then they have a common non-constant factor in $\mathbb{Z}[x]$.

**Theorem 6.1.20.** $\mathbb{Z}[x]$ is a UFD.

**Remark.** $\mathbb{Z}[x]$ is a UFD, and each $f \in \mathbb{Z}[x], f \neq \pm 1$ can be uniquely written as $f = \pm p_1 p_2 \cdots p_m f_1 f_2 \cdots f_n$, where $p_i \in \mathbb{Z}$ are positive primes and $f_j \in \mathbb{Z}[x]$ are primitives.

**Remark.** Similarly $R$ is a UFD $\implies$ $R[x]$ is a UFD.

**Corollary 6.1.21.** $R[x_1, \ldots, x_n]$ is a UFD.

## 6.2 Factoring in $\mathbb{Z}[x]$

Suppose $f(x) = a_n x^n + \cdots + a_0, a_n \neq 0$. Then we know that $(x - a) \mid f \iff f(a) = 0$, where $a \in \mathbb{Z}$. More generally, $b1_x + b + 0 \mid f \iff f(-b_0/b_1) = 0 \implies b_1 \mid a_n$ and $b_0 \mid a_0$.

**Proposition 6.2.1.** If $f = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x], a_n \neq 0$ and $p$ is a prime such that $p \nmid a_n$. Then $\Psi_p(f)$ is irreducible in $\mathbb{Z}_p[x] \implies f$ is irreducible in $\mathbb{Q}[x]$.

**Fact.** If $\overline{a}, \overline{b} \neq 0$ are not squares in $\mathbb{Z}_p$, then $\overline{ab}$ is a square in $\mathbb{Z}_p$, so if $\overline{2}$ and $\overline{3}$ are not squares in $\mathbb{Z}_p$. then $\overline{6} = \overline{2} \cdot \overline{3}$ is.

## 6.3 Eisenstein Criterion

Here's a rule to check if $f \in \mathbb{Z}[x]$ is irreducible in $\mathbb{Q}[x]$.

**Theorem 6.3.1** (Eisenstein Criterion)**.** If $f = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x], a_n \neq 0$ and $p \in \mathbb{Z}$ is a prime such that

- $p \nmid a_n$
- $p \mid a_0, \ldots, a_{n-1}$
- $p^2 \nmid a_0$,

then $f \in \mathbb{Q}[x]$ is irreducible.

### 6.3.1 Gaussian Primes

**Question.** What are the prime elements of $\mathbb{Z}[i]$

**Answer.** $\mathbb{Z}[i]$ is a Euclidean Domain, so primes = irreducibles.

**Example 6.3.2.** $2 \in \mathbb{Z}$ is prime but $2 = (1 + i)(1 - i) \in \mathbb{Z}[i]$ is not prime.

**Remark.** If $n \in \mathbb{Z}$ is composite, then $\in \mathbb{Z}[i]$ is not prime.

**Lemma 6.3.3.** If $p \in \mathbb{Z}$ is prime, then $p \in \mathbb{Z}[i]$ is prime $\iff$ $x^2 + \overline{1}$ is irreducible in $\mathbb{Z}_p[x]$ $\iff$ $\overline{-1}$ is not a square mod $p$.

### 6.3.2 Non-integer Primes

- $a + bi$ prime $\iff$ $\pm(a + bi), \pm i(a + bi)$ prime, so $\pm p, \pm pi$ are prime $\iff$ $p \equiv 3 \pmod 4$ for prime $p$.
- $a + bi \in \mathbb{Z}[i]$ $\iff$ $a - bi \in \mathbb{Z}[i]$ prime.
- $a + bi \in \mathbb{Z}[i]$ prime $\iff$ $a^2 + b^2 \in \mathbb{Z}$ is a prime integer.

# Chapter 7

# Fields

**Definition 7.0.1** (Field)**.** A **field** is a ring in which all non-zero elements are units.

**Definition 7.0.2** (Field extension)**.** If $F \subseteq K$, and $F, K$ are fields, then $K$ is **field extension** of $F$, denoted by $K/F$.

**Definition 7.0.3** (Finite field)**.** If $|F| < \infty$, then $F$ is a **finite field**.

**Example 7.0.4.** $\mathbb{Z}_p$ is a finite field where $p$ is prime.

**Example 7.0.5.** $F \subseteq F(x) = \{\frac{f(x)}{g(x)} \mid f, gF[x], g \neq 0\}/\sim$ is called a **functions field**.

