Louis Meunier

Algebra I MATH235

Course Outline:

Introductory abstract algebra. Sets, functions, relations. Methods of proof. Arithmetic on integers. Fields, rings; groups, subgroups, cosets.

Texts:

Abstract Algebra, *Hungerford;* Algebra, *Artin.*

Based on Lectures from Fall, '23 by Prof. Eyal Goren.

Contents

1 Sets

1.1 Definition

A **set** can be considered as a collection of elements; more intuitively, you can consider something a set if you can determine whether a given object belongs to it. Typically sets are defined as $A = \{1, 2, \dots\}$, by a property $A = \{x \mid x\%2 = 0\}$, or with an appropriate verbal description.

1.2 Set operations

There are a number of ways to "combine" sets:

- **Union**: $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$
- **Intersection**: $A \cap B = \{x \mid x \in A \text{ and } x \in B\}$
- **Difference**: $A \setminus B = \{x \mid x \in A \text{ and } x \notin B\}$

↪ **Lemma 1.1**

$A = (A \setminus B) \cup (A \cap B)$

Proof. To prove set equivalencies, we must prove that both RHS ⊆ LHS and LHS ⊆ RHS; meaning, the LHS and RHS are subsets of each other, and are thus equal.

First, to prove LHS ⊆ RHS, let $a \in A$. If $a \notin B$, then $a \in A \setminus B$, and $a \in$ RHS. Else, if $a \in B$, then $a \in A \cap B$ and $a \in$ RHS. Thus, LHS ⊆ RHS.

Next, to prove RHS ⊆ LHS, let $a \in$ RHS. If $a \in A \setminus B$, then $a \in A =$ LHS. Else, $a \in A \cap B$, and thus $a \in A =$ LHS. Thus, RHS ⊆ LHS. Since LHS ⊆ RHS and RHS ⊆ LHS, LHS = RHS. ■

1.3 Indexed sets

Let I be a set. If for every $i \in I$, we have a set B_i, we say that we have a *collection* of sets B_i indexed by I. We write $\{B_i : i \in I\}$.

⊛ **Example 1.1**

Let $I = \{1, 2, 3\}$, and $B_i = \{1, 2, 3, 4\} \setminus \{i\}$ (B_i is the set of all numbers from 1 to 4, excluding i), for $i \in I$. We thus have $B_1 = \{2, 3, 4\}$ (etc.).

This concept of indexing allows us to introduce repeated unions/intersections. For instance, we can write

$$\bigcup_{i \in I} B_i = B_1 \cup B_2 \cup B_3 = \{1, 2, 3, 4\}.$$

Similarly,

$$\bigcap_{i \in I} B_i = \{4\}.$$ [1]

[1] You can somewhat consider these "large" unions/intersections as analogous to summations Σ and products Π.

⊛ **Example 1.2**

Let $I = \mathbb{R}$, and $B_i = [i, \infty] = \{r \in \mathbb{R} : r \geq i\}$. Then, $\bigcup_{i \in \mathbb{R}} B_i = \mathbb{R}$ and $\bigcap_{i \in \mathbb{R}} B_i = \emptyset$.

1.4 Cartesian product

Let $A_1, A_2, \ldots, A_n$ be sets. We define the **Cartesian product**

$$A_1 \times A_2 \times \cdots \times A_n = \{(x_1, x_2, \ldots, x_n) : x_i \in A_i, \text{ for } 1 \leq i \leq n\}.$$

For instance,

$$A \times B = \{(a, b) : a \in A, b \in B\}.$$

⊛ **Example 1.3**

Let $A = B = \mathbb{R}$. $A \times B = \{(x, y) : x \in \mathbb{R}, y \in \mathbb{R}\} = \mathbb{R}^2$ is the set of all points in the Cartesian plane.

We can also define Cartesian products over an index set. Let I be an index set, with A_i for all $i \in I$. Then, we can write

$$\prod_{i \in I} A_i = \{(a_i)_{i \in I} : a_i \in A_i\}$$

⊛ **Example 1.4**

$$I = \mathbb{N}, A_0 = \{0, 1, 2, \ldots\}, A_1 = \{1, 2, 3, \ldots\}, \ldots, A_i = \{i, i+1, i+2, \ldots\}$$
$$Y := \prod_{i \in I} A_i = \{(a_0, a_1, a_2, \ldots) : a_i \in \mathbb{N}, a_i \geq i\}$$

We can say that a particular vector $(b_0, b_1, \ldots) \in Y$ if for each b_i, $b_i \geq i$ (and $b_i \in \mathbb{N}$, of course). In other words, a particular item of the vector must be greater than or equal to its index. Thus, we can say

$$(0, 1, 2, 3, \dots) \in Y$$

while

$$(2, 2, 2, 2, \dots) \notin Y$$

since $a_3 = 2 \implies i = 3$, and $2 \not\geq 3$.

2 Methods of Proof

2.1 Proving equality via two inequalities

In short, say $x, y \in \mathbb{R}$. $x = y \iff x \leq y$ and $y \leq x$. Similarly, in the context of sets, we can say that, for two sets X, Y, $X = Y \iff X \subseteq Y$ and $Y \subseteq X$.

2.2 Contradiction (bwoc)

Given a statement P, we can prove P true by assuming P false ($\equiv \neg P$), then arriving to a contradiction (this contradiction is often a violated axiom or basic rule of the system at hand.)

⊛ **Example 2.1**

Show that there are no solutions to $x^2 - y^2 = 1$ in the positive integers.

Proof (bwoc). Assume there are, so $x, y \in \mathbb{Z}_+$.[2] We can then write

$$1 = x^2 - y^2 = (x - y)(x + y).$$

$x - y$ and $x + y$ must be integers, and so we have two cases, $\begin{cases} x - y = 1 \\ x + y = 1 \end{cases}$ and $\begin{cases} x - y = -1 \\ x + y = -1 \end{cases}$. In either case, y must be zero, contradicting our initial assumption and thus proving the statement. ■

[2] $\mathbb{Z}_+$ is used to denote positive integers; similarly, $\mathbb{Z}_-$ denotes negative integers.

2.3 Proving the contrapositive

Logically, $A \implies B \iff \neg B \implies \neg A$.[3]

[3] "I am hungry therefore I will eat" $\iff$ "I will *not* eat therefore I am *not* hungry." Notice too that B need not imply A ("I will eat therefore I am hungry"). If $A \implies B \iff B \implies A$, $A = B$

⊛ **Example 2.2**

Let X, Y be sets. Prove $X = X \setminus Y \implies X \cap Y = \emptyset$.

Proof. Prove contrapositive: $X \cap Y \neq \emptyset \implies X \neq X \setminus Y$. $X \cap Y \neq \emptyset \implies \exists t \in X \cap Y \implies t \in X$ and $t \in Y$, thus $t \notin X \setminus Y$, but $t \in X$, so $X \neq X \setminus Y$. ■

2.4 Induction

↪ **Axiom 2.1: Well-Ordering Principle**

Every $S \subseteq \mathbb{N}$, where $S \neq \emptyset$, has a minimal element, ie $\exists a \in S$ s.t. $\forall b \in S, a \leq b$.

↪ **Theorem 2.1: Principle of Induction**

Let $n_0 \in \mathbb{N}$. Say that for every $n \in \mathbb{Z}, n \geq n_0$, we are given a statement P_n. Assume

(a) P_{n_0} is true

(b) if P_n is true, then P_{n+1} is true

then P_n is true for all $n \geq n_0$.

Proof (bwoc). Assume not.[4] Then, we define $S = \{n \in \mathbb{N} : n \geq n_0, P_n \text{ false}\}$. By the Well-Ordering Principle, there exists a minimal element $a \in S$. By definition, $a \geq n_0$, and as P_{n_0} is taken to be true, then $a > n_0$ since $n_0 \notin S$. Thus, $a - 1 \notin S$, as a is the minimal element of S, and therefore P_{a-1} is true. However, by (b), this implies P_a is also true, and thus $a \notin P$, contradicting our initial assumption. ■

[4] note that (a) and (b) of the Principle of Induction are still taken to be true; it is simply the conclusion that is assumed to be false.

2.5 Pigeonhole principle

↪ **Axiom 2.2**

If there are more pigeons than pigeonholes, then at least one pigeonhole must contain more than one pigeon.[5]

[5] Alternatively, you can consider fractional pigeons (though a little gruesome); given $n+1$ pigeons and n holes, each hole will contain, on average, $1 + \frac{1}{n}$ pigeons.

⊛ **Example 2.3**

Consider $n_1, \ldots, n_6 \in \mathbb{N}$. There exist at least two of these n's s.t. $n_i - n_j$ is evenly divisible by 5.

Proof. Let us rewrite each n_i as $n_i = 5k_i + r_i$, where $k_i, r_i \in \mathbb{N}$, k_i is the quotient, and r_i is the residual. $r_i \in \{0, 1, 2, 3, 4\}$ (the only possible remainders when a number is divided by 5), and so there are 5 possible values of r_i, but 6 different n_i. Thus, two n_i

must have the same r_i, and we can write:

$$\begin{aligned} n_i = 5k_i + r; n_j = 5k_j + r \\ n_i - n_j &= (5k_i + r) - (5k_j + r) \\ &= 5(k_i - k_j) \end{aligned}$$

$(k_i - k_j) \in \mathbb{Z}$, and so $n_i - n_j$ is evenly divisible by 5. ■

3 Functions

3.1 Types of Functions

↪ **Definition 3.1: Function**

Given 2 sets A, B, a *function* $f : A \to B$ is a rule such that $\forall a \in A, \exists! f(a) \in B$, where $\exists!$ denotes “there exists a unique”.

↪ **Definition 3.2: Graph**

Given a function $f : A \to B$, a *graph* $\Gamma_f = \{(a, f(a)) : a \in A\} \subseteq A \times B$. We can say that, $\forall a \in A$, $\exists! b \in B$ such that $(a, b) \in \Gamma_f$.

⊛ **Example 3.1**

Consider the Cartesian plane, denoted $\mathbb{R}^2$. It is simply a graph Γ_f where $f : \mathbb{R} \to \mathbb{R}$ is the identity function, $f(x) = x$.

↪ **Definition 3.3: Injective**

A function is an *injection* iff $\forall a_1, a_2 \in A, f(a_1) = f(a_2) \implies a_1 = a_2$.

↪ **Definition 3.4: Surjective**

A function is a *surjection* iff $\forall b \in B, \exists a \in A$ such that $f(a) = b$. In other words, every element of B is mapped to by at least one element of A; you can pick any element in the range and it will have a preimage.

↪ **Definition 3.5: Bijective**

Both.

↪ **Definition 3.6: Fibre**

The fibre of some $y \in Y$ is $f^{-1}(y) = f^{-1}(y)$

3.2 Cardinality

↪ **Definition 3.7: Cardinality**

The *cardinality* of a set A, denoted $|A|$, is the number of elements in A, if A is finite, or a more abstract notion of size if A is infinite.

We say that two sets A, B have the same cardinality ($|A| = |B|$) if $\exists$ a bijection $f : A \to B$.[6] This necessitates the question, however: if two sets are not equal in cardinality, how do we compare their sizes?

[6] Consider this in the finite case: a bijection indicates that all elements in the domain map uniquely to a single element in the range, and the range is completely "covered" sts by the function.

We write

$$|A| \leq |B| \impliedby \exists f : A \to B \text{ where } f \text{ is } \textit{injective}$$

and

$$|A| \geq |B| \impliedby \exists f : A \to B \text{ where } f \text{ is } \textit{surjective.}$$ [7]

Note that $|B| \leq |A|$ if either $A = \varnothing$ or, as above, $\exists f : B \to A$ surjective.

[7] Consider this intuitively; if your domain is smaller than your range, then you will "run out" of things to map from the domain to the range before you "run out" of things in the range, hence, you have a injection. Similarly, if your domain is larger than your range, then you will have "leftover" elements in the domain (that will map to "already mapped to" elements in the range), hence, you have a surjection.

↪ **Definition 3.8: Composition**

Given two functions $f : A \to B$, $g : B \to C$, the *composition* is the function $g \circ f : A \to C$

↪ **Proposition 3.1**

If $|A| = |B|$ and $|B| = |C|$ then $|A| = |C|$

Proof. $\exists f : A \to B$ bijective, and $\exists g : B \to C$ bijective. We desire to show that $\exists h : A \to C$ that is bijective. We can write $h = g \circ f$, where $h(a) = g(f(a))$.

To show that h bijective:

- **injective:** Suppose $h(a_1) = h(a_2)$, then $g(f(a_1)) = g(f(a_2))$, and since g is injective, $f(a_1) = f(a_2)$. Since f is injective, $a_1 = a_2$, and thus h is injective.
- **surjective:** Let $c \in C$. Since g is surjective, $\exists b \in B$ such that $g(b) = c$. Since f is surjective, $\exists a \in A$ such that $f(a) = b$. Thus, $h(a) = g(f(a)) = g(b) = c$, and thus h is surjective.

Thus, h is bijective, and $|A| = |C|$. ■

↪ **Lemma 3.1**

If $g \circ f$ injective, f injective. If $g \circ f$ surjective, g surjective.

↪ **Definition 3.9: Image**

The *image* of a function $f : A \to B$ is the set $\mathrm{Im}(f) = \{f(a) : a \in A\}$, ie the set of all elements in B that are mapped to by f. Note that $\mathrm{Im}(f) \subseteq B$, and $\mathrm{Im}(f) = B$ if f is surjective.

↪ **Proposition 3.2**

$|A| \leq |B|$if $|B| \geq |A|$

Proof. If $A = \varnothing$, $|B| \geq |A|$ clearly.

If $A \neq \varnothing$, we are given $\exists f : A \to B$ injective. Let us choose some $a_0 \in A$. We define $g : B \to A$ as

$$g(b) = \begin{cases} a_0 & b \notin \mathrm{Im}(f) \\ a & b = f(a) \in \mathrm{Im}(f)^{8} \end{cases}$$

Note that $g(f(a)) = g(b) = a$, so g is surjective. Thus, $|B| \geq |A|$. ■

[8]Note that a is unique in A, as f is injective.

↪ **Proposition 3.3**

$|B| \geq |A|$ if $|A| \leq |B|$

↪ **Theorem 3.1: Cantor-Bernstein Theorem**

$|A| \leq |B|$ and $|B| \leq |A| \implies |A| = |B|$. [9]

Equivalently, if $\exists f : A \to B$ injective and $\exists g : B \to A$ injective, then $\exists h : A \to B$ bijective.

[9]It is often very difficult to define an arbitrary bijective function between two sets in order to prove their cardinality is equal. The Cantor-Bernstein Theorem allows us to prove that two sets have the same cardinality by proving that there exists an injection from A to B and an injection from B to A, which is typically far easier.

↪ **Proposition 3.4**

If $|A_1| = |A_2|$ and $|B_1| = |B_2|$ then $|A_1 \times B_1| = |A_2 \times B_2|$.

Proof. The first two statements define bijections $f : A_1 \to A_2$ and $g : B_1 \to B_2$, and we desire to have $f \times g : A_1 \times B_1 \to A_2 \times B_2$. We define $f \times g(a_1, b_1) := (f(a_1), g(b_1))$. We must show that $f \times g$ is bijective. ■

⊛ **Example 3.2**

Consider A as the set of all points in the unit circle centered at $(0,0)$ in $\mathbb{R}^2$, and B as the set of all points in the square of side length 2 centered at $(0,0)$ in $\mathbb{R}^2$ (ie, the circle is inscribed in the square). We wish to prove that $|A| = |B|$.

Proof. Let $f : A \to B$, $f(x) = x$. f is injective, and thus $|A| \leq |B|$. Let $g : A \to B$, $g(x) = \begin{cases} 0; \sqrt{2}x \notin B \\ \sqrt{2}x; \sqrt{2}x \in B \end{cases}$. In simpler terms, consider this as multiplying points of A by $\sqrt{2}$; any point in this new "expanded" circle that lies within B maps to itself, and any that lies outside maps to 0. This is thus a surjection, and thus $|B| \leq |A|$. By the Cantor-Bernstein Theorem, $|A| = |B|$. ∎

↪ **Proposition 3.5**

$A = \{0, 1, 4, 9, \ldots\}$. $|A| = |\mathbb{N}|$.

Proof. Define $f : \mathbb{N} \to A$, $f(n) = n^2$. This is clearly injective [10], and thus $|A| \leq |\mathbb{N}|$. ∎

[10] Notice that f is only injective if we restrict the domain to $\mathbb{N}$; if we were to consider $\mathbb{Z}$, for instance, $f(-1) = f(1) = 1$.

↪ **Definition 3.10: Countable/enumerable**

A set A is *countable* if $|A| = |\mathbb{N}|$, or A is finite.

If A is finite of size n, $\exists$ a bijection $f : \{0, 1, 2, \ldots, n-1\} \to A$.

If A is infinite, $\exists$ a bijection $f : \mathbb{N} \to A$.

↪ **Proposition 3.6**

$|\mathbb{N}| = |\mathbb{Z}|$

Proof. We aim to find a bijection $f : \mathbb{Z} \to \mathbb{N}$, ie one that maps integers to natural numbers. Consider the function

$$f(x) = \begin{cases} 2x & x \geq 0 \\ -2x - 1 & x < 0 \end{cases}.$$

This function is an injection because if $f(x_1) = f(x_2)$, then $x_1 = x_2$ (positive case: $2x_1 = 2x_2 \implies x_1 = x_2$, negative case: $-2x_1 - 1 = -2x_2 - 1 \implies x_1 = x_2$, and $2x_1 \neq -2x_2 - 1$ for any integer). It is also a surjection (there is no natural number that cannot be mapped to by an integer). Thus, the function is a bijection and $|\mathbb{N}| = |\mathbb{Z}|$. [11] ∎

[11] Note what would happen if f was defined as $-2x$ for $x < 0$; then, f would not be surjective (eg, $f(-1) = 2 = f(1)$.)

↪ **Proposition 3.7**

$|\mathbb{N}| = |\mathbb{N} \times \mathbb{N}|$

Remark 3.1. *It is possible to construct a bijective $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$; see assignment 1.*

Proof. Let $f : \mathbb{N} \to \mathbb{N} \times \mathbb{N}, f(n) = (n, 0)$, clearly an injection ($\implies |\mathbb{N}| \leq |\mathbb{N} \times \mathbb{N}|$)[12]. The function $g(m, n) = 2^n 3^m$ is also injective, and thus $|\mathbb{N}| = |\mathbb{N} \times \mathbb{N}|$. ■

[12] Note that this function is *not* surjective!

↪ **Corollary 3.1**

$|\mathbb{Z}| = |\mathbb{Z} \times \mathbb{Z}|$

Proof. Consider $h : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$, a bijection[13], and $f : \mathbb{N} \to \mathbb{Z}$. Let $g = (f, f) : \mathbb{N} \times \mathbb{N} \to \mathbb{Z} \times \mathbb{Z}$. The composition $g \circ h \circ f^{-1} : \mathbb{Z} \to \mathbb{N} \to \mathbb{N} \times \mathbb{N} \to \mathbb{Z} \times \mathbb{Z}$ is also a bijection, and thus $|\mathbb{Z}| = |\mathbb{Z} \times \mathbb{Z}|$. ■

[13] Which must exist by the proof of the previous proposition.

⊛ **Example 3.3**

Show that $|\mathbb{N}| = |\mathbb{Q}|$.

Proof. First, we find an injection $\mathbb{Q} \to \mathbb{N}$. Let $f : \mathbb{Q} \to \mathbb{Z} \times \mathbb{Z}, f(n) = (p, q)$ where $\frac{p}{q} = n$ (by definition of $\mathbb{Q}$). Using the same function definitions as in corollary 3.1, the composition $h^{-1} \circ g^{-1} \circ f : \mathbb{Q} \to \mathbb{Z} \times \mathbb{Z} \to \mathbb{N} \times \mathbb{N} \to \mathbb{N}$. This is a composition of injections, and is thus an injection itself, and thus $|\mathbb{Q}| \leq |\mathbb{N}|$. The identity function $1 : \mathbb{N} \to \mathbb{Q}, 1(n) = n$ is clearly an injection as well as all naturals are rationals, and thus $|\mathbb{N}| \leq |\mathbb{Q}|$. By the Cantor-Bernstein Theorem, $|\mathbb{N}| = |\mathbb{Q}|$. ■

↪ **Definition 3.11**

We say $|A| < |B|$ if $|A| \leq |B|$ but $|A| \neq |B|$, ie $\exists f : A \to B$ is injective, but no such bijective.

Remark 3.2. *We denote an injective function as $\mathbb{N} \hookrightarrow \mathbb{Z}$, and a surjective function as $\mathbb{Z} \twoheadrightarrow \mathbb{N}$. We say that a particular element n maps to some other element n' by $n \mapsto n'$*

↪ **Theorem 3.2: Cantor**

$|\mathbb{N}| < |\mathbb{R}|$

Proof (Cantor's Diagonal Argument). We clearly have an injection $\mathbb{N} \hookrightarrow \mathbb{R}, n \mapsto n$, thus $|\mathbb{N}| \leq |\mathbb{R}|$.

Now, suppose $|\mathbb{N}| = |\mathbb{R}|$. Then, we can enumerate the real numbers as $a_0, a_1, \ldots$ with signs ϵ_i. We denote the decimal expansion of each number as[14]

$$\begin{aligned} a_0 &= \epsilon_0 0.a_{00}a_{01}a_{02}\ldots \\ a_1 &= \epsilon_1 0.a_{10}a_{11}a_{12}\ldots \\ a_2 &= \epsilon_2 0.a_{20}a_{21}a_{22}\ldots \\ &\vdots \end{aligned}$$

Consider the number $0.e_0e_1e_2\ldots$, where $e_i = \begin{cases} 3 & a_{ii} \neq 3 \\ 4 & a_{ii} = 3 \end{cases}$. This number is different than any given a_i at the $i+1$-th decimal place, and is thus not in the enumeration, contradicting our initial assumption. ■

[14] We make the clarification that, despite the fact that $1.000\cdots = 0.999\ldots$, we will take the "infinite zeroes" interpretation, and thus every real number has a unique decimal expansion. This is an important, if subtle, distinction.

Remark 3.3 (Continuum Hypothesis). *Cantor claimed that there's no set $|A|$ such that $|\mathbb{N}| < |A| < |\mathbb{R}|$. It has been proven today that this is "undecidable".*

↪ **Definition 3.12: Algebra on Cardinalities**

If α, β are cardinalities $\alpha = |A|, \beta = |B|$, Cantor defined:

$$\begin{aligned} \alpha + \beta &= |A \sqcup B| \text{ (disjoint union)} \\ \alpha \cdot \beta &= |A \times B| \\ \alpha^\beta &= |B^A| \text{ (set of all functions from } A \text{ to } B) \end{aligned}$$

4 Relations

4.1 Definitions

↪ **Definition 4.1: Relation**

A *relation* on a set A is a subset $S \subseteq A \times A (= \{(x,y) : x, y \in A\})$.

We say that x is *related* to y if $(x,y) \in S$, where we denote $x \sim y$.

Conversely, if we are given $x \sim y$, we can define an $S = \{(x,y) : x \sim y\}$.

⊛ **Example 4.1**

Following are examples of relations on A.

1) Let $S = A \times A$; any $x \sim$ any y because $(x,y) \in S$ for all (x,y).

2) Let $S = \varnothing$; no $x \sim$ any y (even to itself).

3) $S = \text{diag.} = \{(a,a) : a \in A\}$; $x \sim x \forall x$, but $x \nsim y$ if $y \neq x$.

4) $A = [0,1] (\in \mathbb{R})$. Say $x \sim y$ if $x \leq y$. Thus, $S = \{(x,y) : x \leq y\}$ (the diagonal, and everything above).

5) $A = \mathbb{Z}$, $x \sim y$ if $5 | (x - y)$, ie x and y have same residue mod 5.[15]

[15] Where $a|b$ denotes that b divides a.

↪ **Definition 4.2: Reflexive**

A relation is *reflexive* if for any $x \in A$, $x \sim x$.

This includes examples 1), 2) (iff A is empty), 3), 4), and 5) above.

↪ **Definition 4.3: Symmetric**

A relation is *symmetric* if $x \sim y \implies y \sim x$.

This includes 1), 2), 3), and 5) above.

↪ **Definition 4.4: Transitive**

A relation is *transitive* if $x \sim y$ and $y \sim z$ implies $x \sim z$.

This includes 1), 2), 3), 4), and 5) above.

4.2 Orders, Equivalence Relations and Classes, Partitions

↪ **Definition 4.5: Partial Order**

A *partial order* on a set A is a relation $x \sim y$ s.t.

1. $x \sim x$ *(reflexive)*
2. if $x \sim y$ and $y \sim x$, $x = y$ *(antisymmetric)*
3. $x \sim y$ and $y \sim z \implies x \sim z$ *(transitive)*

It is common to use $\leq$ in place of $\sim$ for partial orders.

We call a set on which a partial order exists a *partially ordered set* (poset).

This is called partial, as it is possible that for some $x, y \in A$ we have $x \nsim y$ and $y \nsim x$, ie x, y are not comparable. A partial order is called *linear/total* if for every $x, y \in A$, either $x \leq y$ or $y \leq x$, eg., $A = [0,1], \mathbb{R}, \mathbb{Z}, \ldots$, with $x \leq y$. Consider the above examples:

1) is *not* total, if A has at least two element, because $\exists x \neq y$ but both $x \sim y$ and $y \sim x$, and thus not antisymmetric.

3) yes

5) no, as this is symmetric, since $5|(x-y) \implies 5|(y-x)$, and thus $x \sim y, y \sim x \not\Longrightarrow y = x$

⊛ **Example 4.2**

Let[16] $A = \mathbb{N}_+ = \{1, 2, 3, 4 \dots\}$, and define $a \sim b$ if $a|b$. We verify:

- $a \sim a$ (since $a|a$)
- $a \sim b, b \sim a \implies a = b$, since in $\mathbb{N}_+$, $a|b \implies a \leq b$, and we thus have $a \leq b$ and $b \leq a$, and thus $a = b$.
- suppose $a \sim b$ and $b \sim c$, then $a|b$ and $b|c$. We can write $b = a \cdot m$ and $c = b \cdot n$ for $n, m \in \mathbb{N}$. This means that $c = bn = amn = a(mn)$, which means that $a|c$, so $a \sim c$.

Thus, A is a poset. Note that this is not a linear order, as $2 \nsim 3$, and $3 \nsim 2$ (not all a, b are comparable).

[16] Try this with integers, see where it fails

↪ **Definition 4.6: Equivalence Relation**

We aim to, abstractly, define some $\sim$ such that if $x \sim x, x \sim y$, then $y \sim x$, and if $x \sim y, y \sim z$, then $x \sim z$.

Specifically, an equivalence relation $\sim$ on the set A is a relation $x \sim y$ s.t. it is

- reflexive;
- symmetric;
- transitive.[17]

[17] Note that, generally, equivalence and order relations are very different.

⊛ **Example 4.3**

1. Let $n \geq 1$ be an integer. A *permutation* σ of n elements is a bijection $\sigma : \{1, 2, \dots, n\} \to \{1, 2, \dots, n\}$. Their number is $n!$, ie there are $n!$ permutations of n elements. The collection of all permutations of n elements is denoted S_n, which we call the "symmetric group" on n elements. We aim to define an equivalence relation on S_n.

   Let us define $\sigma \sim \tau$ if $\sigma(1) = \tau(1)$. We verify that this is an equivalence relation:

   (a) $\sigma \sim \sigma, \sigma(1) = \sigma(1)$, so yes

(b) $\sigma \sim \tau$ means $\sigma(1) = \tau(1)$, so yes

(c) $\sigma \sim \tau, \tau \sim \rho, \sigma(1) = \tau(1), \tau(1) = \rho(1)$, so $\sigma(1) = \rho(1)$, hence $\sigma \sim \rho$, so yes.

Thus, $\sim$ is an equivalence relation on S_n.

⊛ **Example 4.4**

Define a relation on $\mathbb{Z}$ by saying that $x \sim y$ if $x - y$ even, ie $2|(x-y)$. This is reflexive, as $2|(x-x) = 0, x \sim x$, symmetric, since $(y-x) = -(x-y)$, and transitive $x - z = \underbrace{(x-y)}_{\text{even}} + \underbrace{(y-z)}_{\text{even}} \implies x \sim z$.

⊛ **Example 4.5**

We say two sets $A \sim B$ if $|A| = |B|$. $1_A = \mathrm{Id} : A \to A, a \mapsto a$ shows $A \sim A$. $A \sim B \implies \exists f : A \to B$ bijective, then $f^{-1} : B \to A$ also bijective so $B \sim A$. If $A \sim B, B \sim A$ then $A \sim C$ (since $|A| = |B|, |B| = |C| \implies |A| = |C|$ as proved earlier).

↪ **Definition 4.7: Disjoint Union**

Let S be a set, and $S_i, i \in I, \subseteq S$. S is the *disjoint union* of the S_i's if $S = \cap_{i \in I} S_i$, and for any $i \neq j$, $S_i \cap S_j = \varnothing$[18]; we denote $S = \amalg_{i \in I} S_i$. We can say that $\{S_i\}$ for a *partition* of S.

[18]ie, no S_i's share elements; think of "partitioning" S such that no subsets overlap.

⊛ **Example 4.6**

Let $S = \{1, 2\}$. Partitions are $\{1, 2\}$, and $\{1\}, \{2\}$.

Let $S = \{1, 2, 3\}$. Partitions are $\{1, 2, 3\}, \{1\}, \{2\}, \{3\}, \ldots$

↪ **Definition 4.8: Equivalence Class**

Given an equivalence relation $\sim$ of A and some $x \in A$, the *equivalence class* of x is $[x] = \{y \in A : x \sim y\} \subseteq S$.

↪ **Theorem 4.1**

The following theorems are related to equivalence classes:

(1) the equivalence classes of A form a partition of A;

(2) conversely, any partition of A defines an equivalence relation on A given by the partition.

↪ Lemma 4.1

Let X be an equivalence class; $a \in X$, then $X = [a]$.

Proof of lemma 4.1. If X is an equivalence class, $X = [x]$ for some $x \in A$, by definition. Let $a \in X$. If $b \in [a]$ then $b \sim a$ and as $a \in [x]$ then $a \sim x \implies b \sim x \implies b \in [x] \implies [a] \subseteq [x]$.

Otoh, $a \sim x \implies x \in [a]$, so $[x] \subseteq [a]$, and thus $[x] = [a]$. ■

Proof of theorem 4.1. We prove (1), (2) individually.

(1) We aim to show that if the equivalence classes are $\{X_i\}_{i \in I}$ then $A = \amalg_{i \in I} X_i$. We say the following:

1. Every $a \in A$ is in some equivalence class ($a \in [a]$).
2. Two different equivalence classes are disjoint $\iff$ if X, Y equiv. classes s.t. $X \cap Y \neq \varnothing$ then $X = Y$.[19]

Let $a \in X \cap Y \overset{\text{lemma}}{\implies} [a] = X, [a] = Y \implies X = Y$.

Here, consider the examples above;

- example 4.3; S_n: there are n equiv classes $X_i = \{\sigma \in S_n : \sigma(1) = i\}$. $S_n = X_1 \sqcup X_2 \sqcup \ldots X_n$. $\sigma \in S_n$ and $\sigma(1) = i$, then $\sigma \in X_i$.
- example 4.4; $\mathbb{Z}$: two equiv. classes; $X =$ even integers $= [0]$, $Y =$ odd integers $= [1]$, so $\mathbb{Z} =$ even $\sqcup$ odd
- example 4.5; sets: an equivalence *is* a cardinality. $n := [\{1, 2, \ldots n\}] =$ all sets with n elements. Similarly, we often write that $\aleph_0 := [\mathbb{N}] =$ inf. countable sets = sets un bijection with $\mathbb{N}$, and $2^{\aleph_0} := [\mathbb{R}]$.

(2) We are given a partition $A = \amalg_{i \in I} X_i$. We say $x \sim y$ if $\exists i \in I$ s.t. x and y belong to X_i (noting that such an i is unique if it exists by definition of a partition).

- $x \sim x$, clearly, since $x \in X_i \implies x \in X_i$
- $x \sim y \implies y \sim x$, by similar logic
- $x \sim y, y \sim z$ means that x and y in some same X_i, and y and z in some same X_j. So, $y \in X_i \cap X_j$, but we are working with a partition so X_i and X_j are disjoint and so this intersection is either $\varnothing$, or the sets are equal; since we know it is not empty, $X_i = X_j$, and so $x \sim z$.

Thus, $\sim$ is an equivalence relation.[20] ■

[20]Contrapositive...

[20]This whole proof/theorem can sound pretty confusing. Abstractly,

⊛ **Example 4.7**

Let $A =$ students in this class. $x \sim y$ if x, y have the same birthday. The equivalence classes in this case are the dates s.t. $\exists$ some student with that birthday.

↪ **Definition 4.9: Complete set of representatives**

If is an equiv. relation on A, a subset $\{a_i : i \in I\} \subseteq A$ is called a *complete set of representatives* if the equivalence classes are $[a_i], i \in I$ with no repetitions.

You find such a subset by choosing from every equiv class one element.Considering our examples:

- For example 4.3, $S_n = X_1 \sqcup \ldots X_n$, $X_i = \{\sigma : \sigma(1) = i\}$. We define

$$\sigma_i(j) = \begin{cases} i & j = 1 \\ 1 & j = i \\ j & \text{otherwise} \end{cases} = [\sigma_i]$$

  (switch i, j and leave all others intact). $\{\sigma_1, \ldots, \sigma_n\}$ are a complete set of representatives.

- For example 4.4 (even/odd in $\mathbb{Z}$), a complete set of reps could be $\{0, 1\}$, ie $\mathbb{Z} = [0] \sqcup [1]$.

5 Number Systems

5.1 Complex Numbers

↪ **Definition 5.1: Complex Numbers**

$\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$. Equivalently, we can consider complex numbers as the points $(a, b) \in \mathbb{R}^2$.[21]

Given some $z = a + bi$, we can write $\mathrm{Re}\,(z) = a, \mathrm{Im}\,(z) = b$.

[21] We can define the function $f : \mathbb{C} \to \mathbb{R}^2, f(a + bi) = (a, b)$, a bijection.

↪ **Definition 5.2: Algebra on Complex Numbers**

Given $z_i = x_i + y_i i$, we define:

- *Addition*: $z_1 + z_2 = (x_1 + x_2) + (y_1 + y_2)i$. This is associative and commutative.
- *Multiplication*: $z_1 z_2 = (x_1 x_2 - y_1 y_2) + (x_1 y_2 + x_2 y_1)i$

- *Inverse*: $z \neq 0$, $\frac{1}{z} := \frac{\overline{z}}{|z|^2}$, noting that $z \cdot \frac{1}{z} = z \cdot \frac{\overline{z}}{|z|^2} = 1$

↪ **Definition 5.3: Complex Conjugate**

Given $z = a + bi$, the *complex conjugate* of z is $\overline{z} = a - bi$.

↪ **Lemma 5.1**

The following hold for complex conjugates:[22]

(a) $\overline{\overline{z}} = z$.

(b) $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}, \overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$.

(c) $\mathrm{Re}\,(z) = \frac{z + \overline{z}}{2}, \mathrm{Im}\,(z)\, i = \frac{z - \overline{z}}{2}$.

(d) Given $|z| = \sqrt{a^2 + b^2}$,

  (i) $|z|^2 = z \cdot \overline{z}$

  (ii) $|z_1 + z_2| \leq |z_1| + |z_2|$

  (iii) $|z_1 \cdot z_2| = |z_1| \cdot |z_2|$

[22](a), (b), and (c) are simply algebraic rearrangements of two complex numbers. (d.i) and (d.iii) follow from similar arguments, and finally (ii) is the triangle inequality restated in terms of complex numbers.

5.2 Fundamental Theorem of Algebra, Etc

↪ **Theorem 5.1: Fundamental Theorem of Algebra**

Any polynomial $a_n x^n + \cdots + a_1 x + a_0$ for $a_i \in \mathbb{C}, n > 0, a_n \neq 0$, has a root in $\mathbb{C}$.

⊛ **Example 5.1: Roots of Unity**

Let $n \geq 1, n \in \mathbb{Z}$. $x^n = 1$ has n solutions in $\mathbb{C}$, called the roots of unity of order n. They are given as $(1, \frac{2\pi k}{n}), k = 0, 1, 2, \ldots, n - 1$ in polar notation.

↪ **Theorem** 5.2

Let $f(x) = a_n x^n + \cdots + a_1 x + a_0$ be a complex polynomial of degree n. Then, there are complex numbers $z_1, \ldots . z_n$ s.t.

$$f(x) = a_n \prod_{i=1}^{n} (x - z_i) \qquad (i)$$

each (ii) $f(z_j) = 0 \forall j = 1, \ldots, n$, and (iii) $f(\lambda) = 0 \implies \lambda = z_j$ for some j.[23]

[23]Proof sketch: we prove by induction. First, we prove the base case of polynomials of deg $= 1$, then we assume it holds for deg $\leq n$. We then prove a separate lemma (also by induction) that allows us to rewrite our polynomial as the product of some $(x - \lambda)$ factor, another polynomial, and some residual. We then rewrite our original polynomial as the product of some linear term and another polynomial, plus some residual, then show that this residual is 0, and thus show that our polynomial of degree $n + 1$ is simply the product of some linear term and a polynomial of degree n, the inductive assumption, and thus the general statement is true.
The "sub"-claims follow naturally.

Proof (by induction). If $n = 1$, $f(x) = a_1 x + a_0 = a_1 \left(x - \frac{-a_0}{a_1} \right) = a_1 (x - z_1)$. Clearly, $f(z_1) = 0$.

Assume that true for polynomials of degree $\leq n$ and prove for $n + 1$; let f be a polynomial of degree $n + 1$, $f(x) = a_{n+1} + x^{n+1} + \cdots$. Let z_{n+1} be a root of $f : f(z_{n+1}) = 0$. Such exists by the Fund'l Thm. We introduce the following lemma:

↪ **Lemma** 5.2

Let g be a polynomial with complex coefficients. Let $\lambda \in \mathbb{C}$; then we can write $g(x) = (x - \lambda) h(x) + r, r \in \mathbb{C}, h$ a polynomial with complex coefficients as well.

Proof of Sub-Lemma. By induction; we can write $g(x) = a_n x^n + \cdots a_1 x + a_0$. If $\deg(g) = 0$, then $g = a_0 \implies h(x) = 0, a_0 = r$.

Assume this is true for degrees $\leq n$,and that g has degree $\leq n + 1$.

$$g(x) = (x - \lambda) a_{n+1} x^n + b(x),$$

where $b(x) = g(x) - (x - \lambda) a_{n+1} x^n = a'_n x^n + a'_{n-1} x^{n-1} + \cdots$, for some $a'_n, \ldots, a'_0 \in \mathbb{C}$. We can apply induction to $b(x)$ (that has $\deg \leq n$); $b(x) = (x - \lambda) h_1(x) + r$, so

$$g(x) = (x - \lambda) \underbrace{(a_{n+1} x^n + h_1(x))}_{h(x)} + r,$$

as desired. ■

Now, we write our $f(x)$ as

$$f(x) = (x - z_{n+1}) h(x) + r,$$

using the lemma. Then,

$$\begin{aligned} 0 = f(z_{n+1}) &= (z_{n+1} - z_{n+1}) h(z_{n+1}) + r \\ &= 0 + r + 0 \implies r = 0, \end{aligned}$$

so

$$f(x) = (x - z_{n+1})h(x).$$

Comparing the highest terms:

$$a_{n+1}x^{n+1} + \dots = (x - z_{n+1})(*x^n + \dots)$$
$$\implies \text{ leading coefficient of } h(x) \text{ also } a_{n+1}.$$

By induction,

$$h(x) = \underbrace{a_{n+1}}_{\text{lead coef of } h} \cdot \prod_{i=1}^{n}(x - z_i)$$
$$\implies f(x) = a_{n+1}\prod_{i=1}^{n+1}(x - z_i) \qquad (i) \text{ holds}$$

Further:

- (ii): $f(z_j) = a_{n+1}\prod_{i=1}^{n+1}(z_j - z_i) = 0$ when $i = j$.
- (iii): if $f(\lambda) = 0$, then $a_{n+1}\prod_{i=1}^{n+1}(\lambda - z_i) = 0$. But if a product of two complex numbers is 0, then one of them is 0. $a_{n+1} \neq 0$, so some $\lambda - z_i = 0$, ie $\lambda = z_i$ for some i[24]

■

[24] This claim relies on the claim that $s_1 \cdot s_2 = 0 \iff s_1$ or $s_2 = 0$ for $s_1, s_2 \in \mathbb{C}$. This is fairly straightforward to prove, and can be extended to any number of complex numbers, ie $\prod_{i=1}^{n} s_i = 0 \iff$ some $s_i = 0$

↪ Definition 5.4: Complex Exponential

The complex exponential, $e^z = 1 + \frac{z}{1} + \frac{z^2}{2!} + \dots$ can be Taylor expanded and we have that

$$e^{i\theta} = \cos\theta + i\sin\theta.$$

⊛ Example 5.2

If $z = e^{x+yi} = e^x \cdot e^{yi} = e^x(\cos y + i\sin y)$, then $z = (e^x, y)$ in polars.

We can apply this idea to prove some trigonometric formulas. Consider $e^{2i\theta}$;

$$e^{2i\theta} = (\cos\theta + i\sin\theta)^2 = \underbrace{\cos^2\theta - \sin^2\theta}_{\text{Re}} + \underbrace{2\sin\theta\cos\theta}_{\text{Im}} i$$
$$e^{2i\theta} = \underbrace{\cos(2\theta)}_{\text{Re}} + i\underbrace{\sin(2\theta)}_{\text{Im}}$$
$$\implies \cos(2\theta) = \cos^2\theta - \sin^2\theta$$
$$\implies \sin(2\theta) = 2\sin\theta\cos\theta$$

6 Rings (A Brief Introduction)

6.1 Definitions

↪ **Definition 6.1: Ring**

A ring R is a set with two operations[25]

- *Addition:* $R \times R \xrightarrow{+} R, \quad (a,b) \mapsto a+b$
- *Multiplication:* $R \times R \xrightarrow{\cdot} R, \quad (a,b) \mapsto a \cdot b$

The following hold:

1. (+ is commutative) $a+b=b+a, \forall a,b \in R$.
2. (+ is associative) $a+(b+c)=(a+b)+c, \forall a,b,c \in R$.
3. (0) ∃ a zero element, 0, s.t. $0+a=a+0=a, \forall a \in R$.
4. (negative) $\forall a \in R, \exists b \in R$ s.t $a+b=0$.
5. (· associative) $a(bc)=(ab)c, \forall a,b,c \in R$.
6. (1, multiplicative identity) $\exists 1 \in R$ s.t. $1 \cdot a = a \cdot 1 = a, \forall a \in R$.[26]
7. (distributive) $\forall a,b,c \in R, a(b+c)=ab+ac$

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{R}[i] := \{a+b_i : a,b \in \mathbb{Z}\}, M_2(\mathbb{Z}) := \{\begin{matrix} a & b \\ c & d \end{matrix} : a,b,c,d \in \mathbb{Z}\}, \dots$ are all examples of rings.

[26]Though not always explicitly stated, it is often specified that rings are *closed* under addition/multiplication; $a,b \in R \implies a+b$ and $a \cdot b \in R$.

[26]Some texts (Hungerford) do not require the multiplicative identity to exist in a ring; those with this property are called "rings with identity". In general, these are all relatively arbitrary conventions - they are defined as such to make other operations/observations clearer; they are not steadfast, natural definitions.

Remark 6.1. *We do not require multiplication to be commutative; if it is, we call R a **commutative ring** (eg $M_2(\mathbb{Z}), M_2(\mathbb{R})$ are not commutative).*

We also do not require inverse for multiplication (eg 2 doesn't have an inverse in $\mathbb{Z}$).

↪ **Definition 6.2: Field**

A *commutative*, non-zero, ring R s.t. $\forall x \in R$ and $x \neq 0$ ($\iff 1 \neq 0$ in R, ie R is not a zero ring), $\exists y \in R$ s.t. $xy=yx=1$ is a *field*.

Fields include $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Q}[i]$

↪ **Definition 6.3: Zero Ring**

$\{0\}$ with $0+0=0, 0\cdot 0=0$, where $1=0$ (identity element is 0).

⊛ **Example 6.1**

Show that $\mathbb{Q}[i]$ is a field.

If $x \in \mathbb{Q}[i], x = a+bi \neq 0$ then

$$\frac{1}{a+bi} = \frac{a-bi}{(a+bi)(a-bi)} = \underbrace{\frac{a}{a^2+b^2}}_{\in\mathbb{Q}} - \underbrace{\frac{b}{a^2+b^2}}_{\in\mathbb{Q}} i \in \mathbb{Q}[i],$$

and thus $\mathbb{Q}[i]$ has multiplicative inverses in $\mathbb{Q}[i]$.

↪ **Corollary 6.1**

Note the following consequences of the above axioms:

1. 0 is unique; if $x \in R$ has the property that $x+a=a+x=a\forall a \in R$, then $x=0$.
2. 1 is unique; if $x \in R$ has the property that $x\cdot a=a\cdot x=a\forall a \in R$, then $x=1$.
3. The element b s.t. $a+b=b+a=0$ is uniquely determined by a; if $x \in R$ and $x+a=a+x=0$, then $x=b$. We denote such b as $-a$, ie

$$-a+a=a+(-a)=a-a=0.$$

4. $-(-a)=a$.
5. $-(x+y)=-x-y$.
6. $x\cdot 0=0\cdot x=0\forall x \in R$.

↪ **Definition 6.4: Subring**

Let R be a ring. A subset $S \subseteq R$ is a *subring* if

1. $0, 1 \in S$.
2. $x, y \in S \implies x+y, -x, x\cdot y \in S$.

Then, S is a ring itself.

$\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ are subrings; $\mathbb{Z} \subseteq \mathbb{Z}[i] \subseteq \mathbb{Q}[i] \subseteq \mathbb{C}$ are subrings; $M_2(\mathbb{Z}) \subseteq M_2(\mathbb{R})$ are subrings.

7 Division

7.1 With Residue

↪ **Theorem 7.1**

Let $a, b \in \mathbb{Z}$ with $b \neq 0$. There exist unique integers q (quotient) and r s.t.

$$a = q \cdot b + r, 0 \leq r < |b|.$$

Proof. Assume $b > 0$ (similar proof applies for $b < 0$). Consider the set $S = \{a - bx : x \in \mathbb{Z}, a - bx \geq 0\}$. Note that $S \neq \varnothing$. If $a \geq 0$, take $x = 0$. If $a < 0$, take $x = a$ to get $a - bx = a - ba = a(1 - b) \geq 0$.
Thus, S has a minimal element; let $r = \min(S)$. Because $r \in S, r \geq 0$, and

$$r = a - bq \text{ some } q \in \mathbb{Z} \implies a = bq - r.$$

Here, we claim $r < b$. If $r \geq b$, then $0 \leq r - b = a - b(q + 1) \in S$, contradicting the minimality of r. Thus, $0 \leq r < b$.
We wish to show that q, r are unique, meaning that if $a = bq' + r', q' \in \mathbb{Z}, 0 \leq r < b \implies q = q', r = r'$.
If $q = q'$, then $r = a - bq = a - bq' = r' \checkmark$.
Otherwise, wlog, say $q > q'$. We then have

$$\begin{aligned} 0 &= a - a = (bq + r) - (bq' + r') \\ &= b(q - q') + (r - r') \\ &\implies r' = r + b(q - q') \geq b, \perp (0 \leq r' < |b|) \end{aligned}$$

■

7.2 Without Residue

↪ **Definition 7.1**

Let $a, b \in \mathbb{Z}$. We say a divides b, $a|b$ if $b = a \cdot c$, some $c \in \mathbb{Z}$ (If $a \neq 0$, this is the case $\iff$ the residue of dividing b by a is 0).