**Definition 7.0.6** (Algebraic/Transcendental)**.** If $K/F$ is a field extension, and $\alpha \in K$, then $\alpha$ is **algebraic** over $F$ if $\alpha$ is the root of a polynomial in $F[x]$. Otherwise, it's **transcendental** over $F$.

**Example 7.0.7.** $\frac{1}{2}, \sqrt{2}, \sqrt{3}, i$ are algebraic over $\mathbb{Q}$ since they are roots to $x - \frac{1}{2}, x^2 - 2, x^2 - 3, x^2 + 1$.

**Example 7.0.8.** $\pi$ is transcendental over $\mathbb{Q}$ but is algebraic over $\mathbb{R}$.

Another way to think about algebraic/transcendental is to consider the *evaluation map* $\varphi_\alpha : F[x] \to K$ defined by $f(x) \mapsto f(\alpha)$. $\alpha \in K$ is algebraic over $F \iff \varphi_\alpha$ is NOT injective.

**Remark.** Image of $\varphi_\alpha$i s $F[\alpha]$, which is the ring of polynomials in $\alpha$ with coefficients in $F$.

**Remark.** If $\alpha$ is transcendental over $F$, then $\varphi_\alpha$ is injective, so $F[x] \cong \mathrm{im}(\varphi_\alpha) = F[\alpha]$.

**Definition 7.0.9** (Irreducible polynomial)**.** If $K/F$ is a field extension, and $\alpha \in K$ is algebraic over $F$, then the unique monic irreducible polynomial $f \in F[x]$ with $f(\alpha) = 0$ is called the **irreducible polynomial** of $\alpha$ over $F$.

Equivalence of "$f$ is irreducible":

- $(f)$ is a maximal ideal in $F[x]$.
- $f$ has minimal degree over all polynomials $g$ with $g(\alpha) = 0$.

**Definition 7.0.10** (Degree)**.** The **degree** of $\alpha$ over $F$ is the degree of its irreducible polynomial.

**Example 7.0.11.** $\deg \sqrt{2}$ over $\mathbb{Q}$ is 2.

**Example 7.0.12.** $\alpha = \sqrt{i}$ has degree 4 over $\mathbb{Q}$ $(x^4 + 1)$, but degree 2 over $\mathbb{Q}[i]$ $(x^2 - i)$.

**Example 7.0.13.** $\deg \alpha = 1$ over $F \iff \alpha \in F$ since $\deg \alpha = 1 \iff x - a \in F[x]$ has $\alpha$ as a root for some $a \in F \iff \alpha \in F$.

**Definition 7.0.14** (Adjoin)**.** $F(\alpha)$ is the smallest *subfield* of $K$ containing $F$ and $\alpha$. We call it $F$ **adjoin** $\alpha$.

**Remark.** $F(\alpha)$ is the field of fractions of $F[\alpha]$.

**Theorem 7.0.15.** If $K/F$ is a field extension, $\alpha \in K$ is algebraic over $F$ with minimal polynomial $f \in F[x]$, then $F[x]/(f) \cong F[\alpha]$, and hence $F[\alpha] = F(\alpha)$ is a field.

Recall that

**Theorem 7.0.16.** If $\alpha$ is algebraic over $F$, $f$ is the minimal polynomial of $\alpha$ over $F$ with $\deg f = n$, then $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ is a basis for $F(\alpha)$ as a vector space over $F$, i.e. $F(\alpha) = \{A_0 + A_1\alpha + \cdots + A_{n-1}\alpha^{n-1} \mid A_i \in F, i = 0, \dots, n-1\}$.

**Remark.** If $|F| < \infty$, then $|F(\alpha)| = |F|^n$, since there are $|F|$ choices for each coefficients $A_i$.

**Proposition 7.0.17.** If $F$ is a field, $K/F$ and $L/F$ are field extensions, $\alpha \in K, \beta \in L$ are both algebraic over $F$, then there exists isomorphism $\varphi : F(\alpha) \to F(\beta)$ such that $\varphi(\alpha) = \beta$ and $\varphi(a) = a$ for all $a \in F \iff$ the minimal polynomials of $\alpha, \beta$ over $F$ are equal.

**Definition 7.0.18** (Isomorphic extensions)**.** If $F$ is a field, $K/F, L/F$ are two extensions, then they are **isomorphic extensions** if $\exists$ isomorphism $\varphi : K \to L$ such that $\varphi(a) = \alpha$ for all $a \in F$. We call $\varphi$ a $F$-isomorphism.