↪ **Lemma 7.1: Properties of Division**

1. 0 is divisible by any integer a
2. 0 only divides 0

3. $a|b \implies a|(-b)$

4. $a|b$ and $a|d \implies a|(b \pm d)$

5. $a|b \implies a|bd \forall d$

6. $a|b$ and $b|a \implies a = \pm b$

Proof. 1. $0 = a \cdot 0 \forall a$ ✓

2. $0|b$, then $b = 0 \cdot c$ some $c \implies b = 0$ ✓

3. $b = ac \implies -b = a \cdot (-c)$ ✓

4. $b = a \cdot c_1, d = a \cdot c_2$. $b \pm d = a(c_1 \pm c_2) \in \mathbb{Z}$ ✓

5. $b = ac$, so $bd = a \cdot (cd)$ ✓

6. $a|b \implies b = a \cdot c, b|a \implies a = b \cdot d$. If either $a = 0$ or $b = 0$, both are 0, so $a = \pm b$. Assume $a \neq 0, b \neq 0$. Then, we have that $a = bd = acd \overset{a \neq 0}{\implies} cd = 1$. Either, $c = d = 1 \implies a = b$, or $c = d = -1 \implies a = -b$ ✓

■

⊛ **Example 7.1**

Which integers could divide both n and $n^3 + n + 1$?
Suppose d does. then $d|n$ and $d|(n^3 + n + 1)$, then $d|n^3 \implies d|(n^3 + n) \implies d|((n^3 + n + 1) - (n^3 + n))$, and so $d|1$ so $d = \pm 1$.

7.3 Greatest Common Divisor (gcd)

↪ **Definition 7.2: GCD**

Let a, b be integers, not both 0. The $\gcd$ of a, b denoted $\gcd(a, b)$ is the greatest positive number divided both a and b.

Remark 7.1. *Note that if both a, b are not 0, then $d = \gcd(a, b) \leq \min\{|a|, |b|\}$ because if $d|a$ then $a = d \cdot c \implies |a| = |d| \cdot |c| \implies |d| = d \leq |a|$.*
Similarly, $|d| \leq |b|$.

↪ **Theorem 7.2**

Let $a, b \in \mathbb{Z}$, not both 0. Let $d = \gcd(a, b)$. Then,

1. $\exists u, v \in \mathbb{Z}$ s.t. $d = ua + vb$;

2. d is the minimal positive integer of the form $ua + vb$, $u, v \in \mathbb{Z}$;

3. every common divisor of a, b divides d.

Proof. Let $S = \{ma + nb : m, n \in \mathbb{Z}, ma + nb > 0\}$. $S \neq \varnothing$ because $a \cdot a + b \cdot b = a^2 + b^2 > 0$, so $a^2 + b^2 \in S$.
Let $D = \min(S)$, so $D = ua + vb, u, v \in \mathbb{Z}$. We claim that this D equals $d = \gcd(a, b)$.
We claim first that $D|a$. We can write

$$\begin{aligned} a &= D \cdot q + r, 0 \leq r < D, \\ r &= a - Dq = a - (ua + vb)q \\ &= a(1 - uq) + b(-vq) \\ &\implies r > 0 \implies r \in S, \text{ contradicts minimality of } D \end{aligned}$$

Thus, D divides both a and b, and so $D \leq d$ (any common divisor is leq gcd).
Let e be any common divisor of a, b. We have

$$e|a \implies e|ua \quad \text{and} \quad e|b, \implies e|vb \implies e|(ua + vb) = D.$$

In particular, $d|D \implies d \leq D$. It follows that $D = d$. ■

⊛ **Example 7.2**

$\gcd(7611, 592) = 1$.
One can write $1 = 195 \times 7611 - 2507 \times 592$. How do we know? Mathematica.

7.4 Euclidean Algorithm

Remark 7.2. $\gcd(-a, b) = \gcd(a, b) = \gcd(a, -b) = \cdots$

↪ **Theorem 7.3: Euclidean Algorithm**

Let a, b be positive integers $a \geq b$.
If $b|a$, then $\gcd(a, b) = b$.
Else, perform the following:

$$\begin{aligned} a &= b \cdot q_0 + r_0, \quad 0 < r_0 < b \\ b &= r_0 \cdot q_1 + r_1, \quad 0 < r_1 < r_0 \\ r_0 &= r_1 \cdot q_2 + r_2 \\ &\vdots \quad \vdots \\ r_{t-2} &= r_{t-1} \cdot q_t + r_t, \quad 0 < r_t < r_{t-1} \\ r_{t-1} &= r_t \cdot q_{t+1} + \underbrace{0}_{r_{t+1}} \end{aligned}$$

Because the residues are non-negative decreasing integers, the process must stop; there is a first t s.t. $r_{t+1} = 0$. Then, $\gcd(a, b) = r_t$, the last non-zero residue.[27]

[27] Sketch: we show the equivalence by proving that they each divide each other, and are thus equal by lemma 7.1. This is done by induction on the residuals dividing "each other", and working "backwards" essentially, then by induction on an arbitrary element dividing the residuals to show that it must then divide the gcd.

Proof. We first prove by induction that for all $0 \leq i \leq t+1$, r_t divides both r_{t-i} and r_{t-i-1}. ($\implies r_t | r_{-1} = b, r_t | r_{-2} = a$.)

(1) $i = 0$, then $r_t | r_t$ and $r_t | r_{t-1}$ (as $r_{t-1} = r_t \cdot q_{t+1}$)

(2) Suppose $r_t | r_{t-i}$ and $r_t | r_{t-i-1}$ for some $0 \leq i < t+1$. We have that

$$r_{t-i-2} = r_{t-i-1} \cdot q_{t-i} + r_{t-i}$$

We then have that

$$r_t | (r_{t-i} + r_{t-i-1} q_{t-i}) = r_{t-i-2},$$

so $r_t | \underbrace{r_{t-i-1}}_{r_{t-(i+1)}}$ and $r_t | \underbrace{r_{t-i-2}}_{r_{t-(i+1)-1}}$. Then, $r_t | \gcd(a, b)$.

Next we show that if $e|a$ and $e|b$ then $r|r_t$ ($\implies \gcd(a, b)|r_t$, then we would have $r_t = \gcd(a, b)$). We prove by induction on $0 \leq i \leq t+1$ that $e | r_{i-2}$ and $e | r_{i-1}$.

(1) $i = 0$, then $e | r_{-2} = a$ and $e | r_{-1} = b$, base case holds

(2) Suppose $e | r_{i-2}$ and $e | r_{i-1}$ for some $i < t+1$. We have that

$$r_{i-2} = r_{i-1} \cdot q_i + r_i, \quad e | (r_{i-2} - r_{i-1} \cdot q_i) = r_i.$$

So,

$$e | \underbrace{r_i}_{r_{(i+1)-2}} \quad \text{and} \quad e | \underbrace{r_i}_{r_{(i+1)-1}}$$

■

Remark 7.3 (Extended Euclidean Algorithm). *After completing the algorithm, one can then "work backwards" to write any $d = \gcd(a, b)$ as $d = ua + vb$.*
Start by writing $d = r_{t-2} - r_{t-1} \cdot q_t$; then, substitute in preceding residuals, simplifying along the way (but making sure to leave the quotients *from each substitution, as these are what you will substitute in the next step), and continue until you have the desired form. Consider the following example:*

⊛ **Example 7.3**

$a = 48, b = 27, d = \gcd 48, 27 = ?$

$$\begin{aligned}
48 &= 27 \cdot 1 + 21 \\
27 &= 21 \cdot 1 + 6 \\
21 &= 6 \cdot 3 + 3 \\
6 &= 3 \cdot 2 + 0 \\
&\implies \gcd(48, 27) = 3 \\
&\implies 3 = 21 - 6 \cdot 3 \\
&= 21 - (27 - 21)3 \\
&= 21 \cdot 4 - 27 \cdot 3 \\
&= (48 - 27) \cdot 4 - 27 \cdot 3 \\
&= 48 \cdot 4 - 7 \cdot 27
\end{aligned}$$

7.5 Primes

↪ **Definition 7.3: Prime**

An integer $n \neq 0, 1, -1$ is called prime if its only divisors are $\pm 1, \pm n$.
A positive integer n is prime iff its only positive divisors are $1, n$.

Remark 7.4. *The goal of this section is to prove theorem 7.5, of unique prime factorization; we then extend it to the rationals. We introduce a number of lemmas/auxiliary results regarding primes to build up to the proof.*

↪ **Lemma 7.2**

Every natural number $n > 1$ is a product of prime numbers.

Proof. We prove by induction.
Base case; $n = 2$, 2 is prime, done.
Suppose it is true for all integers $1 < r \leq n$; we will prove for $n + 1$.[28]

- If $n + 1$ is prime, we are done.
- Else, $n + 1$ has a non-trivial factorization, $n + 1 = r \cdot s$, where $1 < r \leq n, 1 < s \leq n$. By induction, there exists primes p_i, q_i such that $r = p_1 \cdots p_a$ and $s = q_1 \cdots q_b$. We can then write
$$n + 1 = r \cdot s = p_1 \cdots p_a q_1 \cdots q_b,$$
a product of primes, and so we are done.

■

[28] Complete induction...

↪ **Definition 7.4: Empty Product**

1; when we say $n = p_1 \cdots p_a, 0 \leq a$, a product of primes, a = 0, empty product, means $n = 1$.

↪ **Corollary 7.1**

Any non-zero integer n is of the form

$$\epsilon \cdot p_1 \cdots p_a, \quad \epsilon \in \{\pm 1\},$$

where p_i are primes numbers, $a \geq 0$.

Proof. If $n > 1$, this is the lemma 7.2 where $\epsilon = 1$. If $n < -1$, the by lemma 7.2,

$$-n = p_1 \cdots - p_n$$

so $n = -1 p_1 \cdots p_a = -p_1 \cdots p_a$. ■

↪ **Theorem 7.4: Sieve of Eratosthenes**

Let $n > 1$ be an integer. If n is not prime, then n is divisible by some prime $1 < p \leq \sqrt{n}$.

Sketch Proof. $n = p_1 \cdots p_a$. n not prime, $a \geq 2$. If each $p_i > \sqrt{n}$, then $p_1 p_2 \cdots p_a < \sqrt{n} \cdot \sqrt{n} = n, \perp$ ■

↪ **Lemma 7.3**

Let $p > 1$ be an integer. The following are equivalent:

1. p is prime
2. If $p | ab$, product of two nonzero integers, then $p | a$ or $p | b$.

Proof. Assume 2., suppose $p = st \in \mathbb{Z}$. wlog, $s, t > 0$ (else replace s by $-s$, t by $-t$). $p | st$, so by 2., say $p | s$, wlog. We can write $s = p \times w$, then $p = s \cdot t = p \cdot w \cdot t$, which are all positive integers. It must be that $w = t = 1$, and thus $s = p$. Therefore, p has no non-trivial factorizations and is thus prime.
Assume now that 1. holds; $p | ab$. If $p | a$, we are done.
Suppose $p \nmid a$. Then, $\gcd(p, a) = 1$ (since only divisors of p are 1, p, so $\gcd$ could only be $1, p$, but if $\gcd = p$ then $p | a$ which is not the case). From a property of gcd's, we can write $1 = up + va$ for some $u, v \in \mathbb{Z}$. Multiplying this by b, we have $b = upb + vab$.

We have

$$
\begin{aligned}
p|ab &\implies p|vab \\
p|p &\implies p|upb \\
&\implies p|(upb + vab), \text{ so } p|b
\end{aligned}
$$

■

↪ **Corollary 7.2**

Let p be prime. Suppose $p|a_1 a_2 a_3 \cdots a_m$ where $a_i \in \mathbb{Z}, m \geq 1$. Then, $p|a_i$ for some i

Proof. By induction; we just showed the case $m = 2$. Suppose it is true for $m \geq 2$ and $p|a_1 a_2 \cdots a_{m+1}$; then, $p|\underbrace{(a_1 a_2 \cdots a_m)}_{(i)} \cdot \underbrace{a_{m+1}}_{(ii)}$. Then, either $p|(i)$ or $p|(ii)$, so $p|a_{m+1}$ or $p|a_i, 1 \leq i \leq m$, as required. ■

↪ **Theorem 7.5: Fundamental Theorem of Arithmetic**

Let $n \in \mathbb{Z}, n \neq 0$. There exists $\epsilon \in \{\pm 1\}$ and prime numbers $p_1, \cdots, p_a, a \geq 0$ such that $n = \epsilon \cdot p_1 \cdots p_a$, **uniquely**.[29]

Proof. First, it is clear that the sign is unique, so wlog, we only consider positive n. We have already proved that ∃ such a factorization by lemma 7.2; we now aim to show that this is unique. We proceed by induction.
Base case: $n = 1$; $p_i, q_j \geq 2$, only option is the empty product $a = b = 0$.
Assumption: say holds for integers $1 \leq m \leq n-1, n \geq 2$ (numbers smaller than n). We are given

$$n = p_1 \cdots p_a = q_1 \dots q_b.$$

- Suppose $p_1 = q_1$. Then $m = \frac{n}{p_1} = p_2 \cdots p_a = q_2 \cdots q_b \implies a = b$ and $p_i = q_i$ for $2 \leq i \leq a$ (and also, $p_1 = q_1$) (covered by inductive hypothesis)
- Otherwise, $p_1 \neq q_1$, and wlog (symmetric) $p_1 < q_1$. We have $p_1 | n$ so $p_1 | q_1 \cdots q_b \overset{p \text{ prime}}{\implies} p_1 | q_i$ for some $1 \leq i \leq b$ (by lemma 7.3, extended to the product of any number of numbers). As p_i prime, $p_1 = q_i$, implying $p_1 < q_1 \leq q_2 \leq \cdots q_i = p_1$, a contradiction to the assumption that $p_1 < q_1$. Thus, $p_1 = q_1$.

Alternatively, we could write $n = \epsilon p_1^{a_1} \cdots p_s^{a_s}$ where p_i are distinct prime numbers and $a_i > 0$ (ie, we are "collecting" the identical primes, and raising them to the power of how many times they appear) where p_i and a_i are unique. ■

[29]Sketch: this shows only uniqueness, existence is proven by lemma 7.2. Use induction; base case, $n = 2$ trivial. Use complete induction, and proceed by contradiction (kind of). Assume that n has two distinct prime factorizations. Then, break down by cases; $p_1 = q_1$ or not. If they are, then take some small m covered by inductive assumption, set equal to $\frac{n}{p_1}$, meaning that if $p_1 = q_1$, the remaining $p_i = q_i$.
For inequality, show that $p_1 < q_1 \implies p_1 < p_1$ by showing that $p_1 | q_1 \cdots$, and thus $p_1 = q_i$ for some i, so $p_1 < q_1 \leq \cdots q_i = p_1$, and thus you have a contradiction.

↪ **Theorem 7.6: Version of FTA for Rationals**

Let $q \neq 0$ be a rational number. Then, $\exists$ a unique sign $\epsilon \in \{\pm 1\}$, integer s, primes $p_1, \ldots, p_a$ and exponents $a_i \in \mathbb{Z}, a_i \neq 0$ s.t.

$$q = \epsilon \cdot p_1^{a_1} \cdots p_s^{a_s}$$

Proof. Write $q = \frac{m}{n}$, where $m, n \in \mathbb{Z}$. Then, we can write m as

$$m = \epsilon_m \cdot p_1^{b_1} \cdots p_s^{b_s}; \qquad n = \epsilon_n \cdot p_1^{c_1} \cdots p_s^{c_s}$$

Remark 7.5. *If we allow 0 as an exponents, we can write these such that the same primes appear in both n and m.*

We can then write

$$\frac{m}{n} = \frac{\epsilon_m}{\epsilon_n} p_1^{b_1 - c_1} \cdots p_s^{b_s - c_s}.$$

We can now omit the primes with $b_i - c_i = 0$ to get only non-zero exponentiated primes. We have thus shown existence
To show uniqueness, we can disregard the sign as before. Say $0 < q = p_1^{a_1} \cdots p_s^{a_s} = p_1^{a_1'} \cdots p_s^{a_s'}$. If these are equivalent representations, then letting $c_i = a_i - a_i'$, we get that $1 = p_1^{c_1} \cdots p_s^{c_s}$; thus, we aim to show that $c_1 = \cdots c_s = 0$. wlog, we can rearrange these c's such that $c_1, \cdots, c_t < 0, c_{t+1}, \cdots, c_s \geq 0$. This implies that $p_1^{-c_1} \cdots p_t^{-c_t} = p_{t+1}^{c_{t+1}} \cdots p_s^{c_s}$. This is an equality on integers, and as given by FTA, this is only possible if $c_i = 0 \forall i$. ■

↪ **Proposition 7.1**

$\sqrt{2} \notin \mathbb{Q}$

Proof. Suppose it is. Then $\sqrt{2} = p_1^{a_1} \cdots p_s^{a_s}$, $a_i \neq 0, p_i$ distinct primes. Then, we have

$$2 = (p_1^{a_1} \cdots p_s^{a_s})^2 = p_1^{2a_1} \cdots p_s^{2a_s}.$$

But, $2 = 2^1$, and by uniqueness of factorization, we get a contradiction because $1 \neq 2a_i$ for any i. ■

↪ **Theorem 7.7**

There exist infinitely many prime numbers.

Proof. Suppose $p_1, \ldots, p_n$ are distinct prime numbers. Then, there exists a prime number p_{n+1} which is not one of these. Let $N = p_1 p_2 \cdots p_n + 1 > 1$, so $\exists p | N$ where p prime. If $p =$ on of

$p_1 \dots p_n$, say some p_i; then, $p|N$ and $p|p_1 p_2 \cdots p_n \implies p|(N - p_1 \cdots p_n) \implies p|1$, which is a contradiction. ■

↪ **Proposition 7.2**

Let $a, b \neq 0, a, b \in \mathbb{Z}$. Then $a|b \iff a|\epsilon p_1^{a_1} \cdots p_m^{a_m}, a_1 > 0, p_i$ prime, $\epsilon \in \{\pm 1\}$ and $b = \mu p_1^{a_1'} \cdots p_m^{a_m'} q_1^{b_1} \cdots q_t^{b_t}, a_i' \geq a_i, q_i$ primes, $b_i > 0$.

Proof. If we can, then $\frac{b}{a} = \underbrace{\frac{\mu}{\epsilon} \cdot p_1^{a_1'-a_1} \cdots p_m^{a_m'-a_m} q_1^{b_1} \cdots q_t^{b_t}}_{:=c} \implies b = a \cdot c \implies a|b$.

If $a|b$ so $b = a \cdot d$. We can write $a = \epsilon p_1^{a_1} \cdots p_m^{a_m}$, and $d = \epsilon' p_1^{r_1} \cdots p_m^{r_m} q_1^{b_1} \cdots q_t^{b_t}$, and let $b = (\epsilon\epsilon') p_1^{a_1+r_1} \cdots p_m^{a_m+r_m} q_1^{b_1} \cdots q_t^{b_t}$ (where $r_i > 0$), and let $a_i' = a_i + r_i \geq a_i$. ■

↪ **Corollary 7.3**

Let $n = \epsilon p_1^{a_1} \cdots p_t^{a_t} \in \mathbb{Z}$, $\epsilon = \pm 1$, p_i distinct primes, $a_i > 0$. Then the divisors of n are precisely the integers

$$\mu p_1^{c_1} \cdots p_t^{c_t}, \quad \mu = \pm 1, 0 \leq c_i \leq a_i.$$

Remark 7.6. *Let $a, b \in \mathbb{Z} \setminus \{0\}$; we write*

$$a = \epsilon p_1^{a_1} \cdots p_t^{a_t}, b = \mu p_1^{b_1} \cdots p_t^{b_t}.$$

We have $d = \gcd(a, b) = p_1^{\min(a_1,b_1)} \cdots p_t^{\min(a_t,b_t)}$.
theorem 7.2 also follows naturally from this manner of thinking, and can be proved accordingly.

⊛ **Example 7.4**

$90 = 2 \cdot 3^2 \cdot 5 \cdot 7^0; 210 = 2 \cdot 3 \cdot 5 \cdot 7. \gcd(90, 210) = 2 \cdot 3 \cdot 5 \cdot 7^0 = 30 \checkmark$.

8 Congruences, Modular Arithmetic

8.1 Definitions

↪ **Definition 8.1**

Fix $n \geq 1, n \in \mathbb{Z}$. We define a relation of $\mathbb{Z}$ by $x \sim y$ if $n|(x - y)$.

⊛ **Example 8.1**

$n = 2$; $x \sim y$ if they have the same parity, ie both even or both odd.

↪ **Lemma 8.1**

The above relation is an equivalence relation. We will denote the equivalence class of an integer r by $\overline{r}$. Then,

$$\overline{r} = \{\dots r-2n, r-n, r, r+n, r+2n, \dots\}.$$

The set

$$\{\overline{0}, \overline{1}, \cdots, \overline{n-1}\}$$

is a complete set of representatives.

Proof. We first show that the relation is an equivalence relation:
Reflexive: $x - x = 0 \implies n|(x-x)\forall n$, so $x \sim x$.
Symmetric: say $x \sim y \implies n|(x-y) \implies n|-(x-y) \implies n|(y-x) \implies y \sim x$.
Transitive: say $x \sim y, y \sim z \implies n|(x-y), n|(y-z) \implies n|((x-y)+(y-z)) \implies n|(x-z) \implies x \sim z$.
Now, we show that the described set is a complete set of representatives, ie we aim to show

1. *any $x \in \mathbb{Z}$ belongs to some $\overline{r}, 0 \leq r \leq n-1$.*

   Proof of 1: Given $x \in \mathbb{Z}$, we can write $x = q \cdot n + r, 0 \leq r \leq n-1$, and $x - r = q \cdot n \implies n|(x-r)$, so $x \sim r$. Ie, $x \in \overline{r}$.

2. *if $0 \leq r \leq s \leq n-1$ and $\overline{r} = \overline{s}$, then $r = s$ (no repetitions, ie "repeat representation").*

   Proof of 2: If $\overline{r} = \overline{s}$, then $r \in \overline{r}$ and $r \in \overline{s}$, so $r \sim s$. So, $n|(s-r)$; but $0 \leq s-r \leq n-1 < n$, implying $s - r = 0 \implies s = r$ (since it must be a multiple of n, but less than n).

■

⊛ **Example 8.2**

For $n = 2$, we have two equivalence classes, $\overline{0} = \text{evens} = \{2x : x \in \mathbb{Z}\}, \overline{1} = \text{odds} = \{2x + 1s : x \in \mathbb{Z}\}$.
For $n = 3$, we have three; $\overline{0} = \{3x : x \in \mathbb{Z}\}, \overline{1} = \{1 + 3x : x \in \mathbb{Z}\}, \overline{2} = \{2 + 3x : x \in \mathbb{Z}\}$.

↪ **Definition 8.2**

$x \sim y$, we say x is congruent to y modulo n, and write

$$x \equiv y \mod n.$$

↪ **Definition 8.3**

We use $\mathbb{Z}/n\mathbb{Z}$ or $\mathbb{Z}_n$ to denote the collection of congruence classes $\mod n$, ie $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$.

↪ **Theorem 8.1**

$\mathbb{Z}/n\mathbb{Z}$ is a commutative ring with n elements. It is a field iff n is prime.
We often denote $\mathbb{Z}/p\mathbb{Z}$ where p prime as $\mathbb{F}_p$.

Proof. We define $\overline{r} + \overline{s} = \overline{r+s}$, $\overline{r} \cdot \overline{s} = \overline{rs}$. This is well defined; meaning if we use other representatives r', s', we'll get the same result. Ie, given $r \sim r', s \sim s'$, we need to show $\overline{r' + s'} = \overline{r+s}, \overline{r' \cdot s'} = \overline{r \cdot s}$, ie $n|((r+s) - (r'+s')), n|(rs - r's')$.
$(r+s) - (r'+s') = (r - r') + (s - s')$; both $r - r'$ and $s - s'$ are divisible by n, so we can write $rs - r's' = r(s-s') + s'(r - r')$; this whole thing is divisible by n. Now, we can verify the axioms:

1. $\overline{r} + \overline{s} = \overline{s} + \overline{r}; \overline{r} + \overline{s} = \overline{r+s} = \overline{s+r} = \overline{s} + \overline{r}$ *(commutativity of addition)*
2. $\dots$
3. $\overline{0}$ is the neutral element; $\overline{0} + \overline{r} = \overline{0+r} = \overline{r}$ *(neutral addition element)*
4. $\overline{(}r) + \overline{(-r)} = \overline{(-r)} + \overline{r} = \overline{0}$ *(inverse wrt addition)*
5. $\dots$
6. $\overline{1} \cdot \overline{r} = \overline{r}$
7. $\dots$

We now aim to show that $\mathbb{Z}/n\mathbb{Z} \iff n \in \mathbb{P}$. Suppose n composite, namely $na \cdot b$, $1 < a < n, 1 < b < n$. Note that $\overline{a}, \overline{b} \neq \overline{0}$; but, $\overline{a} \cdot \overline{b} = \overline{a \cdot b} = \overline{n} = \overline{0}$. If $\mathbb{Z} \setminus n\mathbb{Z}$ is a field, then $\exists \overline{y}$ s.t. $\overline{y} \cdot \overline{a} = \overline{1}$. We have $(\overline{y} \cdot \overline{a}) \cdot \overline{b} = \overline{1} \cdot \overline{b} = \overline{b}$, but $\overline{y} \cdot (\overline{a} \cdot \overline{b}) = \overline{y} \cdot \overline{0} = \overline{0}$, a contradiction.
Suppose, now, $n \in \mathbb{P}$. To show $\mathbb{Z}/n\mathbb{Z}$ is a field; let $\overline{a} \neq \overline{0} \in \mathbb{Z}/n\mathbb{Z}$, that is $n \nmid a$. But n is prime, so $\gcd(a, n) = 1$, so $\exists u, v \in \mathbb{Z}$ such that $1 = ua + vn$. But this means

$$n|(1 - ua) \implies ua \equiv 1 \mod n \implies \overline{u} \cdot \overline{a} = \overline{1} \in \mathbb{Z}/n\mathbb{Z},$$

and we have thus found a multiplicative inverse. ■

⊛ **Example 8.3**

$n = 2$; we have

$+$	0	1
0	0	1
1	1	0

and

$\times$	0	1
0	0	0
1	0	1

; $\overline{1} + \overline{1} = \overline{2} = \overline{0}$.

⊛ **Example 8.4**

$n = 3$; we have

$+$	0	1	2
0	0	0	0
1	1	2	0
2	2	0	1

and

$\times$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

; $\overline{2} + \overline{2} = \overline{4} = \overline{1}$.

↪ **Lemma 8.2**

Let R be a commutative ring. If R has zero divisors then R is not a field.

Proof. Let $x \neq 0$ be a zero divisor, and $y \neq 0$ s.t. $xy = 0$. If R a field, then $\exists z \in R$ s.t. $zx = 1$. But then, $z(xy) = z \cdot 0 = 0$, and $z(xy) = (zx)y = 1 \cdot y = y$, hence y must be 0, a contradiction. ■

↪ **Definition 8.4: Unit**

An element x in a ring R is called a *unit* if $\exists y \in R$ such that $xy = yx = 1$.

⊛ **Example 8.5**

If R a field, then any nonzero $x \in R$ is a unit. If $R = \mathbb{Z}/6\mathbb{Z}$, then $2, 3, 4$ are not units, but 1 and 5 are units.

↪ **Proposition 8.1**

Take $n > 1$. An element $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ is a unit iff $\gcd(a, n) = 1$.

Proof. Note: $\gcd(a, n) = 1$ depends only on the congruence class $\overline{a}$; $\gcd(a+kn, n) = \gcd(a, n)$. Suppose $\overline{a}$ is a unit, ie $\exists \overline{y} \in \mathbb{Z}/n\mathbb{Z}$ s.t. $\overline{y} \cdot \overline{a} = \overline{1} \implies \overline{ya} = \overline{1} \implies ya - 1 = k \cdot n$, for some $k \in \mathbb{Z}$, ie $ya - kn = 1$. Thus, if $d | a$ and $d | n$, then $d | 1 \implies d = \pm 1 \implies \gcd(a, n) = 1$. Conversely, suppose $\gcd(a, n) = 1$. Then, $\exists u, v \in \mathbb{Z}$ s.t. $ua + vn = 1 \implies \overline{u} \cdot \overline{a} + \overline{vn} = \overline{1}$. Now, $\overline{n} = \overline{0} \implies \overline{v} \cdot \overline{n} = \overline{0}$, so $\overline{u} \cdot \overline{a} = 1$, hence $\overline{a}$ is a unit. ■

↪ **Corollary 8.1**

If n is prime any $\overline{a} \neq \overline{0}$ is a unit.

8.2 Binomial Coefficients

↪ **Definition 8.5: Binomial Coefficient**

Let $m \geq n$ be non-negative integers. $\binom{m}{n}$ (m choose n) ways to choose m objects among n objects, where order doesn't matter, where $\binom{m}{n} = \frac{m!}{n!(m-n)!}$.
We also have that

$$\binom{n}{l} + \binom{n}{l-1} = \binom{n+1}{l}$$

$$\begin{array}{ccccccc} & & & \binom{0}{0} & & & \\ & & \binom{1}{0} & & \binom{1}{1} & & \\ & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & \\ \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} \end{array}$$

Pascal's Triangle

↪ **Lemma 8.3**

Let $p \in \mathbb{P}$, and let $1 \leq n \leq p - 1$. Then,

$$p \mid \binom{p}{n}$$

.

Proof. First note that if $1 \leq a \leq p-1, p \not| a!$. If $p|a! = 1 \cdot 2 \cdot 3 \cdots a$, then $p|b$ where $b = \{1, 2, \ldots a\}$. But we have that $1 \leq b \leq p$, so this is not possible.

Now, we have $\binom{p}{n} = \frac{p!}{n!(p-n)!} = d \in \mathbb{Z} \implies p! = d \cdot n!(p-n)!$. As $p|p!$ and $p \not| n!$ nor $(p-n)!$, (as shown above) since $n \leq p-1, p-n \leq -1$, so, since p prime, $p|d$. ■

8.3 Solving Equations in $\mathbb{Z}/n\mathbb{Z}$

↪ **Definition 8.6**

8.3.1 Linear Equations

8.4 Fermat's Little Theorem

↪ **Theorem 8.2: Fermat's Little Theorem**

Let p be a prime number. Let $a \not\equiv 0 \mod p$ then

$$a^{p-1} \equiv 1 \mod p.$$

Remark 8.1. *This implies that, for every a, $a^p \equiv a \mod p$. Conversely, If $a \not\equiv 0 \mod p$, then $a^p \equiv a \mod p \implies a^{p-1} \equiv 1 \mod p$ by multiplying both sides with the congruence class b s.t. $ba \equiv 1 \mod p$.*

↪ **Lemma 8.4**

Let R be a commutative ring and $x, y \in R$. Interpret $\binom{n}{i}$ as adding 1 to itself $\binom{n}{i}$ times. Then, the binomial formula holds in R, ie

$$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}.$$

Ie, $\binom{n}{j}$ means $1_R + \cdots + 1_R$, $\binom{n}{j}$ times.

Proof. (Of lemma 8.4) We proceed by induction. Case $n = 1$, clear; $(x+y)^1 = x^1 + y^1 \checkmark$.
Assume it holds for n. We write

$$(x+y)^{n+1} = (x+y)^n(x+y) = \underbrace{\left(\sum_{j=0}^{n} \binom{n}{j} x^{n-j}y^j\right)}_{\text{assumption}} \cdot (x+y)$$
$$= \sum_{l=0}^{n+1} c_l x^{n+1-l} \cdot y^l$$

where $c_l = \underbrace{\binom{n}{l}}_{\text{from } \binom{n}{l} x^{n-l}y^l x} + \underbrace{\binom{n}{l-1}}_{\text{from } \binom{n}{l-1} x^{n-(l-1)}y^{l-1}y} = \binom{n+1}{l}$, hence $(x+y)^{n+1} = \sum_{l=0}^{n+1} \binom{n+1}{l} x^{n+1-l}y^l$.

∎

Proof. (Of Fermat's Little Theorem) We aim to show that $a^p \equiv a \mod p$ for any a. It is sufficient to show that it holds for $1 \le a \le p-1$.
We prove by induction on $1 \le a \le p-1$. $a = 1 \implies 1^p \equiv 1 \mod p$.

Suppose it holds for $1 \leq a \leq p-2$, and prove for $a+1$. Then, by lemma 8.4,

$$\begin{aligned}
(a+1)^p &= \sum_{i=0}^{p} \binom{p}{i} a^i && (1)\\
&\equiv a^p + \binom{p}{1} a^{p-1} + \binom{p}{2} a^{p-2} + \cdots + \binom{p}{p-1} a + 1 && (2)\\
&\equiv 1 + a^p \quad \text{(by lemma 8.3)} && (3)\\
&\equiv 1 + a \quad \text{by induction hypothesis} && (4)
\end{aligned}$$

Since $1+a \not\equiv 0 \mod p$, it has an inverse in $y \in \mathbb{F}_p$, $y(1+a) \equiv 1$. Then, $y(1+a)^p \equiv y(1+a) \equiv 1$. Also, $y(1+a)^p = y(1+a)(1+a)^{p-1} \equiv (1+a)^{p-1}$, hence $(1+a)^{p-1} \equiv 1$. ■

⊛ **Example 8.6: Application of Fermat's Little Theorem**

Calculate $2^{2023} \cdot 3^9 \mod 7$. Divide 2023 by $6 = 7 - 1 = p - 1$ with residue. $2023 = 6 \cdot 337 + 1$, and $9 = 1 \cdot 6 + 3$.
$2^{2023} \cdot 3^9 = 2(2^6)^{337} \cdot 3^6 \cdot 3^3$. By FLT, this is equivalent to $2(1)^{337} \cdot 1 \cdot 3^3 \equiv 2 \cdot 27 \equiv 54 \equiv 5 \mod 7$.

9 Arithmetic of Polynomials

9.1 Definitions

↪ **Definition 9.1: Polynomial Ring**

Let $\mathbb{F}$ be a field, and let $\mathbb{F}[x]$ be the ring of polynomials with coefficients in $\mathbb{F}$, ie

$$\mathbb{F}[x] = \{a_n x^n + \cdots a_1 x + a_0 : a_i \in \mathbb{F}\}.$$

Operations of addition, multiplication are defined as is familiar.

⊛ **Example 9.1**

$\mathbb{F} = \mathbb{Z}/3\mathbb{Z}$. We have

$$\begin{aligned}
(x^2+x+1)(2x+1) + 2x^2 + 5 &\equiv 2x^3 + \cancelto{0}{(1+2)}x^2 + \cancelto{0}{(1+2)}x + 1 + 2x^2 + 6\\
&\equiv 2x^3 + 2x^2 + \cancel{6} \mod 3
\end{aligned}$$

↪ **Definition 9.2:** deg

If $f = a_n x^n + \cdots a_1 x + a_0$ has $a_n \neq 0$, we say $\deg f = n$, unless $f = 0$, where $\deg f$ undefined.

If f, g not zero, then $\deg(f \cdot g) = \deg(f) + \deg(g)$; thus, if f, g are not zero, $f \cdot g \neq 0$. If $f \cdot g = 0$, we must have either that $f = 0$ or $g = 0$, or both. Thus, this is a commutative ring with no zero divisors.

↪ Theorem 9.1: Division with Residue

Let $f, g \in \mathbb{F}[x]$, $g \neq 0$. Then, $\exists!$ polynomials $g, r \in \mathbb{F}[x]$ s.t. $f = q \cdot g + r$, where either $r = 0$ or $\deg(r) < \deg(g)$; furthermore, q, r are unique.

Proof. If $f = 0$, then take $q = 0, r = 0$ (no other choice). Take $f \neq 0$ wlog. We first prove *existence* by induction on $\deg f$.

- *Base:* $\deg f = 0$: If $\deg g > 0$, let $q = 0$, $r = f$, hence $f = 0 \cdot g + f$. Otherwise, if $\deg g = 0$, then g is a constant, then $f = (fg^{-1}) \cdot g + 0$.
- *Assumption:* suppose true for all polynomials $h \in \mathbb{F}[x]$ such that $\deg h \leq n$ and $\deg f = n + 1$. Say $f = a_{n+1}x^{n+1}+$ l.o.t.[30], and $g = b_m x^m+$ l.o.t., where $b_m \neq 0$.
  - If $n + 1 < m$, then $f = 0 \cdot g + f$, $\deg f < \deg g$.
  - If $n + 1 \geq m$, then $f(x) = \underbrace{a_{n+1}b_m^{-1}x^{n+1-m}g}_{=a_{n+1}x^{n+1}+\text{ l.o.t}} + h(x)$, where h is essentially the "difference" between the expression. Note that $\deg h \leq n$; hence, by induction $h(x) = \tilde{q}(x) \cdot g(x) + r(x)$, where either $r(x) = 0$ or $\deg r < \deg g$. This implies that

$$f(x) = \underbrace{\left(a_{n+1}b_m^{-1}x^{n+1-m} + \tilde{q}(x)\right)}_{q(x)} g(x) + r(x).$$

Thus, the proof holds for all $\deg f$. We know show uniqueness. Suppose $f = q_1 g + r_1 = q_2 g + r_2$, where $r_i = 0$ or $\deg r_i < \deg g$. Consider

$$(q_1 - q_2)g = r_2 - r_1.$$

If RHS $\neq 0$, then the LHS $\neq 0$, hence $q_1 - q_2 \neq 0$. Since $g \neq 0$, then $\deg(\text{LHS}) = \deg(q_1 - q_2) + \deg g \geq \deg g$. But $\deg \text{RHS} \leq \max(\deg r_1, \deg r_2) < \deg g$, and we have a contradiction. Hence, RHS = 0 $\implies$ LHS = 0, hence $q_1 - q_2 = 0$, so $r_1 = r_2$, $q_1 = q_2$, and the polynomial is thus unique. ■

[30] Lower order terms

↪ Definition 9.3: Divisibility

We say $g | f$ if $r = 0$; namely,

$$f = q \cdot g \text{ for some } q \in \mathbb{F}[x].$$

As before, $g|f \implies g|hf$ for any $h \in \mathbb{F}[x]$; $g|f_1, g|f_2 \implies g|(f_1 \pm f_2)$; etc. Many of the other consequences of divisibility in integers follow similarly.

9.2 GCD

↪ Definition 9.4: GCD of Polynomials

Let $f, g \in \mathbb{F}[x]$ not both 0. The greatest common divisor of f, g denoted $\gcd(f, g)$ is a *monic* polynomial of largest degree dividing both f and g.

↪ Definition 9.5: Monic

$f = a_n x^n + \cdots + a_0$, $a_n \neq 0$ is *monic* if $a_n = 1$ (leading term is one).

↪ Theorem 9.2: GCD

$\gcd(f, g)$ exists and is unique. Furthermore, of the nonzero monic polynomials of the form

$$u(x)f(x) + v(x)g(x),$$

it has the minimal degree. Any common example of f, g divides the gcd.

Proof.

- *Existence:* Let $S := \{a(x) : a(x) \text{ monic, nonzero}; a(x) = u(x)f(x) + v(x)g(x).\}$. $S \neq \varnothing$; if $f \neq 0$, rather $f = a_n x^n +$ l.o.t., then $a(x) = a_n^{-2} f(x) \cdot f(x) + 0 \cdot g(x) \in S$ (if $f = 0$, use g by same argument). Choose some $h(x) \in S$ have the minimal positive degree.

- *Unique:* suppose $h_1(x) \in S$ and $\deg h = \deg h_1 = d$, $h = x^d + \text{lot} = uf + vg$, $h_1 = x^d + \log = u_1 f + v_1 g$. Now either:
  - $h - h_1 = 0$ (done)
  - $\deg(h - h_1) < \deg h$. However, $h - h_1 = (u - u_1)f + (v - v_1)g$. $h - h_1 = a_e x^e + \text{lot}$, then $ae^{-1}(h - h_1)$ is monic of $\deg < \deg h$, and is in S, a contradiction.

    Hence, h must be unique.

- $h|f, h|g$: Write

  $$f = q \cdot h + r.$$

  If $r = 0$, $h|f$. Else, $r = f - q \cdot h$, and thus $r \in S$, and we can write $r = f - q(uf + vg) = (f - qu)f - (qv)g$. Thus, after normalization (ie "divide out" to make monic), $r \in S$, and has a smaller degree then h, and we thus have a contradiction, and so $r = 0$. Thus, $h|f, h|g$.

- *Maximality of* $\deg(h)$*:* Suppose $t(x)|f, t(x)|g$, thus $t(x)|(uf + vg)$, so $t|h$. Thus, $\deg t \leq \deg h$, and further h has the maximal possible degree, hence h is the monic common divisor of max degree.

- *Uniqueness of GCD:* Say h_1 another common divisor of f, g of the same degree of h. We have that $\deg h = \deg h_1$ and $h_1 | h$, and further h, h_1 monic, then $h = h_1$.

■

↪ **Theorem 9.3: Euclidean Algorithm (Polynomials)**

Each

$$\begin{aligned} f &= q_0 \cdot g + r_0, \quad && r_0 = 0 \text{ or } \deg(r_0) < \deg(g) \\ g &= q_1 \cdot r_0 + r_1, \quad && r_1 = 0 \text{ or } \deg(r_1) < \deg(r_0) \\ r_0 &= q_2 \cdot r_1 + r_2 \quad && \cdots \\ &\vdots \\ r_{n-1} &= q_{n+1} r_n \end{aligned}$$

We have that r_n, once normalized, is the $\gcd(f, g)$ (ie if $r_n(x) = a_n x^n + \text{lot}$, we normalize by dividing by a_n).

Proof. ■

⊛ **Example 9.2**

$f = x^3 - x^2 + 2x - 2$, $g = x^2 - 4x + 3 \in \mathbb{Q}[x]$.

$$\begin{aligned} f &= (x^2 - 4x + 3)(x + 3) + (11x - 11) \\ x^2 - 4x + 3 &= (11x - 11)(\frac{1}{11}x - \frac{3}{11}) \end{aligned}$$

Hence, $\gcd(f, g) = \frac{1}{11}(11x - 11) = x - 1$. The same process follows to find u, v; we have $x - 1 = \frac{1}{11}(f - g(x + 3)) = \frac{1}{11} f - \frac{1}{11}(x + 3) g$.

⊛ **Example 9.3**

$\mathbb{F} = \mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z} = \{0, 1\}$ where $1+1 = 0$. Take $f = x^5 + x^3 + x^2 + x$, $g = x^3 + x^2 + x$.

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

Hence, $\gcd(f, g) = x$. We also have that $x = g - x^2(x + 1) = g - (f - (x^2 + x + 1)g)(x + 1) = g(1 + (x^2 + x + 1)(x + 1)) - (x + 1)f = g \cdot x^3 + f \cdot (x + 1)$

↪ **Lemma 9.1**

Let $f(x) \in \mathbb{F}[x]$ and $\alpha \in \mathbb{F}$ such that $f(\alpha) = 0$. Then, $(x - \alpha)|f(x)$

Proof. Divide with residue: $f(x) = q_0(x)(x - \alpha) + r$, st $r = 0$ or $\deg(r) < 1$. If $r = 0$, we are done. Now, substitute α; $0 = f(\alpha) = \underbrace{q(\alpha) \cdot (\alpha - \alpha)}_{=0} + r \implies r = 0$. ■

↪ **Corollary 9.1**

If f has $\deg n > 0$ and $f(\alpha_i) = 0$ for distinct $\alpha_1, \ldots, \alpha_n$, then $f = c \cdot \prod_{i=1}^{n}(x - \alpha_i)$. This implies that, if $\beta \neq \alpha_i$ for any i, then $f(\beta) \neq 0$. We can conclude that a polynomial of degree n has at most n distinct roots.

⊛ **Example 9.4**

Do the polynomials in $\mathbb{R}[x]$ $f = x^6 + x^4 - x^2 - 1, g = x^3 + 2x^2 + x + 2$ have a common solution? They do, iff $d = \gcd(f, g)$ has a real root. In this case, $\gcd(f, g) = x^2 + 1 = (x - i)(x + i)$, so f, g have no common real roots.

↪ **Definition 9.6: Associates**

Two nonzero polynomials $f, g \in \mathbb{F}[x]$ are called *associates* if $\exists \alpha \in \mathbb{F}, \alpha \neq 0$, st $\alpha f = g$ (we commonly denote $\mathbb{F}^{\times} = \mathbb{F} \setminus \{0\}$)

Remark 9.1. *Associate polynomials have the same degree.*

↪ **Lemma 9.2**

This is an equivalence relation and the representatives for the equivalence are the monic polynomials.

Proof. $f \sim f$, since $1 \cdot f = f$.
If $f \sim g$, we have $\alpha f = g \implies \frac{1}{\alpha} g = f \implies g \sim f$.
If $f \sim g, g \sim h$ ie $\alpha f = g$ and $\beta g = h$, then $(\alpha\beta)f = \beta g = h$, noting that $\alpha\beta \neq 0$. Thus, this is an equivalence relation.
If $f = a_n x^n + \text{lot}$, $a_n \neq 0$, then $\frac{1}{a_n} f \sim f$, and $\frac{a_n f}{=} x^n + \text{lot}$, a monic polynomial, hence any equivalence class has a representative which is a monic polynomial.
Further, if f, g monic and $\alpha f = g$, then $\alpha = 1$, hence $f = g$. ■

↪ **Definition 9.7: Irreducible Polynomial**

A non-constant polynomial f ($\deg f > 0$) is called *irreducible* if any $g|f$ satisfies g 1 (namely, a constant) or $g \sim f$ (namely, $g = \alpha f$ for some $\alpha \in \mathbb{F}^{\times}$).[31]

Remark 9.2. *If* $\deg f > 1$, $f(x)$ *irreducible* $\implies$ f *has no root in* $\mathbb{F}$*; if* $f(\alpha) = 0$*, then* $f(x) = (x - \alpha) f_1(x)$, $f_1(x) \in \mathbb{F}[x]$*, hence we have a non-trivial factorization since* $(x - \alpha) \not\sim 1, (x - \alpha) \not\sim f \implies f$ *reducible.*
The converse does not hold; consider $x^2 + 1, x^2 + 2 \in \mathbb{R}[x]$; $f(x) = (x^2 + 1)(x^2 + 2)$ *is reducible, clearly, but has no real root.*

Remark 9.3. *Any linear polynomial, of the form* $ax + b$ *where* $a \neq 0$*, is irreducible.*

Remark 9.4. *Irreducibility depends on the field in question, eg* $x^2 + 1$ *is irreducible in* $\mathbb{R}[x]$*, but* $x^2 + 1 = (x - i)(x + i)$*, so it is reducible in* $\mathbb{C}[x]$.

↪ **Proposition 9.1**

Suppose[32] $\deg f \geq 1$. The following are equivalent:

1. f irreducible;
2. $f|gh \implies f|g$ or $f|h$.

[31] This can be seen as an analog to primes; $p \in \mathbb{Z}$ prime if $m|p \implies m = \pm 1$ or $m = \pm p$. Irreducible polynomials are the "primes of the rings of polynomials."

[32] Recall lemma 7.3, in the integers

Proof. **1. $\implies$ 2.:** suppose f irreducible and $f|gh$. If $f \not| g$, then $\gcd(f, g) = 1$. Then, we can write

$$\begin{aligned} 1 &= uf + vg, \text{ some } u(x), v(x) \in \mathbb{F}[x] \\ \implies h &= \underbrace{ufh}_{f|} + \underbrace{vgh}_{f|} \implies f|h \end{aligned}$$

1. $\impliedby$ 2.: suppose $f = gh$, and say wlog $f|g$. So, $f|g$ and $g|f \implies \deg g = \deg f$ and so $g = f \cdot t$, and $\deg t$ must be 0, therefore t constant, and thus h must be constant ie $h \sim 1$, hence f irreducible. ■

↪ **Lemma 9.3**

Any non-zero polynomial $f \in \mathbb{F}[x]$ can be written as

$$f = c \cdot f_1 \cdot f_2 \cdots f_n,$$

where all $f_i \in \mathbb{F}[x]$ are irreducible, monic, and $c \in \mathbb{F}[x]$.

Proof. (By induction on $\deg f$)

- $\deg f = 0 \implies f$ constant ($f = f$)

- Suppose true for $0 \leq \deg g \leq n$ and let f be a polynomial of $\deg f = n + 1$.