## 7.1 Degrees of Field Extensions

**Definition 7.1.1.** The dimension of $V$ over $F$ is $\dim_F V = |S|$, where $S$ is any basis.

**Definition 7.1.2** (Degree)**.** The **degree** of a field extension $K/F$ is the dimension of $K$ as a vector space over $F$, i.e. $\dim_F K$, denoted by $[K : F]$.

**Example 7.1.3.** $F = \mathbb{Q}, K = \mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}]$. The basis for $K$ over $F$ is $\{1, \sqrt{2}\}$ (since $K = F[x]/(x^2 - 2)$, $\deg x^2 - 2 = 2) \implies [(\sqrt{2}) : \mathbb{Q}] = 2$.

**Fact.** If $F$ is any field, $K = F[x]/(f)$, where $f$ is irreducible, $\deg f = n$, then $[K : F] = n$.

**Proposition 7.1.4.** $[K : F] = 1 \iff K = F$.

**Proposition 7.1.5.** If $\mathrm{char} F \neq 2$, and $K/F$ is a field extension, then $[K : F] = 2 \iff K = F(\delta)$, where $\delta^2 = d \in F$, and $d$ has no square root in $F$.

**Theorem 7.1.6.** If $\alpha$ is algebraic over $F$, then $[F(\alpha) : F] < \infty$. If $\alpha$ is transcendental over $F$, the $[F(\alpha) : F] = \infty$,

**Theorem 7.1.7** (Tower Law)**.** If $F \in K \subseteq L$ are fields, then $[L : F] = [L : K] \cdot [K : F]$

**Corollary 7.1.8.** If $K/F$ is a field extension, and $\alpha \in K$ and $[K : F] = n$, then $[F(\alpha) : F] \leqslant n$.

### 7.1.1 Algebraic Extensions

**Definition 7.1.9** (Algebraic)**.** A field extension $K/F$ is algebraic over $F$ if every element $\alpha \in K$ is algebraic over $F$.

## 7.2 Straightedge and Compass Constructions

**Definition 7.2.1** (Constructible)**.** A point $\alpha \in \mathbb{C}$ is **constructible** if it can be constructed with straightedge and compass constructions in a finite number of steps.

**Example 7.2.2.** $-1 \in \mathbb{C}$ is constructible.

**Theorem 7.2.3.** The set of constructible numbers forms a subfield of $\mathbb{C}$.

**Corollary 7.2.4.** The field of constructible numbers is closed under taking $\sqrt{}$, i.e., if $\alpha \in$ field, then so is $\sqrt{\alpha}$.

**Theorem 7.2.5.** If $\alpha \in \mathbb{C}$ is constructible, then $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^k$ for some $k \geqslant 0$.

**Remark.** The converse is not true.

**Corollary 7.2.6.** $\sqrt[3]{2}$ is NOT constructible.

**Corollary 7.2.7.** It is not possible to double the cube via straightedge and compass, i.e., given a cube of volume $V$, it is not possible to construct a cube of volume $2V$.

**Corollary 7.2.8.** There is no trisection algorithm with straightedge and compass.

**Remark.** But bisection of angles is possible.

**Theorem 7.2.9.** $\alpha \in \mathbb{C}$ is constructible $\iff \exists$ sequence of extensions $\mathbb{Q} = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n$ such that $\alpha \in F_n$ and $[F_i : F_{i-1}] = 2$ for $i = 1, \ldots, n$.

**Theorem 7.2.10.** $\alpha \in \mathbb{C}$ is constructible $\iff [K : \mathbb{Q}] = 2^m$ for some $m$ where $K = \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n)$, and $\alpha_1, \ldots, \alpha_n$ are the roots of the minal polynomial of $\alpha$ over $\mathbb{Q}$.

**Theorem 7.2.11** (Guass-Wantzel)**.** A regular $n$-gon is constructible $\iff n = 2^k p_1 p_2 \cdots p_n \geqslant 3$ where $k \geqslant 0$ and $p_i$ are distinct Fermat primes ($p_i = 2^{2^m} + 1$, for some $m$ and prime).

Let $\delta_n = e^{i2\pi/n}$ ($n$th root of unity).

**Lemma 7.2.12.** If $p$ prime, $[\mathbb{Q}(\delta_{p^a}) : \mathbb{Q}] = p^{a-1}(p-1)$.

**Lemma 7.2.13.** $\delta_{p^a}$ is constructible $\iff p = 2, a \geqslant 2$, or $p = 2^{2^m} + 1$, $a = 1$.

## 7.3 Finite Fields

Let $p$ be a prime, $q = p^k, k \geqslant 1$. Then a field of order $q$ is $\mathbb{F}_q = \mathbb{Z}_p[x]/(f)$, where $f \in \mathbb{Z}_p[x]$ is an irreducible polynomial of degree $k$. Since the quotient ring has basis $\left\{1, \alpha, \ldots, \alpha^{k-1}\right\}$ over $\mathbb{Z}_p$ (where $\alpha = \overline{x}$ is a root of $f$), the quotient ring is $\left\{A_0 + A_1 x + \cdots + A_{k-1}\alpha^{k-1} \mid A_i \in \mathbb{Z}_p\right\}$. Hence, $|\mathbb{F}_q| = p^k = q$.