  If f irreducible, $\exists c$ (leading coefficient, in fact) such that $f = c \cdot f_1$, with f_1 monic and irreducible (if $f \sim h$, then f irreducible $\iff$ h irreducible), and we are done.

  Else, $f = f_1 \cdot f_2$ is a non-trivial factorization ie $\deg(f_1) < \deg f, \deg f_2 < \deg f$ (neither scalars). We can write, $f_1 = c_1 p_1(x) \cdots p_a(x)$ and $f_2 = c_2 p_{a+1}(x) \cdots p_b(x)$, where each p_i irreducible and monic, by our assumption, hence $f = f_1 f_2 = (c_1 c_2) p_1 \cdots p_b(x)$, and our inductive step is done and thus the statement holds.

■

↪ **Theorem 9.4: Unique Factorization for Polynomials**

Let $f(x) \in \mathbb{F}[x]$ be a non-zero polynomial. Then, we have

$$f = c \cdot p_1(x)^{a_1} \cdots p_r(x)^{a_r}$$

where $c \in \mathbb{F}^\times, p_i(x)$ monic, distinct, irreducible polynomials, and $a_i > 0$. Moreover, c, $p_i(x)$'s, and a_i's are uniquely determined.

Remark 9.5. *Existence follows from lemma 9.3 by collecting like polynomials under a_i. It remains to prove uniqueness.*

Proof. Because $p_i(x)$ monic, leading coefficient of rhs c must be the leading coefficient of the lhs, ie c determined by f.
Suppose we have two decompositions, say

$$f = c \cdot p_1(x)^{a_1} \cdots p_r(x)^{a_r} = \tilde{c} \cdot q_1(x)^{b_1} \cdots q_s(x)^{b_s}.$$

We must have $c = \tilde{c}$. Then, $r = s$ and after renaming the q_i, we have that $q_i = p_i$ and $a_i = b_i$. We proceed by induction on $\deg f$.

- $\deg f = 0$: since we have irreducible polynomials which must have positive degree[33], hence the only option is $r = s = 0$, hence $f = c = \tilde{c}$.

- Suppose true for polynomials $h(x)$ such that $0 \leq \deg h \leq n$, and $\deg f = n + 1$. Note, first, that $r \geq 1$, $s \geq 1$ (else f constant). We have that

  $$p_1(x) | f = c \cdot q_1(x)^{b_1} \cdots q_s(x)^{b_s} \overset{\text{proposition 9.1}}{\Longrightarrow} \underbrace{p_1(x) | c}_{c \text{ const, not possible}} \quad \text{or } p_1(x) | q_i(x) \text{ for some } i.$$

  We have that $q_i(x)$ irreducible, so $p_1(x) \sim q_i(x)$, but they are both monic, so $p_1(x) = q_i(x)$. Rename, then, q_i as q_1, ie $p_1 = q_1$. This implies, then that $c \cdot p_1^{a_1 - 1} p_2^{a_2} \cdots p_r^{a_r} = c \cdot q_1^{b_1 - 1} q_2^{b_2} \cdots q_s^{b_s}$. Then, by induction, we can "rename" each of the q_i, if needed, hence $p_i = q_i \forall i$, and we are done.

■

[33] Analog to primes $\neq 0, \pm 1$

↪ **Theorem 9.5: Unique Factorization for Polynomials**

Let $f(x) \in \mathbb{F}[x]$ be a non-zero polynomial. There exists a unique $c \in \mathbb{F}^x$ and distinct, monic, irreducible polynomials $f_1(x), \ldots, f_r(x)$ with $r \geq 0$ and positive integers a_i s.t.

$$f(x) = c \cdot f_1(x)^{a_1} \cdots f_r(x)^{a_r}.$$

↪ **Corollary 9.2**

Let $f(x), g(x)$ be non-zero polynomials. Then, $f|g$ iff we can write

$$f(x) = cf_1(x)^{a'_1} \cdots f_r(x)^{a'_r}, g(x) = df_1(x)^{a_1} \cdots f_r(x)^{a_r}$$

where $c, d \in \mathbb{F}^x$, f_i are irreducible monic polynomials with $r \geq 0$, and $0 \leq a'_i \leq a_i, 0 < a_i$.

Proof. If we have such an expression, then $g = f \cdot h$ where $h = dc^{-1} \cdot f_1(x)^{a_1 - a'_1} \cdots f_r(x)^{a_r - a'_r}$ is a polynomial as $a_i - a'_i \geq 0$. Conversely, suppose $f|g$ so $g = fh$. Write

$$\begin{aligned} f &= c \cdot f_1(x)^{a'_1} \cdots f_s(x)^{a'_s}, c \in \mathbb{F}^x, a'_i > 0 \\ h &= e \cdot f_1(x)^{b_1} \cdots f_s(x)^{b_2} f_{sh}(x)^{a_{sh}} \cdots f_r(x)^{a_r} \\ \implies g &= (ce) \cdot f_1(x)^{a'_1 + b_1} \cdots f_s(x)^{a'_s + b_s} f_{s+1}(x)^{a_{sh}} \cdots f_r(x)^{a_r}, \end{aligned}$$

and let $d = c \cdot e$, $a_i = a'_i + b_i$ for $1 \leq i \leq s$. ■

↪ **Corollary 9.3: GCD, LCM**

If f, g are non-zero polynomials $f(x) = c \cdot f_1(x)^{a_1} \cdots f_r(x)^{a_r}, g = d \cdot f_1(x)^{b_1} \cdots f_r(x)^{b_r}$, $c, d \in \mathbb{F}^x, a_i \geq 0, b_i \geq 0$, f_i distinct monic irreducible. Then

$$\begin{aligned} \gcd(f, g) &= f_1^{\min(a_1, b_1)} \cdots f_r^{\min(a_r, b_r)} \\ \operatorname{lcm}(f, g) &= f_1^{\max(a_1, b_1)} \cdots f_r^{\max(a_r, b_r)} \end{aligned}$$

Remark 9.6. *How does one tell if a polynomial is irreducible?*

1. *Any linear polynomial* $ax + b, a \neq 0$ *is irreducible.*
2. *If* $f(x) \in \mathbb{F}[x]$ *has degree 2 or 3,* $f(x)$ *reducible iff* $f(x)$ *has a root in* $\mathbb{F}$*.*
3. *Over* $\mathbb{C}$*, the only irreducible polynomials are the linear polynomials (recall theorem 5.2)*
4. *Over* $\mathbb{R}$ *any irreducible polynomial has degree 1 or 2.* [34]
5. *Let* $f(x) \in \mathbb{Q}[x]$ *of degree* d*.*

[34] Show

(a) $d = 1$: $f(x)$ *irreducible*

(b) $d = 2, 3$: $f(x)$ *reducible* $\iff$ f *has a rational root.*

(c) $d > 3$: $f(x) reducible$ $\impliedby$ f *has a root.*

6. *Let* $\mathbb{F} = \mathbb{F}_p$ *where* p *prime. Let* $g(x) \in \mathbb{F}$ *be a non-constant polynomial. Then,* $g(x)$ *has a root in* $\mathbb{F}$ *iff* $\gcd(g, x^p - 1) \neq 1$.

While no general method exists to determine reducibility, there is a general method to determine existence of roots.

↪ **Proposition 9.2**

Let $f(x) = a_n x^n + \cdots + a_1 x + a_0$ be a non-constant polynomial with integer coefficients, $a_n \neq 0$. Let $f(\frac{a}{b}) = 0$ where $(a, b) = 1$. Then, $b|a_n$, $a|a_0$.

Proof. We have $\left(\frac{a}{b}\right)^n a_n + \left(\frac{a}{b}\right)^{n-1} a_{n-1} + \cdots + \left(\frac{a}{b}\right) a_1 + a_0 = 0$. Multiple by b_n to get

$$\underbrace{a^n \cdot a_n + \overbrace{a^{n-1} b a_{n-1} + \cdots + a b^{n-1} a_1}^{b|}}_{a|} + a_0 b^n = 0$$

Which implies

$$\begin{cases} a | a_0 b^n \implies a | a_0 \\ b | a^n a_n \implies b | a_n \end{cases}$$

■

↪ **Proposition 9.3**

$f(x) \in \mathbb{F}[x]$ has a root $a \in \mathbb{F} \iff (x - a)|f(x) \iff \gcd(f(x), x^p - x) \neq 1$. Further, $f(x) \in \mathbb{F}[x]$ has a non-zero root $a \in \mathbb{F}\backslash\{0\} \iff (x-a)|f(x) \iff \gcd(f(x), x^{p-1}-1) \neq 1$.

⊛ **Example 9.5**

Is -1 a square in $\mathbb{F}_{113}$? [35]

[35] Yes/No $\iff p \equiv_4 1, 3$

Proof. This is equivalent to asking is $x^2 + 1$ irred in $\mathbb{F}_{113} \iff \gcd(x^2 + 1, x^{112} - 1) \neq 1$.

$$x^{112} - 1 = (x^2 + 1)(x^{110} - x^{108} + x^{106} - \cdots + \underbrace{(-1)^{55}}_{\frac{p-3}{2}}) - (\underbrace{(-1)^{55}}_{\frac{p-3}{2}} + 1)$$

$$\implies (x^2 + 1)|x^{112} - 1 \implies \gcd(x^2 + 1, x^{112} - 1) = x^2 + 1$$

Hence, -1 is indeed a square ($-1 \equiv_{113} 15^2$, in fact). ■

10 Rings

10.1 Ideals

↪ **Definition 10.1: Ideal**

An *ideal* I of R is a subset of R such that

1. $0 \in I$;
2. $x, y \in I \implies x + y \in I$;
3. $x \in R, y \in I \implies xy \in I$.[36]

[36] Consider 2. to state that I closed under addition. 3. can be considered as a sort-of "absorption" quality; thinking about this in the more concrete case of $n\mathbb{Z}$ may make more sense. Think about this $x \cdot y$ as a "multiple" in a sense of y.

Remark 10.1. *Typically, $1 \notin I$. If $I = R$, then it is; if $1 \in I$, then $\forall r \in R, r \cdot = r \in I$, hence $I = R$ (by criterion (3)). In other words, ideals are typically* not *subrings.* [37]

[37] This is a direct result of our convention of requiring subrings to contain 1; many texts do not require subrings to contain the multiplicative elements, so in these cases ideals would then typically be subrings as well. We will not adopt this convention.

⊛ **Example 10.1**

We consider some trivial examples:

- $I = \{0\}$
- $I = R$.
- $R = \mathbb{F}$ a field, and $I \neq \{0\}$, then $I = R$. That is, any non-zero ideals of a field are trivial and generally uninteresting.

↪ **Definition 10.2: Principal Ideals**

Let $r \in R$ and let $(r) = \langle r \rangle := Rr = \{sr : s \in R\} = rR$. This is an ideal; $0 = 0 \cdot r$; $s_1 r + s_2 r = (s_1 + s_2) r \in I$; $s \cdot s_1 r = (s s_1) \cdot r \in I$.

⊛ **Example 10.2**

Any integer $m \in \mathbb{Z}$, $m\mathbb{Z}$ is an ideal of $\mathbb{Z}$.

↪ **Definition 10.3: Units of R**

Consider a commutative ring R. We denote

$$R^\times = \{u \in R : \exists v \in R \text{ with } uv = vu = 1\}$$

the *units* of R.

Remark 10.2. $1 \in R^{\times}$. *If* $u_1, u_2 \in R^{\times}$ *then* $u_1 u_2 \in R^{\times}$, *because* $\exists v_i$ *s.t.* $v_i u_i = 1$ *hence* $(v_2 v_1)(u_1 u_2) = v_2 \cancelto{1}{(v_1 u_1)}(u_2) = (v_2 u_2) = 1$. *That is, the product of units is a unit.*

⊛ **Example 10.3**

Consider the following examples of units:

- $\mathbb{Z}^{\times} = \{\pm 1\}$
- $R = \mathbb{F}$ then $\mathbb{F}^{\times} = \mathbb{F} \setminus \{0\}$.
- $\mathbb{F}[x]^{\times} = \mathbb{F}^{\times}$ (the degree of the units must be zero, hence they are simply the constants of the field.)
- $\mathbb{Z}[\sqrt{2}]^{\times} = \{a + b\sqrt{2} : a^2 - 2b^2 = \pm 1\}$[38]

[38] These (a, b) solve the *Pell Equations*, $x^2 - 2y^2 = \pm 1$

.

↪ **Definition 10.4: Associates**

Define $r_1, r_2 \in R$ as *associates* if there $\exists u \in R^{\times}$ s.t. $ur_1 = r_2$.[39]

[39] This is an extension of the previous definition of associates for polynomials to an arbitrary ring.

↪ **Proposition 10.1**

Take $r_1, r_2 \in R$. Then $r_1 \sim r_2$ is an equivalence relation.

Proof. ■

↪ **Lemma 10.1**

Let $r_1, r_2 \in R$. If $r_1 \sim r_2$ then $(r_1) = (r_2)$.

Remark 10.3. *The converse does not always hold; it holds if* R *is an* integral domain.

↪ **Definition 10.5: Integral Domain**

A ring R is an *integral domain* if $xy = 0 \implies x = 0$ or $y = 0$.

Proof. Say $ur_1 = r_2$; then $(r_2) = Rr_2 = Rur_1 = (Ru) \cdot r_1 \subseteq R \cdot r_1 = (r_1)$. Then, $r_1 \sim r_2 \implies (r_2) \subseteq (r_1)$. Equivalence relation $\implies$ symmetric, hence $r_2 \sim r_1 \implies (r_1) \subseteq (r_2)$, hence we have equality.
We consider the converse; $(r) = (s) \implies r \sim s$. $r \in (r) = (s) \implies r = us$ for some $u \in R$, and $s \in (r) \implies s = vr$ for some $v \in R$. This implies then that

$$(1 - uv) \cdot r = 0.$$

This gives two possibilities: $r = 0 \implies s = vr = 0$, or $r \neq 0 \implies 1 - uv = 0 \implies uv = 1 \implies u, v$ units, hence $r = u \cdot s \implies r \sim s$ by definition. This holds only if the ring is an integral domain. ■

↪ **Theorem 10.1**

Every ideal of $\mathbb{Z}$ is of the form $\langle m \rangle = m \cdot \mathbb{Z}$ for a unique non-negative integer m which implies the ideals of $\mathbb{Z}$ are all principal and are exactly

$$(0) = \{0\}, (1) = \mathbb{Z}, (2) = 2\mathbb{Z}, (3) = 3\mathbb{Z}, (4) = 4\mathbb{Z}, \ldots$$

Proof. If[40] $I \lhd \mathbb{Z}$, if $I = \{0\}$ then $I = (0)$. If $I \neq \{0\}$, $\exists$ some $m \neq 0$ such that $m \in I$ and then also $-m = -1 \cdot m \in I \implies I$ contains a positive integer. Let $n \in I$ be the minimal positive element belonging to I. We claim that $I = (n)$.
On the one hand, $n \in I \implies kn \in I \forall k \in \mathbb{Z} \implies (n) \subseteq I$. Conversely, let $t \in I$, and write

$$t = kn + r, 0 \leq r < n.$$

If $r \neq 0$, note that $r = t - kn$, and since both t and $n \implies -kn \in I$, then it must be that $r \in I$. But $r < n$, hence we have a contradiction, and it must be that $r = 0 \implies t = kn \in (n) \implies I \subseteq (n)$. ■

[40] The symbol $I \lhd R$ denotes I is a principal ideal of R

↪ **Theorem 10.2**

[41] Let $I \lhd \mathbb{F}[x]$, $\mathbb{F}$ a field. Then, $I = (0)$ or $I = (f)$ for a unique monic polynomial f. Moreover, if $f \neq g$ are monic polynomials, then $(f) \neq (g)$.

[41] This proof follows almost precisely from the logic of the previous proof.

Proof. If $I = \{0\}$ then $I = (0)$. Else, $\exists f \in I, f \neq 0$. Then, for a suitable $\alpha \in \mathbb{F}^{\times}$, then αf monic, and it must be that $\alpha f \in I$. This implies that I contains some monic polynomial.
Let $g \in I$ be a monic polynomial of minimal degree among all nonzero polynomials of I. Note that $(g) = \mathbb{F}[x] \cdot g \subseteq I$. Let $h \in I$ and divide h by g with residue. Then, we have

$$h = q \cdot g + r, r = 0 \text{ or } \deg(r) < \deg(g).$$

Note that $r = h - qg$ where $h \in I$ and $q \cdot g \in I$, hence if $r =\neq 0$, then $\deg(r) < \deg(g)$ and we found a smaller degree polynomial in the ideal and we have a contradiction of our choice of g. So, we must have

$$r = 0 \implies h = q \cdot g \implies h \in (g) \implies I \subseteq (g).$$

It remains to show that f, g monic and $(f) = (g) \implies f = g$. We have that $(f) = (g) \implies f \sim g$, as $\mathbb{F}[x]$ is an integral domain (lemma 10.1), so we can write $f = u \cdot g$ for some $u \in$

$\mathbb{F}[x] = \mathbb{F}^\times = \mathbb{F} - \{0\}$, which implies

$$f = u \cdot g \implies x^n + \text{l.o.t.} = u \cdot (x^n + \text{l.o.t}) \implies u = 1 \implies f = g.$$

■

⊛ **Example 10.4**

Consider $x \in \mathbb{F}[x]$, and the ideal

$$\begin{aligned}(x) &= \{a_n x^n + \cdots + a_1 x \cancel{+ a_0} : a_i \in \mathbb{F}, a_0 = 0\} \\ &= \{f \in \mathbb{F}[x] : f(0) = 0\}\end{aligned}$$

⊛ **Example 10.5**

$I = \{f \in \mathbb{F}[x] : f(0) = 0, f(1) = 0\}$. Show that I is an ideal, and that $I = (x \cdot (x - 1))$.

↪ **Definition 10.6: Generalized Way to Create Ideals**

Let $r_1, \ldots, r_n$ be elements of a ring R. We write

$$\begin{aligned}\langle r_1, \ldots, r_n \rangle &:= Rr_1 + Rr_2 + \cdots + Rr_n \\ &= \{\sum_{i=1}^n s_i r_i : s_i \in R\}\end{aligned}$$

For instance, $r_1 = 1 \cot r_1 + 0 \cdot r_2 + \cdots + 0 \cdot r_n \in \langle r_1, \ldots, r_n \rangle$. We call this ideal the "generalize ideal"; call it $I = \langle r_1, \ldots, r_n \rangle$. We show that it is indeed an ideal below.

Proof.

$$\begin{aligned}(1) \quad 0 = 0 \cdot r_1 + \cdots + 0 \cdot r_n \in I \\ (2) \quad \sum_{i=1}^n s_i r_i + \sum_i^n r_i r_i \\ = \sum^n (s_i + t_i) r_i \in I \\ (3) \quad s \cdots \sum s_i r_i = \sum (s s_i) r_i \in I\end{aligned}$$

■

⊛ **Example 10.6**

Let m, n be nonzero integers. Then, we can write $\langle m, n \rangle = \langle \gcd(m, n) \rangle$.

⊛ **Example** **10.7**

Let $R = \mathbb{C}[x, y] = \{\sum_{i,j=0}^{N} a_{ij} x^i y^j : a_{ij}\}$. An ideal would be

$$I = \langle x, y\rangle = \{f(x, y) : f \text{ has no constant term, ie } a_{00} = 0\}$$

This is because if $f \in$ LHS, then $f = f_1 \cdot x + f_2 \cdot y$, $f_1, f_2 \in \mathbb{C}[x, y]$ (noting that it has no constant term), and conversely, if $f \in$ RHS, it does not have a constant term either, that is, $f = \sum a_{i,j} x^i y^j$ with $a_{00} = 0$, so we can write $f = x \cdot \sum_{i\geq 1,j} a_{ij} x^{j-1} y^j + y \sum_{i=0,j} a_{ij} x^i y^{j-1}$; $i = 0 \implies j \geq 1$, and thus have "x times something plus y times something" and hence $f \in I$. We can equivalently write

$$I = \{f(x, y) \in \mathbb{C}[x, y] : f(0, 0) = 0\}.$$

Note that this ideal is *not* a principal ideal, that is, $\nexists$ polynomial $f(x, y)$ s.t. $\langle x, y\rangle = \langle f(x, y)\rangle$.

10.2 Homomorphism

↪ **Definition** **10.7: Homomorphism**

Let R, S be commutative rings.[42] A function $f : R \to S$ is called a *ring homomorphism* if[43]

1. $f(1_R) = 1_S$ *(identity)*
2. $f(x + y) = f(x) + f(y)$ *(respects addition)*
3. $f(xy) = f(x)f(y)$ *(respects multiplication)*

$\forall x, y \in R$.

↪ **Proposition** **10.2**

These axioms imply the following consequences:

(i) $f(0_R) = 0_S$

(ii) $-f(x) = f(-x)$

(iii) $f(x - y) = f(x) - f(y)$

Proof. (i) $f(0_R) = f(0_R + 0_R) = f(0_R) + f(0_R)$. Adding $-f(0_R)$ to both sides, we get $0_S = f(0_R)$.

[43] Throughout this section, references to arbitrary sets R, S may be made. It is safe to assume that these are rings even if not explicitly stated.

[43] Note the "preservation" of the properties of rings each requirement necessitates.

(ii) We will aim to show that $f(x) + f(-x) = 0_S$, equivalently. We have

$$\begin{aligned} f(x) + f(-x) &= f(x + (-x)) \quad \text{by axiom 2} \\ &= f(0_R) = 0_S \quad \text{by (1)} \end{aligned}$$

as desired.
(iii) $f(x - y) = f(x + (-y)) = f(x) + f(-y) = f(x) + (-f(y)) = f(x) - f(y)$. ■

↪ Proposition 10.3

$\mathrm{Im}(f) = \{f(r) : r \in R\}$ is a subring of S.

Remark 10.4. *We need to check the following (ring axioms):*

(i) $0, 1 \in \mathrm{Im}(f)$

(ii) $x_1, x_2 \in \mathrm{Im}(f) \implies x_1 + x_2 \in \mathrm{Im}(f)$

(iii) $x_1, x_2 \in \mathrm{Im}(f) \implies x_1 \cdot x_2 \in \mathrm{Im}(f)$

(iv) $x \in \mathrm{Im}(f) \implies -x \in \mathrm{Im}(f)$

Proof. (i) $f(0_R) = 0_S, f(1_R) = 1_S$, by the previous proposition and by definition resp.

(ii), (iii) Say $x_i = f(r_i)$; then $x_1 \overset{+}{\times} x_2 = f(r_1) \overset{+}{\times} f(r_2) = f(r_1 \overset{+}{\times} r_2) \in \mathrm{Im}(f)$

(iv) If $x = f(r), -x = -f(r) = f(-r) \in \mathrm{Im}(f)$, from the previous proposition.

■

↪ Definition 10.8: Kernel

Let $f : R \to S$ be a homomorphism. The *kernel* of f is defined as

$$\ker F := \{r \in R : f(r) = 0_S\} \equiv f^{-1}(0).$$

↪ Proposition 10.4

The following propositions relate to the kernel of a homomorphism:

(i) $\ker(f) \triangleleft R$

(ii) f injective $\iff \ker(f) = \{0_R\}$

(iii) $f(x) = f(y) \iff x - y \in \ker(f)$

Remark 10.5. *To show that some* $t \in \ker(f)$*, we need only to show that* $f(t) = 0_S$.

Proof. (i) We show each axiom: $f(0_R) = 0_S \in \ker(f)$; $x, y \in \ker(f) \implies f(x) + f(y) = 0_S + 0_S = 0_S$; $f(rx) = f(r)f(x) = f(r) \cdot 0_S = 0_S$.

(ii) Suppose f injective. Then, 0_R is the unique element mapping to 0_S, by definition of an injective function. Hence, $\ker f = \{0_R\} = (0_R)$. Conversely, suppose $\ker f = \{0_R\}$ and that $f(x) = f(y)$. Note that $f(x-y) = f(x) - f(y) = f(x) - f(x) = 0_S \implies x - y \in \ker(f) \implies x - y = 0_R \implies x = y$.

(iii) $f(x) = f(y) \iff f(x) - f(y) = 0_S \iff f(x-y) = 0_S \iff x - y \in \ker(f)$.

■

↪ Corollary 10.1

Let $s \in S$ and let $f^{-1}(s) = \{r \in R : f(r) = s\}$. Then, either $f^{-1}(s) = \varnothing$, or $f^{-1}(s) = x + \ker(f) = \{x + r : r \in \ker(f)\} \subseteq R$ for any x s.t. $f(x) = s$.

Proof. If $f^{-1}(s) \neq \varnothing$, $\exists x \in R$ s.t. $f(x) = s$. If $x + r \in x + \ker R$, then $f(x+r) = f(x) + f(r) = s + 0_S = s$. Hence, $f^{-1}(s) \supseteq x + \ker(f)$.

Suppose $y \in f^{-1}(s) \implies f(x) = f(y) = s$. This implies $r = y - x \in \ker f$ (by previous proposition). Note that $x + r = y$; hence $y \in x + \ker(f) \implies f^{-1}(s) \subseteq x + \ker(f)$. ■

⊛ Example 10.8

$R = \mathbb{Z}$, $S = \mathbb{Z}/n\mathbb{Z}$ where $n \geq 1 \in \mathbb{Z}$. Take $f : R \to S$ where $f(a) = a \mod n = \bar{a}$. This is a ring homomorphism:

- $f(1) \equiv_n 1$, the identity of $\mathbb{Z}/n\mathbb{Z}$.
- $\overline{a+b} = \bar{a} + \bar{b}$.
- $\overline{ab} = \bar{a} \cdot \bar{b}$.

This is surjective, hence $\mathrm{Im}(f) = \mathbb{Z}/n\mathbb{Z}$. We have that $\ker(f) = \{a \in \mathbb{Z} : \bar{a} \equiv_n 0\} = (n) = n\mathbb{Z}$.

Now what is $f^{-1}(\bar{1})$? Take some $x \in \mathbb{Z}$. $f(x) = \overline{x} = \bar{1}$; take $x = 1$, then $f^{-1}(1) = 1 + n\mathbb{Z}$. Generally, then, we have $f^{-1}(\overline{r}) = r + n\mathbb{Z}$.

⊛ Example 10.9

Let $\mathbb{F}$ be a field and $b \in \mathbb{F}$ a fixed element. $\varphi : \mathbb{F}[x] \to \mathbb{F}$, where $\varphi(f(x)) = f(b)$. So, $f(x) = a_n x^n + \cdots + a_1 x + a_0$, $\varphi(f(x)) = a_n b^n + \cdots + a_1 b + a_0$. This is a ring homomorphism.

- $f(1) = 1$

We have too that φ is surjective; given $c \in \mathbb{F}$, we can show that $\varphi(x + (c - b)) = b + (c - b) = c$.

$\ker \varphi = (x - b)$

⊛ **Example 10.10**

Let R, S be rings. Then, $R \times S$ is a ring.

⊛ **Example 10.11**

Consider the map

$$R \to R \times S, \quad r \mapsto (r, 0).$$

This is *not* a ring homomorphism since $f(1) = (1, 0) \neq (1, 1)$ (that is, unless $0_s = 1_s$, that is, S is the zero ring).

OTOH, take

$$\varphi : R \times S \to R, \quad (r, s) \mapsto r$$
$$\psi : R \times S \to S, \quad (r, s) \mapsto s$$

These are indeed ring homomorphisms.

We also have

$$\ker \varphi = \{0\} \times S, \ker \psi = R \times \{0\}.$$

⊛ **Example 10.12**

Take a polynomial in $\mathbb{R}[x]$ and fix $\alpha_1 < \alpha_2 < \cdots < \alpha_n \in \mathbb{R}$. Take

$$\varphi : \mathbb{R}[x] \mapsto \mathbb{R}^n, \quad f(x) \mapsto (f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_n)).$$

This is a homomorphism. We also have that φ is surjective. Let

$$e_i = \cdots (0, \ldots, 0, 1, 0, \ldots, 0),$$

ie a unit vector where the ith entry is 1. Take

$$f_i(x) = \prod_{j=1, j \neq i}^{n} (x - \alpha_j) / \prod_{j=1, j \neq i}^{n} (\alpha_i - \alpha_j).$$

Note that $f_i(\alpha_i) = 1$ and 0 for all other α_j, and thus $\varphi(f_i) = e_i$. Further, $\varphi(r_1 f_1 + \cdots + r_n f_n) = \sum_{i=1}^n \varphi(r_i f_i) = \sum_{i=1}^n \varphi(r_i)\varphi(f_i) = \sum_{i=1}^n r_i e_i = (r_1, \ldots, r_n)$, hence φ

surjective.

Finally, we have that $\ker \varphi = \langle \prod_{i=1}^{n} (x - \alpha_i) \rangle$.

10.3 Cosets

↪ Definition 10.9: Coset

Let R be a ring and $I \triangleleft R$. A *coset* of I is a subset of R of the form

$$a + I = \{a + i : i \in I\},$$

where $a \in R$.

Remark 10.6. *Note that the coset, while defined with respect to I, need not be a subset of I, but is by definition a subset of the ring R.*

↪ Definition 10.10: Relation on Cosets

Let R be a commutative ring and $I \triangleleft R$. Define a relation on R as $x \sim y$ if $x - y \in I$.

↪ Lemma 10.2

The following relate to relation defined previously.

1. This is an equivalence relation.
2. Every equivalence class is of the form $x + I$, where $x + I$ is called a *coset* of I, for some $x \in R$.
3. $x + I = y + I \iff x - y \in I$.
4. Either $(x + I) \cap (y + I) = \varnothing$ or $x + I = y + I$.

Proof.

1. (i) $x \sim x \impliedby x - x = 0$. $x - x = 0 \in I$ by definition. (ii) $x \sim y \implies x - y \in I \implies -1(x - y) \in I \implies y - x \in I \implies y \sim x$, again by definition. (iii) $x \sim y$, $y \sim z \implies x - y, y - z \in I \implies x - y + y - z \in I \implies x - z \in I \implies x \sim z$, as the ideal is closed under addition, hence $\sim$ is an equivalence relation.
2. $x + I = \{x + t : t \in I\} \subseteq R$. Suppose $y \in x + I$, then $y = x + t$ then $x - y = x - (x + t) = -1 \cdot t \in I$. That is, $x \sim y$. Suppose $y \sim x$. Then, $y - x =: t \in I \implies y = x + (y - x) = x + t \in x + I \implies$ equivalence class of x is $x + I$.
3. This is equivalent to saying the equivalence class of x is the equivalence class of y iff $x \sim y$, which follows by definition.

4. Follows by the fact that equivalence classes partition the set they are defined on (recall theorem 4.1).

■

⊛ **Example 10.13**

Say $R = \mathbb{Z}, I = n\mathbb{Z}$. Then, the cosets are just the congruence classes $(n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}) \mod n$.

10.4 Quotient Rings: The Ring R/I

↪ **Definition 10.11: Quotient Ring**

Consider [44] R/I. We define operations as

$$(x+I) + (y+I) := (x+y) + I, \quad (x+I)\cdot(y+I) := (x \cdot y) + I.$$

Equivalently, letting $\overline{x} = x + I$, we write

$$\overline{x} + \overline{y} = \overline{x+y}, \quad \overline{x} \cdot \overline{y} = \overline{x \cdot y}.$$

[44] Recall how we defined the elements of the ring $\mathbb{Z}/n\mathbb{Z}$. This can be seen as a generalization of this idea; read "R" mod "I".

Remark 10.7. *By this definition, we can see that every element of R/I is a coset, that is, of the form $x + I$; this is not unique, however, as it is possible that $x + I = y + I$ despite $x \neq y$.*

↪ **Theorem 10.3: R/I is a Commutative Ring**

$R/I = \{\overline{x} : x \in R\}$ is a commutative ring, where $0 = \overline{0} = I, 1 = \overline{1} = 1 + I$. Moreover, the function

$$\pi : R \to R/I, \quad x \mapsto \overline{x},$$

is a surjective ring homomorphism with $\ker \pi = I$.

↪ **Corollary 10.2**

Any[45] ideal is the kernel of some ring homomorphism.

[45] Direct consequence of theorem 10.3

Proof. (Of theorem 10.3) We first sow that the operations are well defined, that is, if $\bar{x} = \bar{x}_1, \bar{y} = \bar{y}_1$, then $\overline{x+y} = \overline{x_1 + y_1}$, and $\overline{x} \cdot \overline{y} = \overline{x_1 \cdot y_1}$. [46] We have, then,

$$x - x_1 \in I, y - y_1 \in I \implies (x+y) - (x_1 + y_1) = \underbrace{(x - x_1)}_{\in I} + \underbrace{(y - y_1)}_{\in I} \in I$$

$$xy - x_1 y_1 = \underbrace{x}_{\in R}\underbrace{(y - y_1)}_{\in I} + \underbrace{y_1}_{\in R}\underbrace{(x - x_1)}_{\in I} \in I,$$

hence the operations are well defined. We now verify (some of) the ring axioms:

[46] For instance, in $\mathbb{Z}/8\mathbb{Z}$, we have that $\overline{3} + \overline{10} = \overline{3+10} = \overline{13} = \overline{5}$, which is equivalent to saying $\overline{3} + \overline{2} = \overline{3+2} = \overline{5}$. We aim to show this holds for general R/I.

1. $\overline{x}+\overline{y}=\overline{x+y}=\overline{y+x}=\overline{y}+\overline{x}$

2. $\overline{0}+\overline{x}=\overline{0+x}=\overline{x}$

3. $\overline{x}+(\overline{-x})=\overline{x+(-x)}=\overline{0} \implies \overline{x}$ has an inverse for addition, $-\overline{x}=\overline{-x}$

4. $\cdots$

5. $\cdots$

6. $\cdots$

7. $\cdots$

8. $\overline{x}(\overline{y}+\overline{z})=\overline{x}\cdot\overline{x+y}=\overline{x(y+z)}=\overline{xy+yz}=\overline{xy}+\overline{xz}=\overline{x}\cdot\overline{y}+\overline{x}\cdot\overline{z}$,

hence, it is a commutative ring.

Now consider the map $\pi : R \to R/I, \pi(x)=\overline{x}$. We verify it is indeed a ring homomorphism:

1. $\pi(1)=\overline{1}=1_{R/I}$

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

3. $\pi(x\cdot y)=\overline{x\cdot y}=\overline{x}\cdot\overline{y}=\pi(x)\cdot\pi(y)$

Hence, π is indeed a ring homomorphism. Its kernel is:

$$\ker(\pi)=\{x\in R:\pi(x)=\overline{0}\}=\{x\in R:x+I=0+I=I\}=\{x\in R:x\sim 0\}=\{x\in R:x\in I\}=I.$$

■

⊛ **Example 10.14: Of R/I's**

1. $R=\mathbb{Z}, I=n\mathbb{Z}, a+n\mathbb{Z}=\overline{a}=a \mod n$, that is, this is modular arithmetic on the integers. The homomorphism is $\mathbb{Z}\to\mathbb{Z}/n\mathbb{Z}, a\mapsto\overline{a}$, which has a kernel of $n\mathbb{Z}$.

2. $R=\mathbb{F}[x], I=\langle f(x)\rangle, f(x)$ monic, non-constant polynomial. (We have that $\langle f(x)\rangle=\langle\alpha f(x)\rangle\forall\alpha\in\mathbb{F}^\times$, so monic wlog; a constant polynomial $f=\alpha,\alpha\in\mathbb{F}^\times$ would have $I=\mathbb{F}[x]$ so $R/I=\{0\}$, an uninteresting case, so we require non-constant f.)

   In this context, $g(x)\sim h(x) \iff g(x)-f(x)\in\langle f(x)\rangle \iff f(x)|(g(x)-h(x))$, that is, $\overline{g}=\overline{h} \iff f|(g-h)$.

⊛ **Example 10.15**

Consider $\mathbb{R}[x]/\langle x^2+1\rangle$. We claim that $\overline{a_1+b_1x} = \overline{a_2+b_2x} \implies a_1 = a_2, b_1 = b_2$. We can check:

$$\overline{a_1+b_1x} = \overline{a_2+b_2x} \iff (x^2+1)|(a_1-a_2)+(b_1-b_2)x,$$

but this is impossible, since the RHS is linear and the LHS is quadratic, *unless* the RHS is 0, hence, that $a_1 - a_2 = 0 \iff a_1 = a_2$ and $b_1 - b_2 = 0 \iff b_1 = b_2$, as desired.

Further, we claim that any coset is represented by some $a+bx$. Suppose $\overline{g}$ a coset. Then,

$$\begin{aligned} g = q\cdot(x^2+1)+r(x), \quad &, r(x) = 0 \text{ or } \deg(r(x)) < 2 \\ \implies r(x) = a, a\in\mathbb{R} &\text{ or } r(x) = a+bx, a,b\in\mathbb{R} \\ &\implies r(x) = a+bx, a,b\in\mathbb{R}, \end{aligned}$$

that is, $r(x)$ can be written as $a+bx$ for a,b in the field or zero. Hence, we have $g(x)-r(x) = q\cdot(x^2+1)$, and since $(x^2+1)|q\cdot(x^2+1)$, then $g(x)\sim r(x) \implies \overline{g} = \overline{r}$. Hence, we can conclude that every element of $\mathbb{R}[x]/\langle x^2+1\rangle$ is of the form $\overline{a+bx}$, $a,b\in\mathbb{R}$, for unique a,b.

Operations in this case would work as:

$$\begin{aligned} \overline{a_1+b_1x}+\overline{a_2+b_2x} &= \overline{(a_1+a_2)+(b_1+b_2)x} \\ \overline{a_1+b_1x}\cdot\overline{a_2+b_2x} &= \overline{(a_1+b_1x)(a_2+b_2x)} = \overline{a_1a_2+(a_1b_2+a_2b_1)x+b_1b_2x^2} \end{aligned}$$

But note that $x^2 = (x^2+1)-1 \implies \overline{x^2} = \overline{-1}$, so $b_1b_2x^2 = -b_1b_2$, so this simplifies to

$$\overline{a_1a_2+(a_1b_2+a_2b_1)x-b_1b_2} = \overline{(a_1a_2-b_1b_2)+(a_1b_2+a_2b_1)x}.$$

But note the similarity to multiplication in $\mathbb{C}$. In this way, we can define a bijection[47]

$$\mathbb{R}[x]/(x^2+1)\cong\mathbb{C}, \quad a+bi\mapsto\overline{a+bx}.$$

[47]Note that $A\cong B$ means that A is *isomorphic* to B.

Remark 10.8. *This concept works generally.*

↪ **Lemma 10.3**

Suppose $n = \deg(f)\geq 1$. Then, a complete set of representatives for the cosets is

$$\circledast = \{g(x) : \deg g < n\} = \{b_{n-1}x^{n-1}+\cdots+b_0 : b_i\in\mathbb{F}\}.$$

Proof. Take $h(x)\in\mathbb{F}[x]$, and write $h(x) = q(x)f(x)+r(x)$, where either $r(x) = 0$ or $\deg r < n$. Then, $h(x)-r(x) = q(x)f(x)\in I \implies h(x)+I = r(x)+I$ (that is, h and r are $\sim$). So, any coset is represented as an element of $\circledast$. It remains to show that this holds for any coset, that is, if $g_1, g_2 \in \circledast$ and $g_1 + I = g_2 + I \implies g_1 = g_2$. We have that $g_1 - g_2 \in I = f(x) \cdot \mathbb{F}[x]$ for any nonzero f, $\deg f \leq n$. Moreover, $\deg(g_1 - g_2) < n$, hence, $g_1 = g_2$. ■

⊛ Example 10.16

Take $f(x) = x^2 + 1$; here, $\circledast = \{ax + b : a, b \in \mathbb{F}\}$.

Remark 10.9. *Consider the analog to integer modular arithmetic. For addition, we have that* $\overline{g_1} + \overline{g_2} = \overline{g_1 + g_2}, \deg g_1 + g_2 < n$. *For multiplication, we have* $\overline{g_1} \cdot \overline{g_2} = \overline{g_1 g_2}$. *But now,*$\deg g_1 g_2$ *is potentially* $\geq n$*, so we write* $\overline{g_1 g_2} = \overline{r}$*, where* r *the residue of dividing* $g_1 g_2$ *by* f *(which then must have degree* $< n$*).*

↪ Theorem 10.4

Let $\mathbb{F}$ be a field. Let $f(x) \in \mathbb{F}$ be a non-constant irreducible polynomial. Then, $R = \mathbb{F}[x]/(f(x))$ is a field *containing* $\mathbb{F}$.

Moreover, if $\#\mathbb{F} = q, \deg(f) = n$, then $\#R = q^n$.

⊛ Example 10.17

Take, $\mathbb{F}_2$, and consider $\mathbb{F}[x]/(x^2 + x + 1)$; this is a field with 4 elements. Namely, they are $0, 1, x, 1 + x$; these are the only polynomials of $\deg < 2$ with coefficients in $\mathbb{F}_2$. We can write operations in the field:

$$\text{(Addition)} \quad \begin{array}{c|cccc} + & 0 & 1 & x & 1+x \\ \hline 0 & 0 & 1 & x & x+1 \\ 1 & 1 & 0 & x+1 & x \\ x & x & x+1 & 0 & 1 \\ 1+x & x+1 & x & 1 & 0 \end{array}$$

$$\text{(Multiplication)} \quad \begin{array}{c|cccc} \cdot & 0 & 1 & x & x+1 \\ \hline 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & x & x+1 \\ x & 0 & x & x+1 & 1 \\ x+1 & 0 & x+1 & 1 & x \end{array}$$

Proof. (Of theorem 10.4) We have shown previously that $\mathbb{F}[x]/I$ a commutative ring; further, $\overline{0} \neq \overline{1}$, because of the set $\circledast$ above. Hence it remains to show that there exists inverses.[48]

Let $\overline{g} \in \mathbb{F}[x]/(f(x)), \overline{g} \neq \overline{0}$, that is, $f \not| g$. This implies, moreover, that $\gcd(f, g) = 1$, since f irreducible (the divisors of f are thus 1 and f; f does not divide g as shown, hence the $\gcd$ is 1). This implies that $\exists u(x), v(x) \in \mathbb{F}[x]$ s.t. $1 = u(x)f(x) + v(x)g(x) \implies \overline{1} = \overline{u(x)f(x)} + \overline{v(x)g(x)}$. But $u(x)f(x)$ a multiple of $f(x)$ hence $\in I \implies \overline{u(x)f(x)} \in \overline{0} \implies$

$\overline{1} = \overline{0} + \overline{v(x)g(x)} \implies \overline{v(x)g(x)} = \overline{1}$, that is, $v(x)$ is the inverse wrt multiplication of $g(x)$, as desired.

■

[48] Note the similarities to proving that $\mathbb{Z}/p\mathbb{Z}$ where p prime a field; that is, yet again, primes in $\mathbb{Z}$ are analogous to irreducible polynomials in $\mathbb{F}[x]$.

⊛ **Example 10.18**

We construct a field with 25 elements. Take $\mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z}$ and $f(x) = x^2 - 2$ (irreducible $\mod 5$). Take $\mathbb{L} = \mathbb{F}_5[x]/(x^2-2)$, which is then a field with 25 elements by theorem 10.4, spec, of the form $\{a + bx : a, b \in \mathbb{F}_5\}$.

Remark 10.10. *The polynomial $t^2 - 2$ is irreducible in $\mathbb{F}_5$, but it actually has a root in $\mathbb{L}$ as defined above. Namely, the root is x ($\overline{x}$). To check: $\overline{x}^2 - \overline{2} = \overline{x^2 - 2} = \overline{0}$.*[49]

[49] "You're not being cheated, its a tautology."

Remark 10.11. *We could have defined $\tilde{\mathbb{L}} = \mathbb{F}_5[x]/(x^2-3)$; these are isomorphic fields, that is, $\tilde{\mathbb{L}} \cong \mathbb{L}$. Moreover, we have that $t^2 - 3$ has a root in $\tilde{\mathbb{L}}$, so it must have a root in $\mathbb{L}$ as well.*

Take $(ax+b) \in \mathbb{L}$. We want that $(ax+b)^2 = 3$. That is,

$$\begin{aligned}(ax+b)^2 &= a^2x^2 + 2abx + b^2 \\ &= 2a^2 + 2abx + b^2 \\ = 2abx + (b^2 + 2a^2) = 3 &\implies a = 0 \text{ or } b = 0\end{aligned}$$

In the case $a = 0$, we have that $b^2 = 3 \implies 3$ a square, which is not true in $\mathbb{F}_5$. Taking $b = 0$, then, we have $2a^2 = 3 \implies a = \pm 2$. We can verify:

$$\overline{3} = (\overline{2}\overline{x})^2 \in \mathbb{L}.$$

Remark 10.12. *L contains $\mathbb{F}$ is not very precise; more specifically, we have that $\exists$ a map $\mathbb{F} \to L$, $\alpha \mapsto \overline{\alpha} = \alpha + \langle f(x) \rangle$. This an injective ring homomorphism, and thus $\mathbb{F} \cong \Im(\mathbb{F})$, that is, $\mathbb{F}$ is isomorphic to the image of $\mathbb{F}$.*

↪ **Theorem 10.5**

Let $g(t) \in \mathbb{F}[t]$ be a non-constant polynomial. Then, $\exists$ a field $L \supseteq \mathbb{F}$ s.t. g has a root in L.

Proof. WLOG, assume $g(t)$ irreducible. Take another variable x, and let $L = \mathbb{F}[x]/\langle g(x) \rangle$; this is a field as g irreducible, and again, it contains $\mathbb{F}$ (that is, a field isomorphic to $\mathbb{F}$). Then, in L, the element $\overline{x}$ solves $g(t) = a_n t^n + \cdots + a_0, a_i \in \mathbb{F}$. We have, $g(\overline{x}) = \overline{a_n}\overline{x}^n + \cdots + \overline{a_0} = \overline{a_n x^n + \cdots a_0} = \overline{g(x)} = g(x) + \langle g(x) \rangle = \langle g(x) \rangle = 0_L$. ■

⊛ **Example 10.19**

$\mathbb{F} = \mathbb{R}, g(t) = t^2 + 1$. $L = \mathbb{R}[x]/\langle x^2+1\rangle, \overline{x}$ a root of t^2+1. In this case, we can denote $\overline{x} = i$, that is, $i = \sqrt{-1}$; $L \cong \mathbb{C}$.

10.5 Isomorphisms

↪ **Definition 10.12: Isomorphism**

Let $f : R \to S$ be a ring homomorphism. If f bijective, we say that R is *isomorphic* to S, and denote $R \cong S$. We say that f is an *isomorphism* between R and S.

↪ **Theorem 10.6: First Isomorphism Theorem**

Let $\varphi : R \to S$ be a surjective homomorphism of rings. Let $I = \ker \varphi$. Then, $R/I \cong S$.

Proof. Denote the elements of R/I by $\overline{r}$. Define $\Phi : R/I \to S, \Phi(\overline{r}) = \varphi(r)$. We show this is a ring homomorphism:

- (Well defined) if $\overline{r} = \overline{r_1}$, we aim to show that $\varphi(r) = \varphi(r_1)$. $\overline{r} = \overline{r_1} \implies r - r_1 = a \in I = \ker\varphi$. $\varphi(r) = \varphi(a + r_1) = \varphi(a) + \varphi(r_1) = 0 + \varphi(r_1) = \varphi(r_1)$.
- (Homomorphism) $\Phi(\overline{r} + / \cdot \overline{s}) = \Phi(\overline{r + / \cdot \overline{s}}) = \varphi(r + / \cdot s) = \varphi(r) + / \cdot \varphi(s) = \Phi(\overline{r}) + / \cdot \Phi(\overline{s})$.