**Example 7.3.1.** $\mathbb{F}_{25} = \mathbb{Z}_5[x]/(x^2 - \overline{3})$.

**Definition 7.3.2** (Splitting fields)**.** If $f \in F[x]$ and $K/F$ is a field extension, then $f$ **splits** completely in $K$ if $f \in K[x]$ factors into a product of linear polynomials of degree 1.

**Theorem 7.3.3.** If $F$ is a field, $f \in F[x]$ is a monic polynomial ,deg $f > 0$, then $\exists$ field extension $K/F$ in which $f$ splits completely.

**Theorem 7.3.4.** Let $p$ be prime, $q = p^n, n \geqslant 1$.

(i) If $K$ is a field of order $q$, then $x^q - x \in K[x]$ splits completely in $K$, with $q$ distinct roots.

(ii) If $|K| = q$, then the multiplicative group $K\backslash\{0\}$ is cyclic, i.e. $\cong (\mathbb{Z}_{q-1}, +)$.

(iii) $\exists$ field $K$ or order $q$ and all such fields are isomorphic.

(iv) A field of order $q$ contains a subfield of order $p^m \iff m \mid n$.

(v) The irreducible factors of $x^q - x \in \mathbb{Z}_p[x]$ are all the irreducible polynomials in $\mathbb{Z}_p[x]$ whose degree divides $n$.

**Remark.** If $|K| = q = p^n$, we can assume $K = \mathbb{Z}_p[x]/(f)$ and $f$ has degree $n$ and is irreducible.

**Lemma 7.3.5.** $f \in F[x]$ has a multiple root at $\alpha \iff f(\alpha) = 0$ and $f'(\alpha) = 0$.

## 7.4 Simple and Separable Extensions

**Definition 7.4.1** (Simple extension)**.** If $F$ is a field, $K/F$ a field extension, then $K$ is a simple extension of $F$ if $\exists \alpha \in K$ such that $K = F(\alpha)$.

**Example 7.4.2.** $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, $F = \mathbb{Q}$. Then $K$ is simple as $K = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

**Question.** How to check if $K/F$ is simple?

**Answer.** Via separable extension.

**Definition 7.4.3** (Separable)**.** A polynomial $f \in F[x]$ is **separable** if it has distinct roots in any field in which it splits completely.

**Example 7.4.4.** $x^2 - \overline{2} \in \mathbb{Z}_3[x]$ is irreducible as it has no root in $\mathbb{Z}_3$ and $(x^2 - \overline{2})' = 2x \neq \overline{0}$, so its separable.

**Example 7.4.5.** $x^2 - t \in (\mathbb{Z}_2(t))[x]$ is irreducible as $t$ has no square root in $\mathbb{Z}_2(t)$. But $(x^2 - t)' = \overline{2}x = \overline{0}$ as $\overline{2} = \overline{0}$ in $\mathbb{Z}_2$. So $x^2 - t$ is not separable.

In general $f \in F[x]$ is NOT separable $\iff$ $\mathrm{char}F = p > 0$ and $f = g(x^p)$ for some $g \in F[x]$.

**Definition 7.4.6** (Separable extension)**.** An algebraic field extension $K/F$ is a **separable extension** if $\forall \alpha \in K$, the minimal polynomial of $\alpha$ over $F$ is separable.

**Example 7.4.7.** If $\mathrm{char}F = 0$, then all algebraic $K/F$ are separable.

**Theorem 7.4.8.** If $K/F$ is a finite-degree separable field extension, and $|F| = \infty$, then $K$ is a simple extension, i.e. $\alpha \in K$ such taht $K = F(\alpha)$. $\alpha$ is primitive.

**Corollary 7.4.9.** If $F = \mathbb{Q}$, $[K : F] < \infty$, then $K$ is a simple extension of $\mathbb{Q}$.

**Theorem 7.4.10.** If $K/F$ is a finite-degree extension, then $K$ is a simple extension of $F$ $\iff$ there are finitely many fields $L$ with $FL \subseteq K$.