To show Φ bijective:

- (Surjective) Given $s \in S, \exists r \in R$ s.t. $\varphi(r) = s$, since φ surjective. Then, $\Phi(\overline{r}) = \varphi(r) = s \implies \Phi$ surjective.
- (Injective) This is equivalent to showing $\ker\Phi = \{\overline{0}\}$. Suppose $\Phi(\overline{r}) = 0_S \implies \varphi(r) = 0_S \implies r \in \ker\varphi = I \implies \overline{r} = 0_{R/I}$

Hence, Φ a bijective ring homomorphism and so $R/I \cong S$. ■

⊛ **Example 10.20**

Let $R = \mathbb{R}[x], S = \mathbb{C}$. Let $\varphi : R \to S, \varphi(f(x)) = f(i)$. φ is a homomorphism of rings:

$$\varphi(f + / \cdot g) = (f + / \cdot g)(i) = f(i) + / \cdot g(i); \quad \varphi(1) = 1.$$

Let $I = \ker\varphi$. Note that $x^2 + 1 \in I (i^2 + 1 = 0), \implies \langle x^2+1\rangle \subseteq I$. We know, further, that $I = \langle g(x)\rangle$ for some $g(x) \in \mathbb{R}[x]$ (any ideal of $\mathbb{R}[x]$ principal), so $x^2+1 \in I \implies g(x)|(x^2+1)$. But x^2+1 is irreducible, hence $g(x) \sim 1 \implies I = \mathbb{R}[x]$ or $g(x) \sim x^2+1 \implies I = \langle x^2+1\rangle$. This first case is not possible, since this implies

$1 \in \mathbb{R}[x]$, since $\varphi(1) = 1 \neq 0$, hence $g(x) = x^2 + 1 \implies I = \langle x^2 + 1 \rangle$, and thus by First Isomorphism Theorem, $\mathbb{R}[x]/\langle x^2 + 1 \rangle \cong \mathbb{C}$.

↪ **Theorem 10.7: Chinese Remainder Theorem**

Let m, n be relatively prime positive integers. Then, $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

Proof. Define a function $\varphi : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, $\varphi(a) = (a \mod m, a \mod n)$. We show φ a ring homomorphism:

$$\begin{aligned} \varphi(a + / \cdot b) = (a + / \cdot b \mod m, a + / \cdot b \mod n) \\ = (a \mod m + / \cdot b \mod m, a \mod n + / \cdot b \mod n) \\ = (a \mod m, a \mod n) + / \cdot (b \mod m, b \mod n) \\ = \varphi(a) + / \cdot \varphi(b) \\ \varphi(1) = (1 \mod m, 1 \mod n) = 1_{\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}} \end{aligned}$$

We also have

$$\begin{aligned} \ker \varphi = \{a \in \mathbb{Z} : \varphi(a) = (a \mod m, b \mod n) = (0, 0)\} \\ = \{a : m | a \text{ and } n | a\} = \{a : \operatorname{lcm}(m, n) | a\} = \{a : mn | a\} = mn\mathbb{Z} \end{aligned}$$

Let $S = \operatorname{Im}(\varphi)$ which is a subring of $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Then, $\varphi : \mathbb{Z} \to S$ is a surjective ring homomorphism with kernel $mn\mathbb{Z}$, and so by First Isomorphism Theorem, $\mathbb{Z}/mn\mathbb{Z} \cong S$. Note that the LHS has $m \cdot n$ elements, hence S must have $m \cdot n$ elements as well, and thus $S = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Thus, $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

We can alternatively prove surjectivity directly. Since $\gcd(m, n) = 1, \exists u, v \in \mathbb{Z}$ s.t. $1 = um + vn$, hence we have

$$\varphi(um) = (um \mod m, 1 - vn \mod n) = (0, 1)$$

and

$$\varphi(vn) = (1 - um \mod m, vn \mod n) = (1, 0)$$

Hence,

$$\begin{aligned} \varphi(aum + bvn) = \varphi(aum) + \varphi(bvn) = \varphi(\underbrace{um + \cdots + um}_{a \text{ times}}) + \varphi(\underbrace{vn + \cdots + vn}_{b \text{ times}}) \\ = a\varphi(um) + b\varphi(vn) \\ = a(0, 1) + b(1, 0) \\ = (0, a) + (b, 0) = (b, a), \end{aligned}$$

hence φ surjective. Again, the kernel is $\ker \varphi = mn\mathbb{Z}$ and so $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ ■

⊛ **Example 10.21: Application of Chinese Remainder Theorem**

Let $m = 11, n = 13$. Find an integer x s.t. $x \equiv_{11} 2$ and $x \equiv_{13} 3$.

Proof. We can express $1 = \gcd(11, 13) = um + vn = 11u + 13v$. Working out the Euclidean algorithm, this yields $u = 6$ and $v = 5$, that is, $1 = 6 \cdot 11 - 5 \cdot 13 = 66 - 65$. We have

$$66 \mapsto (0, 1) \in \mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z},$$

and

$$-65 \mapsto (1, 0) \in \mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z}.$$

Hence, $3 \cdot 66 + 2 \cdot -65 \mapsto (2, 3) \in \mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z}$, so $x = 3 \cdot 66 + 2 \cdot -65 = 68$. ■

11 Groups

11.1 Definitions

↪ **Definition 11.1: Group**

A *group* G is a non-empty set with an operation

$$G \times G \to G, \quad (a, b) \mapsto a * b,$$

s.t.

1. (Associative) $a * (b * c) = (a * b) * c$
2. (Two-Sided Identity) $\exists$ an element of G, denoted 1_G s.t. $\forall a \in G, 1_G * a = a * 1_G = a$
3. (Two-Sided Unit) $\forall a \in G, \exists b \in G$ s.t. $a * b = b * a = 1_G$

↪ **Proposition 11.1: Basic Properties of Groups**

The following are direct consequences of the definition of a group:

1. 1_G unique: if $c \in G$ s.t. $a \cdot c = c \cdot a = a \forall a \in G$, then $c = 1_G$
2. Given $a \in G, b$ s.t. $a * b = b * a = 1_G$ is unique: if $a * c = c * a = 1_G$, then $c = b$. We denote $b = a^{-1}$.
3. $(a_1 * a_2)^{-1} = a_2^{-1} * a_1^{-1}$.
4. $ab = ac \implies b = c$

5. Define for $a \in G, n \in \mathbb{Z}$,

$$a^n := \begin{cases} 1_G & n = 0 \\ \underbrace{a * \cdots * a}_{a \text{ times}} & n > 0 \\ \underbrace{a^{-1} * \cdots * a^{-1}}_{-n \text{ times}} & n < 0 \end{cases}$$

Then, $a^{n+m} = a^n a^m$.

Proof.

1. $c = c * 1_G = 1_G$
2. $b = b * 1_G = b * (a * c) = (b * a) * c = 1_G * c = c \implies b = c$
3. $(a_1 a_2)(a_2^{-1} a_1^{-1}) = a_1 a_2^{-1} a_2 a_1^{-1} = a_1 1_G a_1^{-1} = a_1 a_1^{-1} = 1_G$. The converse follows.
4. $ab = ac \implies a^{-1}ab = a^{-1}ac \implies 1_G b = 1_G c \implies b = c$
5.

■

↪ **Proposition 11.2: What "Doesn't Hold" in Groups**

1. Only one operation, $*$.
2. Typically, $ab \neq ba$, that is, not commutative (see definition 11.2).

↪ **Definition 11.2: Commutative/Abelain Group**

If $\forall a, b \in G, ab = ba$, G is called *commutative* or *abelian*. Sometimes, if G abelian, we write the operation as $+$ and the neutral element as 0.

⊛ **Example 11.1: Basic Examples of Groups**

- $G = \{1\}$, where $1 * 1 = 1$.
- $G = \mathbb{Z}$ or $G = \mathbb{Z}/n\mathbb{Z}$, where $* = +$. Moreover, if R a ring, then R is an abelian group with addition.
- For a field $\mathbb{F}$, $(\mathbb{F}, +)$ is an abelian group, as is $(\mathbb{F}^\times, \cdot)$.
- If R a ring (need not be commutative), then $R^\times = \{u \in R : \exists v \in R, uv = vu = 1\}$ (the units) is a group with multiplication.
  - $\mathbb{Z}, \mathbb{Z}^\times = \{\pm 1\}$ is a group.
  - $R = M_2(\mathbb{R})$. The units $R^\times$ are all the invertible matrices, that is, with non-zero determinant. $(R, +)$ and $(R, \cdot)$ are both groups.

– More generally, $R = M_2(\mathbb{F})$, a ring, has units $R^\times = M_2(\mathbb{F})^\times =: GL_2(\mathbb{F})$. Note that this is a non-abelian group under multiplication (as matrix multiplication not commutative).

↪ **Definition 11.3: Subgroup**

A *subgroup* H of G is a subset $H \subseteq G$ s.t.

1. (Identity) $1 \in H$
2. (Closed under Multiplication) $a, b \in H \implies a \cdot b \in H$
3. (Closed under Inverses) $a \in H \implies a^{-1} \in H$

Moreover, H a group itself. We denote $H < G$ or $H \leqslant G$.

↪ **Definition 11.4: Cyclic Subgroup**

Take any $g \in G$, and form

$$\langle g \rangle = \{g^n : n \in \mathbb{Z}\} = \{\ldots, g^{-2}, g^{-1}, 1, g, g^2, \ldots\}.$$

This is called the *cyclic subgroup* generated by g. G is itself cyclic if $G = \langle g \rangle$ for some $g \in G$.

If we use additive notation rather than multiplicative, we have

$$\langle g \rangle = \{ng : n \in \mathbb{Z}\} = \{\ldots, -2g, -g, 0, g, 2g, \ldots\}.$$

⊛ **Example 11.2: Cyclic Groups**

For example, $\mathbb{Z}/n\mathbb{Z}$ and $\mathbb{Z}$ are cyclic; we have $\mathbb{Z}/n\mathbb{Z} = \langle \overline{1} \rangle$ and $\mathbb{Z} = \langle 1 \rangle$. Note that cyclic $\implies$ abelian, hence any non-abelian group is not cyclic.

↪ **Definition 11.5: Order of g/G**

The *order* of G, denoted $\sharp G$ or $|G|$, is the number of elements in G. If G infinite, it is denoted ∞.

The *order* of an element $g \in G$ is the minimal positive $n \in \mathbb{Z}_+$ s.t. $g^n = 1$. If not such n exists, we say that the order of g is ∞. We denote $\operatorname{ord}(G)$.

⊛ **Example 11.3: Orders**

1. $\mathbb{Z}, k \neq 0$, then $\operatorname{ord}(k) = \infty$, since $nk = 0 \implies n = 0$
2. $\mu_n = n$th roots of 1 in $\mathbb{C}$ (that is, the nth roots of unity). This is a group with n

elements, under multiplication, and is cyclic, with $\langle \mu_n \rangle = \langle e^{\frac{2\pi i}{n}} \rangle$.

3. $GL_2(\mathbb{F}_2)$ is a non-abelian group of 6 elements. We have, for instance,

$$\operatorname{ord}\left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right) = 2; \quad \operatorname{ord}\left(\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\right) = 3.$$

Multiplying the first by itself once yields the identity $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$; the second requires two multiplications by itself (that is, you cube the matrix) to yield the identity.

↪ **Proposition 11.3**

$\operatorname{ord}(g) = |\langle g \rangle|$. That is, the order of an element is the order of the cyclic subgroup it generates.

Proof. Suppose $\operatorname{ord}(g) = \infty$ and $|\langle g \rangle| < \infty$. This means that there must be repetitions in the subgroup; $\exists a > b \geq 0$ s.t. $g^a = g^b$. This implies, then, that $g^{a-b} = g^b \cdot g^{-b} = 1$, but $a - b > 0$ so $\operatorname{ord} g < \infty$ (as we have found some power n such that $g^n = 1$) and thus we have a contradiction. Hence, if the order of $\operatorname{ord} g = \infty$, then $|\langle g \rangle| = \infty$ as well.

Suppose $\operatorname{ord} g = n, 0 < n < \infty$. We note that $\forall a \in \mathbb{Z}, a = q \cdot n + r, 0 \leq r < n$, and so we can write

$$g^a = g^{q \cdot n + r} = (g^n)^q \cdot g^r = 1^q \cdot g^r = g^r \implies \langle g \rangle = \{1, g, \ldots, g^{n-1}\},$$

that is, g to any power can be reduced to g of a power $\leq n - 1$.

We now aim to show these are distinct. Suppose they are not; that is, $\exists 0 \leq b < a \leq n - 1$ such that $g^a = g^b$. We can write

$$g^{a-b} = 1,$$

but $0 < a - b < n$, so this is a contradiction, as, by definition, n the *minimal* positive integer such that $g^n = 1$, and this implies that we have a smaller element. Hence, these elements are indeed distinct and we thus have precisely n elements, which is equivalent to the order $\operatorname{ord} g$, and the proof is complete. ■

11.2 Symmetric Group

↪ **Definition 11.6: Symmetric Group S_n**

A group with $n!$ elements, non-abelian if $n \geq 3$ (S_1 trivial, S_2 only two elements so abelian). We often denote $[1, n] = \{1, 2, \ldots, n\}$. The *permutations* of $[1, n]$ is a bijective function

$\sigma : [1, n] \to [1, n]$. We write:

$$S_n := \{\sigma : [1, n] \to [1, n] : \sigma \text{ bijective}\}.$$

This is a group under composition of functions; if σ, τ, ρ are permutations, then we have

$$\sigma \circ \tau \text{ bijective, so } \in S_n; \quad \rho \circ (\sigma \circ \tau) = (\rho \circ \sigma) \circ \tau \quad .$$

The identity function and inverses follow similarly

$\sharp S_n = n!$ since we have n choices for $\sigma(1)$, $n-1$ choices for $\sigma(2), \ldots$, 2 choices for $\sigma(n-1)$, and 1 choice for $\sigma(n)$, yield $n!$ choices and hence $\sharp S_n = n!$.

⊛ **Example 11.4: Permutations,** $n = 5$

Consider the following (we denote $[1, \ldots, n] \mapsto [1, \ldots, n]$ as the top $\mapsto$ bottom line of the matrix):

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

This is cumbersome notation.

↪ **Definition 11.7: Cycles**

Let[50] $1 \leq a \leq n$ and $i_1, i_2, \ldots, i_a$ distinct elements of $[1, n]$. We denote $\sigma = (i_1\, i_2 \cdots i_a)$ as a *cycle* of length a, equal to the permutation σ such that $\sigma(i_j) = i_{j+1} \forall j = 1, \ldots, a$ and $\sigma(t) = t \forall t \notin \{i_1, \ldots, i_a\}$. For instance, for $n = 7$,

$$(5\,1\,6) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 2 & 3 & 4 & 1 & 5 & 7 \end{pmatrix}.$$

[50]Note that indices j here should be read mod a. That is, if you have $(i_1 i_2)$, then this would "read" as $i_1 \mapsto i_2$ and $i_2 \mapsto i_{3 \mod 2} = i_1$.

⊛ **Example 11.5:** $n = 3$

$\sigma = (1\,2\,3) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $\tau = (1\,2) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$. Consider:

$$\sigma\tau = (123)(12) = (13)(2) = (13)$$
$$\tau\sigma = (12)(123) = (1)(23) = (23)$$

Hence, since these are not equal, S_3 not commutative; moreover, S_n for $n \geq 3$ is not commutative.

More generally, consider $\sigma = (i_1, \ldots, i_a)$. Let $k \geq 1$ Then,

$$\begin{aligned} \sigma^k &= \sigma \circ \cdots \circ \sigma \\ \sigma^2 &= (i_1, i_2, i_3, i_4, \ldots) \quad k = 2 \\ \sigma^k(i_j) &= i_{j+k} \\ \sigma^k(t) &= t \forall t \notin \{i_1, \ldots, i_a\} \\ \sigma^k &= 1 \text{ for } k = a, \end{aligned}$$

that is, the order of a cycle of length a is a.

↪ **Proposition 11.4: Facts about Cycles**

1. Disjoint cycles commute. Say $\sigma = (i_1, \ldots, i_a)$ and $\tau = (i_{a+1}, \ldots, i_b)$, and $\{i_1, \ldots, i_a\} \cap \{i_{a+1}, \ldots, i_b\} = \varnothing$. Then, $\sigma\tau = \tau\sigma$.
2. Any permutation can be written as a product of disjoint cycles.

Proof. 1. If $t \notin \{i_1, \ldots, i_b\}$, $\sigma\tau(t) = \sigma(\tau(t)) = \sigma(t) = t$. Else, we have

$$\sigma\tau(i_s) = \begin{cases} \sigma(i_{s+1}) & a+1 \leq s \leq b \\ i_{a+1} & s = b \\ \sigma(i_s) & 1 \leq s \leq a \end{cases} = \begin{cases} i_{s+1} & a+1 \leq s \leq b \\ i_{a+1} & s = b \\ i_{s+1} & 1 \leq s \leq a \end{cases}$$

(where indices are read mod a) Calculating $\tau\sigma$ yields the same result.

2. We won't prove. Consider the following example.

■

⊛ **Example 11.6**

Let We can write

$$\sigma = (1\,5\,7\,2)(3)(4\,12)(6\,9\,10\,11\,8).$$

⊛ **Example 11.7: Composition of Disjoint Permutations**

Given $\sigma \in S_n$, write $\sigma = \tau_1\tau_2 \cdots \tau_r$. τ_i is a cycle of length a_i where the τ_i disjoint. Then, we can write

$$\begin{aligned} \sigma^2 &= \tau_1 \cdots \tau_r\tau_1 \cdots \tau_r \\ &= \tau_1^2 \cdots \tau_r^2 \\ \sigma^k &= \tau_1^k\tau_2^k \cdots \tau_r^k \end{aligned}$$

Hence, we have that $\sigma^k = 1 \iff \tau_1^k = \tau_2^k = \cdots = \tau_r^k = 1 \iff a_1|k, a_2|k, \ldots, a_r|k$ (this follows from lemma 11.1). Hence, $\operatorname{lcm}(a_1, \cdots a_r)|k$ and thus $\operatorname{ord}(\sigma) = \operatorname{lcm}(a_1, \ldots, a_r)$. Note that, if the cycles *not* disjoint, this usually fails.

↪ **Lemma 11.1**

Say $g \in G$ has order a. Let $k \geq 1$, then $g^k = 1 \implies a|k$.

Proof. Write $k = q \cdot a + r, 0 \leq r < a$. Then, $1 = g^k = (g^a)^q g^r = 1^q g^r = g^r \implies r = 0 \implies a|k$. ■

⊛ **Example 11.8: Subgroups of S_n**

Let $T \subseteq [1, n], \sharp T = t$, $A_T = \{\sigma \in S_n : \sigma(b) = b \forall b \in T\}$ (that is, all elements in T are fixed.), and $B_T = \{\sigma \in S_n : \sigma(T) = T\}$. We have that $A_T < B_T < S_N$. Moreover, $\sharp A_T = (n-t)!$ and $\sharp B_T = t!(n-t)!$.

11.3 Dihedral Groups D_n

↪ **Definition 11.8: D_n**

D_n or the *dihedral group* is the group of symmetries of a regular n-gon in the plane, where $n \geq 3$ (that is $n = 3$ a triangle, $n = 4$ a square, etc).

Let x represent a planar rotation (about the z axis), and y a rotation about y. Then, $\operatorname{ord} x = n$ and $\operatorname{ord} y = 2$.

↪ **Proposition 11.5**

Every symmetry $\sigma \in D_n$ is uniquely determined by $\sigma(1)$ and $\sigma(2)$. That is, $\sigma = \tau \iff \sigma(1) = \tau(1), \sigma(2) = \tau(2)$.

Moreover, the elements of D_n are precisely

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

that is, D_n has precisely $2n$ elements. Further, D_n not abelian. [51]

[51] Read: "an n-gon has precisely $2n$ distinct symmetries". Note that $e \equiv \nVdash$, that is, the identity element (no rotations).

Proof. We have, for a s.t. $0 \leq a \leq n-1$,

	1	2
x^a	$1+a$	$2+a$
$x^a y$	$1+a$	a

. We claim these are distinct: if $\sigma \in D_n$, then $\sigma(1) = 1 + a$, then either $\sigma(2) = a$ or $2 + a$, and so either $\sigma = x^a y$ or $\sigma = x^a$, respectively.

To show $xyxy = 1$:

To show that D_n not abelian we have that

$$\begin{aligned} xyxy = 1 &\implies xyx = y^{-1} = y \\ &\implies xy = yx^{-1} \end{aligned}$$

In this case, if D_n abelian, then $xy = yx \implies x = x^{-1} \implies x^2 = 1$, which is a contradiction.

Moreover, we have then that $xy = yx^{-1}$, and so we can write

$$\begin{aligned} x^a y = yx^{-a} \implies x^{a+1}y &= x(x^a y) = x(yx^{-a}) \\ &= (xy)x^{-a} = yx^{-1}x^{-a} = yx^{-(a+1)}, \end{aligned}$$

that is, $\forall a$, $x^a y = yx^{-a}$. ■

⊛ **Example 11.9: In D_5**

What is, in D_5, the element $x^3yxyx^2yx^4$?

Proof.

$$\begin{aligned} x^3y(xy)x^2yx^4 &= x^3y(yx^{-1})x^2yx^4 \\ &= x^3\cancel{y^2}x^{-1}x^2yx^4 \\ &= (x^4y)x^4 \\ &= (yx^{-4})x^4 \\ &= y \end{aligned}$$

■

↪ **Definition 11.9: Direct Product**

If G_1, G_2 are groups, $G_1 \times G_2$ also a group, where

- $(x_1, y_1)(x_2 y_2) = (x_1 x_2, y_1 y_2)$.
- $1 = (1, 1)$
- $(x, y)^{-1} = (x^{-1}, y^{-1})$

11.4 Cosets and Lagrange's Theorem

↪ **Definition 11.10: Left Coset**

Let $H < G$. A *left coset* of H in G is a subset of G of the form

$$gH := \{gh : h \in H\}.$$

↪ **Lemma 11.2: Facts about Cosets**

1. The cosets are equivalence classes for the relation on G defined $x \sim y$ if $y^{-1}x \in H$.
2. Two cosets are either equal or disjoint; $G = \amalg_{\{g_i : i \in I\}} g_i H$ for a suitable $\{g_i : i \in I\} \subseteq G$ (I some index set).
3. $xH = yH \iff y^{-1}x \in H \iff x^{-1}y \in H \iff \exists h \in H$ s.t. $x = yh$.
4. $xH = H \iff x \in H$.

⊛ **Example 11.10:** S_3

Let $G = S_3$, $H = \{1, (123), (132)\} = \langle (123) \rangle$. Examples of cosets of H would then be

$$\begin{aligned} &H = \{1, (123), (132)\} \\ &(12)H = (13)H = (23)H = \{(12), (23), (13)\} \end{aligned}$$

We can write, then,

$$G = H \amalg (12)H.$$

⊛ **Example 11.11:** $\mathbb{Z}/6\mathbb{Z}$

Let $G = \mathbb{Z}/6\mathbb{Z}$, $H = \langle 3 \rangle = \{0, 3\}$.

$$\begin{aligned} &1 + H = \{1, 4\} \\ &2 + H = \{2, 5\} \\ &3 + H = \{3, 0\} = H \end{aligned}$$

↪ **Definition 11.11: Index of a Subgroup**

Let G be finite, $H < G$. We define the *index* of H in G, denoted $[G : H]$ as the number of distinct left cosets of H in G.

Proof. (Of lemma 11.2)

1. (Equivalence relation)

   (a) $x \sim x \impliedby x^{-1}x = 1 \in H$

   (b) $x \sim y \implies y^{-1}x \in H \implies x^{-1}y = (y^{-1}x)^{-1} \in H$

   (c) $x \sim y, y \sim z \implies y^{-1}x \in H, z^{-1}y \in H \implies z^{-1}y \cdot y^{-1}x \in H \implies z^{-1}x \in H \implies x \sim y$

   (Equivalence class of x) If $x \in y, y^{-1}x \in H \implies x^{-1}y \in H \implies y = x(x^{-1}y) \in xH$. Conversely, if $y \in xH \implies y = xh$, some $y \in H$. $y^{-1}x = (xh)^{-1}x = h^{-1}x^1x = h^{-1} \in H \implies x \sim y$.

2. (Cosets equal/disjoint) This follows directly from 1. by properties of equivalence relations.

3. (Equivalence) $xH = yH \implies x, y$ have same equivalence class and so $x \sim y \implies x^{-1}y \in H$. Then, $xH = yH \implies yH = xH$, so the same logic follows symmetrically. $x^{-1}y \in H \implies x \sim y \implies x = yh$, some $h \in H$.

4. ($xH = H \iff x \in H$) Let $y = 1$. This then follows directly from 3.

■

↪ **Theorem 11.1: Lagrange's Theorem**

Let G be finite, $H < G$. Then,

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

and in particular,

$$|H| \mid |G|$$

↪ **Corollary 11.1**

Let G be a finite group, $g \in G$. Then, $\operatorname{ord} g| \mid G \mid$.

Proof. $\operatorname{ord} g = |\langle g \rangle| \mid |G|$, by Lagrange's Theorem. ■

Proof. (Of Lagrange's Theorem) Let G be a finite group, $H < G$. Since the cosets of a subgroup form a disjoint union of the group itself, we can write

$$G = \amalg_{i \in I} g_i H,$$

for some index set I. Let $a, b \in G$, and define the function

$$f : aH \to bH, \quad x \mapsto ba^{-1}x.$$

We claim this is a well-defined, bijective function.

- (Well-Defined) Let $x = ah$ for some $h \in H$. Then, $ba^{-1}x = ba^{-1}ah = bh \in bH$, hence the map is well-defined.

- (Surjective) Take $y \in bH, y = bh$. This is the image of ah (where a fixed as defined), that is, $ba^{-1}ah = bh$ as desired.

- (Injective) Consider $ba^{-1}x_1 = ba^{-1}x_2$. Multiplying both sides by $ab^{-1} \implies x_1 = x_2$.

Thus, this is indeed well-defined bijective map, moreover, each coset of $g_i H$ has the same number of elements. Specifically, we have

$$\sharp G = \sum_{i \in I} |g_i H| = \sum_{i \in I} |H| = |I| \cdot |H|.$$

Thus, we have that

$$|G| = |H| \cdot |I|,$$

moreover, in the language of the theorem,

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

■

Remark 11.1 (Applications of Lagrange's Theorem)**.** *1. Let G be a finite group of primer order p; then, G is cyclic, moreover, every element of G, $\neq e$, generates G.*

2. Every element of a group must have an order that divides the order of the group. This follows from Lagrange's combined with the fact that $\operatorname{ord} g =| \langle g \rangle$. *For instance, a group of order* 6 *cannot have an element of order* 4 *nor* 5.

Remark 11.2. *Note that if $n \mid |G|$, this does* not *imply that $\exists$ an element of G of order n. Indeed, taking $n = |G|$, this would imply that group G would be cyclic.*

11.5 Homomorphisms/Isomorphisms

↪ Definition **11.12: Group Homorphism**

Let G, H be groups, and define $f : G \to H$. f is called a *group homomorphism* if

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

$\forall g_1, g_2 \in G$.

The *kernel* of f is taken

$$\ker f = \{g \in G : f(g) = e_H\}.$$

↪ Lemma 11.3: Consequences of Homomorphisms

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

1. $f(e_G) = e_H$[52];
2. $f(g^{-1}) = f(g)^{-1}$;
3. $\text{Im}\,(f) < H$ (that is, the image of f is a subgroup of H)

Proof. 1.

$$\begin{aligned} &f(e_G) = f(e_G e_G) = f(e_G)f(e_G) \\ &\implies f(e_G)^{-1}f(e_G) = f(e_G)^{-1}f(e_G)f(e_G) \\ &\implies e_H = f(e_G) \end{aligned}$$

2.

$$\begin{aligned} &e_H = f(e_G) = f(gg^{-1}) = f(g)f(g^{-1}) \\ &\implies f(g)^{-1}e_H = f(g)^{-1}f(g)f(g^{-1}) \\ &\implies f(g^{-1}) = f(g)^{-1} \end{aligned}$$

3. $e_H = f(e_G) \in \text{Im}\,(f)$. Let $h_1, h_2 \in \text{Im}\,(f)$, and let $h_i = f(g_i)$. Then, $h_1 h_2 = f(g_1 g_2)$ and $h_1^{-1} = f(g_1)^{-1} \implies e_H, h_1 h_2, h_1^{-1} \in \text{Im}\,(f)$, hence $\text{Im}\,(f)$ a subgroup of H.

■

[52]Note that this is a consequence, not an axiom, as it was in ring homomorphisms.

↪ Definition 11.13: Group Isomorphism

A group homomorphism $f : G \to H$ is a *isomorphism* if it is bijective. We denote $G \cong H$ if such a function exists.

↪ Proposition 11.6

Let $f : G \to H$ be an isomorphism. Then, $g = f^{-1} : H \to G$ also an isomorphism.

Proof. g bijective, as f bijective and thus its inverse is also bijective. It remains to show that $\forall x, y \in H, f^{-1}(xy) = f^{-1}(x) \cdot f^{-1}(y)$. We have:

$$f(f^{-1}(xy)) = f(f^{-1}(x)f^{-1}(y)) \implies f(f^{-1}(xy)) = xy \tag{5}$$

$$f(f^{-1}(x)f^{-1}(y)) = f(f^{-1}(x))f(f^{-1}(y)) = xy, \tag{6}$$

noting that as both lines evaluate equivalently while computed in different orders, the claim holds, hence $g = f^{-1}$ a bijective homomorphism and is thus an isomorphism. ■

↪ **Proposition 11.7: Isomorphism an Equivalence Relation**

$\cong$ is an equivalence relation on groups.

Proof. 1. (reflexive) $G \cong G$ by $f = e_G$

2. (symmetric) $G_1 \cong G_2 \implies G_1 \xrightarrow{f} G_2 \implies G_2 \xrightarrow{f^{-1}} G_1 \implies G_2 \cong G_1$

3. (transitive) $f : G_1 \to G_2, g : G_2 \to G_3$, then consider $g \circ f : G_1 \to G_2$. This is bijective (composition of bijections is bijective). Take $x, y \in G_1$, then $(g \circ f)(xy) = g(f(xy)) = g(f(x)f(y)) = g(f(x))g(f(y)) = (g \circ f)(x)(g \circ f)(y)$, hence $g \circ f$ a homomorphism.

■

↪ **Proposition 11.8: Cyclic; $|G| = |H| = n \implies G \cong H$**

Let[53] $n \in \mathbb{Z}^+$. Then, any two cyclic groups of order n are isomorphic.

Proof. Suppose $G = \langle g \rangle, H = \langle h \rangle$ of order n. Define $f(g^a) = h^a$ for any integer a. This is well defined ($g^a = g^b \implies g^{a-b} = e_G \implies n|(a-b) \implies f(g^a) = h^a = h^b(h^n)^k = h^b = f(g^b)$). This is a surjective ($h^a = f(g^a) \forall h, g$) homomorphism ($f(g^a g^b) = f(g^{a+b}) = h^{a+b} = h^a h^b = f(g^a)f(g^b)$), and is also injective because $f(g^a) = h^a = e_H \implies n|a \implies g^a = e_G$. Thus, any cyclic group of order n is isomorphic. Moreover, any cyclic group of order n is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ over addition. ■

[53] This proof assumes finite groups, but this is true generally for non-finite groups.

↪ **Lemma 11.4**

Let $f : G \to H$ be a group homomorphism. $\ker f < G$, and f injective iff $\ker f = \{e_G\}$.

Proof. We have that $e_G \in \ker f$ since $f(1_G) = 1_H$. Suppose $g_1, g_2 \in \ker f \implies f(g_1) = f(g_2) = e_H \implies f(g_1 g_2) = f(g_1)f(g_2) = e_H e_H = e_H \implies g_1 g_2 \in \ker f$. Suppose $g \in \ker f \implies f(g^{-1}) = f(g)^{-1} = e_H^{-1} = e_H \implies g^{-1} \in \ker f$, hence all the group axioms hold and $\ker f < G$.

($\implies$) Suppose f injective. Then, $f(e_G) = e_H$ uniquely, and so $\ker f = \{e_G\}$.

($\impliedby$) Suppose $\ker f = \{e_G\}$, and $f(g_1) = f(g_2)$. Then, $e_H = f(g_1)^{-1}f(g_2) = f(g_1^{-1})f(g_2) = f(g_1^{-1}g_2) \implies g_1^{-1}g_2 \in \ker f \implies g_1^{-1}g_2 = e_G \implies g_1 = g_2 \implies f$ injective. ■

↪ **Corollary 11.2**

Let $p \in \mathbb{P}$. Then, any two groups of order p are isomorphic are cyclic, and isomorphic to $\mathbb{Z}/p\mathbb{Z}$.

Proof. Suppose $|G| = p$. Choose any $g \in G, g \neq e_G$. Let $H = \langle g \rangle$. By Lagrange's Theorem, $|H| \mid |G| = p$, so $|H| = 1$ or p, but by construction, $|H| = p$ (since $g \neq e_G$) , hence $|H| = |G|$. Thus, G a cyclic group of order p and is thus, by the previous example, we have that $G \cong \mathbb{Z}/p\mathbb{Z}$. ∎

↪ Proposition 11.9

Let $f : G_1 \to G_2$ be a homomorphism and $H < G_1$. Then, $f(H) < G_2$.

Proof.

- $1_{G_2} \in H \implies 1_{G_2} = f(1_{G_1}) \in f(H)$
- $x, y \in f(H) \implies \exists a, b \in H$ s.t. $x = f(a), y = f(b) \implies xy = f(a)f(b) = f(ab)$. $a \cdot b \in H \implies f(ab) \in f(H) \implies xy \in f(H)$
- $x \in f(H) \implies x^{-1} = f(a^{-1})$ for $a \in H$. Then, $a^{-1} \in H \implies f(a^{-1}) \in f(H)$.

Hence, $f(H) < G_2$ ∎

↪ Lemma 11.5

Let $g \in G_1, f : G_1 \to G_2$ a homomorphism. Then, $\operatorname{ord}(f(g)) \mid \operatorname{ord}(g)$.

Proof. Suppose $n = \operatorname{ord} g \implies g^n = 1 \implies f(g^n) = f(g)^n = f(1_{G_1}) = 1_{G_2} \implies f(g)^n = 1_{G_2} \implies \operatorname{ord}(f(g)) | n$. ∎

↪ Corollary 11.3

If $f : G_1 \to G_2$ an isomorphism, f induces bijections between subgroups of $H < G_1$ and $K < G_2$, that is,

$$G_1 > H \mapsto f(H) < G_2; \quad G_1 > f^{-1}(K) \mapsfrom K < G_2.$$

↪ Theorem 11.2: Cayley

Let G be a finite group of order n. Then, G is isomorphic to a subgroup of S_n.

Proof. Let $g \in G$, and let $\sigma_g : G \to G, a \mapsto ga$. We claim that σ_g a permutation.

Note first that σ_g injective,

$$\sigma_g(a) = \sigma_g(b) \implies ga = gb \implies a = b,$$

and surjective, since

$$\forall b \in G, \sigma_g(g^{-1}b) = b.$$

Now consider the map

$$G \to S_n, \quad g \mapsto \sigma_g.$$

This map is a homomorphism:

$$\sigma_{gh}(a) = gha = \sigma_g(\sigma_h(a)) \implies \sigma_{gh} = \sigma g \circ \sigma_h,$$

noting that the operation in S_n is $\circ$. This homomorphism is injective; let σ_g be the identity permutation. Then, $\sigma_g(e) = e \implies ge = e \implies g = e$. Thus, since the image of a homomorphism is a subgroup, the image of G under this map is a subgroup of S_n, that is, $G < S_n$ and the proof is complete. ■

↪ **Lemma 11.6**

Let T, Z be sets, and $f : T \to Z$ a bijection. Then, the group of permutations of T and Z are isomorphic.

Proof. Let $\sigma \in S_T$. Then, $f \circ \sigma \circ f^{-1} : Z \to Z$ is a bijection. Hence, we have the map

$$S_T \to S_Z, \quad \sigma \mapsto f \circ \sigma \circ f^{-1}.$$

This is a group homomorphism; given $\sigma_1, \sigma_2 \in S_T$,

$$f \circ \sigma_1 \circ \sigma_2 \circ f^{-1} = (f\sigma_1 f^{-1})(f\sigma_2 f^{-1}).$$

Similarly, given $\tau \in S_Z$, we can define the map

$$S_Z \to S_T, \quad \tau \mapsto f^{-1} \circ \tau \circ f.$$

This is also a homomorphism, hence, there exists a bijective homomorphism between $S_T \to S_Z$ and thus the two are isomorphic. ■

11.6 Group Actions on Sets

↪ **Definition 11.14: Group Action**

Let G a group, $S \neq \varnothing$. G *acts on* S if we have a function

$$G \times S \to S, \quad (g, s) \mapsto g \star s,$$

where

1. $e \star s = s \forall s \in S$;
2. $(g_1 g_2) \star s = g_1 \star (g_2 \star s) \forall g_1, g_2 \in G, s \in S$.

⊛ **Example 11.12**

D_n acts on the vertices of the n-gon;

$$x^a(i) = i + a; \quad y(i) = n - i + 2$$

⊛ **Example 11.13: Conjugation**

G acts on itself by

$$G \times G \to G, \quad (g, h) \mapsto ghg^{-1}.$$

⊛ **Example 11.14**

Let $H < G$. H acts on G by

$$H \times G \to G, \quad (h, g) \mapsto hg = h \star g.$$

⊛ **Example 11.15**

D_4 acts on the set S of 9 elements where the 9 elements form a 3×3 square. Now suppose we were to color each square by one of the three colors red, green, blue. Then, we'd have 3^9 possible colored squares. A natural question would be to ask how many colored 3×3 squares exist, up to symmetries?

⊛ **Example 11.16**

$\mathbb{R}$ acts on the sphere S; some $\theta \in \mathbb{R}$ rotates the sphere by θ.

↪ **Definition 11.15: Orbit**

Let G, S be as defined above. Let $s \in S$. The *orbit* of s is defined

$$\operatorname{Orb} s = \{g \star s : g \in G\} \subseteq S.$$

Note that this is equal to all the images of s under $\star$.

Remark 11.3. *In example 11.16, the orbit of $s \in S$ would be the latitude line; that is, all points with the same distance from the rotation axis.*

In example 11.14, the orbit of $x \in H$ would be $\operatorname{Orb} x = Hx = \{hx : h \in H\}$, a right coset of H in G.

↪ **Definition 11.16: Stabilizer**

Let G, S be as defined above. Let $s \in S$. The *stabilizer* is defined

$$\operatorname{Stab} s = \{g \in G : g \star s = s\} \subseteq G.$$

Remark 11.4. *In example* 11.16*,* $\operatorname{Stab} s = 2\pi\mathbb{Z}$*; unless* s *at the pole, then* $\operatorname{Stab} s = \mathbb{R}$.

In example 11.14*, take* $s \in G$*. Then,* $\operatorname{Stab} s = \{h \in H : h \star s = hs = s\} = \{1\}$.

In example 11.13*,* $\operatorname{Stab} s = \{g \in G : gsg^{-1} = g \star s = s\} = \{g \in G : gs = sg\}$*, which is defined as the* centralizer *of* s*, that is, the elements that commute with* s*.*

↪ **Definition 11.17: Collection of Cosets**

If $H < G$ denote by $G \setminus H$ the collection of left cosets xH of H in G. We have then

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

if G finite (by Lagrange's Theorem).

↪ **Lemma 11.7: Properties of Group Actions**

1. Let $s_1, s_2 \in S$. $s_1 \sim s_2$ if $\exists g \in G$ s.t. $g \star s_1 = s_2$. This is an equivalence relation; the equivalence class of s_1 is $\operatorname{Orb} s_1$.
2. Let $s \in S$. $\operatorname{Stab} s < G$.

Proof. 1.
- (Reflexive) $e \star s = s \implies s \sim s$
- (Symmetric) $s_1 \sim s_2 \implies \exists g \in G$ s.t. $g \star s_1 = s_2 \implies g^{-1} \star (g \star s_1) = g^{-1} \star s_2$ and $(g^{-1}g) \star s_1 = g^{-1} \star s_2$. Hence, $e \star s_1 = g^{-1} \star s_2 \implies s_1 = g^{-1}s_2 \implies s_2 \sim s_1$.
- (Transitive) Suppose $s_1 \sim s_2$, $s_2 \sim s_3$. Then, $\exists g_1, g_2 \in G$ s.t. $g_1 \star s_1 = s_2, g_2 \star s_2 = s_3 \implies (g_2 g_1) \star s_1 = g_2 \star (g_1 \star s_1) = g_2 \star s_2 = s_3 \implies s_1 \sim s_3$.

By definition, the equivalence class of some s_1 is all elements such that $g \star s_1 = s_1$ for some $g \in G$, the very definition of $\operatorname{Orb} s_1$.

2. Let $H = \operatorname{Stab} s$.
   - (Identity) $e \star s = s \implies e \in H$
   - (Closure) Let $g_1, g_2 \in H \implies g_1 \star s = s, g_2 \star s = s \implies (g_1 g_2) \star s = g_1 \star (g_2 \star s) = g_1 \star s = s \implies g_1 g_2 \in H$
   - (Inverses) Let $g \in H \implies g \star s = s \implies g^{-1}(g \star s) = g^{-1} \star s \implies (g^{-1}g) \star s = g^{-1} \star s \implies e \star s = g^{-1} \star s \implies s = g^{-1} \star s \implies g^{-1} \in H$

■

↪ **Proposition 11.10: Orbit-Stabilizer Formula**

There exists a bijection $G \setminus \operatorname{Stab} s \to \operatorname{Orb} s$, that is, between the left cosets of $\operatorname{Stab} s$ in G (see definition 11.17) and the orbit of s.

Proof. Let $H := \operatorname{Stab} s$. Define a function $\Psi : G \setminus H \to \operatorname{Orb} s$, where $\Psi(gH) := g \star s$.

- (Well-defined) Suppose $gH = g_1 H$; then, $g_1 = gh, h \in H \implies g_1 \star s = g \star (h \star s) \underbrace{=}_{h \in \mathrm{Stab}} g \star s$.
- (Surjective) Any element of $\operatorname{Orb} s$ is of the form $g \star s$ for some g, namely, of the form $\Psi(gH)$
- (Injective) Suppose $\psi(gH) = \psi(g_1 H)$. Then, we have

$$g \star s = g_1 \star s \overset{\times g^{-1}}{\implies} s = g^{-1} g_1 \star s \implies g^{-1} g_1 \in \operatorname{Stab} s = H \implies g_1 H = gH$$

■

↪ **Corollary 11.4**

Suppose G finite. Then,

$$|\operatorname{Orb} s| = |G \setminus H| = [G : H] = \frac{|G|}{|\operatorname{Stab} s|} = \frac{|G|}{|H|}.$$

Proof. Follows from Orbit-Stabilizer Formula and Lagrange's Theorem. ■

↪ **Definition 11.18: Fix, I, N**

Let G be a group acting on S. Then, for $g \in G, s \in S$, we have

$$\operatorname{Fix} g := \sharp\{s \in S : g \star s = s\} = \sharp \text{ fixed pts of g}.$$

Define too

$$I(g, s) := \begin{cases} 1 & g \star s = s \\ 0 & \text{else} \end{cases}$$

and

$$N := \sharp \operatorname{Orb} \text{ of } G \text{ in } S.$$

↪ **Theorem 11.3: Burnside's Lemma**

Assume S, G finite.

$$N = \frac{1}{\sharp G} \sum_{g \in G} \operatorname{Fix} g.$$

<u>*Proof.*</u> We will evaluate

$$\begin{aligned}
\sum_{s \in S} \sum_{g \in G} I(g, s) &= \sum_{s \in S} |\operatorname{Stab} s| \\
&\overset{\text{proposition 11.10}}{=} \sum_{s \in S} \frac{|G|}{|\operatorname{Orb} s|} \\
&= |G| \sum_{s \in S} \frac{1}{|\operatorname{Orb} s|} \\
&\overset{\star}{=} |G| \cdot N
\end{aligned}$$

$\star$: any orbit $\operatorname{Orb} s$ of size t contributes $\frac{1}{t} = \frac{1}{|\operatorname{Orb} s|}$ t times.

OTOH,

$$\begin{aligned}
\sum_{s \in S} \sum_{g \in G} I(g, s) &= \sum_{g \in G} \sum_{s \in S} I(g, s) \\
&\sum_{g \in G} \operatorname{Fix} g \\
\implies \sum_{g \in G} \operatorname{Fix} g &= |G| \cdot N \\
\implies N &= \frac{1}{|G|} \sum_{g \in G} \operatorname{Fix} g.
\end{aligned}$$

■

Remark 11.5. *Recall example 11.15; we had asked how many possibilities of a 3×3 square (S), colored with three different colors, existed up to symmetries by D_4. This is equivalent to asking for the number of orbits that exists for S.*

We have

$$\begin{aligned}
&\operatorname{Fix} 1 = \sharp S = 3^9 \quad \textit{anything times 1 brings it to itself} \\
&\operatorname{Fix} x = 3^3 \\
&\operatorname{Fix} x^{-1} = 3^3 \\
&\operatorname{Fix} x^2 = 3^5
\end{aligned}$$

For general D_n, all the elements in $D_n \setminus \langle x \rangle = \{x^a y : a = 0, \ldots, n-1\}$ are reflections. They are also orientation reversing and order two ($x^a y \cdot x^a y = y x^{-a} x^a y = y^2 = 1$).

Hence, we have that $\operatorname{Fix} y = 3^6 = \operatorname{Fix} x^2 y = \operatorname{Fix} xy = \operatorname{Fix} x^3 y$.

Hence, we have from Burnside's,

$$N = \frac{1}{8}\left(3^9 + 2 \cdot 3^3 + 3^5 + 4 \cdot 3^6\right) = 2862.$$

11.7 More on the Dihedral Group

↪ **Lemma 11.8**

Let $x \in D_n$. Then, $\operatorname{ord} x^a = \frac{n}{\gcd a, n}$. As a permutation of the n vertices of the corresponding n-gon, we have $x^a =$ product of disjoint cycles, where all of the elements $\{1, \ldots, n\}$ appear, each of this same length.

⊛ **Example 11.17:** $n = 8$

x^a	$\Pi\sigma_i$	a	ord
x	(12345678)	1	8
x^2	$(1357)(2468)$	2	4
x^3	(14625836)	3	8
x^4	$(15)(26)(37)(48)$	4	2
x^5	$\cdots$	5	8
x^6	$(1753)(2864)$	6	4
x^7	$\cdots$	7	8

Proof. Write x^a as a product of disjoint cycles, in which every $1 \leq i \leq n$ appears. Then, consider the cycle in which i appears (take i as the first element, since we can simply rearrange any permutation such that this holds):

$$(i, ia, i + 2a, \ldots, i + (k-1)a),$$

where k is the minimal positive integer such that $i + ka \equiv_n i$; ie, the first time that this cycle closes. But this means that $ka \equiv_n 0$, that is, this k does not depend on the particular i we are considering; it remains to show that this k is as given in the lemma.

We have that,

$$\begin{aligned} \forall k' \in \mathbb{Z}, n \mid k'a &\iff \frac{n}{(a,n)} \mid k' \cdot \frac{a}{(a,n)} \\ &\iff \frac{n}{(a,n)} \mid k' \\ &\implies \text{min. possible } k' \text{ is } \frac{n}{(a,n)} \end{aligned}$$

■

↪ **Corollary 11.5**

The ♯ of elements $y \in \langle x \rangle$ s.t. $\langle x \rangle = \langle y \rangle$ is $\varphi(n)$. Such $y = x^a$ and of ord n. The ♯ of such y's is $\sharp\{1 \leq a \leq n$ s.t. $(a, n) = 1\} =: \varphi(n)$.

↪ **Corollary 11.6**

For any $d|n$, $\exists$ elt of $\operatorname{ord} = d \in \langle x \rangle$.

Proof. $x^{n/d}$ ■

Remark 11.6. *In fact, there* $\exists \varphi(d)$ *elts of order* d *in* $\langle x \rangle$.

↪ **Proposition 11.11**

Every element on $D_n \setminus \{1, x, \ldots, x^{n-1}\}$ is a reflection. If n odd, the reflection has exactly 1 fixed vertex. If n even, the symmetries y, $x^2 y, \ldots, x^{n-2} y$ have 2 fixed vertices; the symmetries $xy, \ldots, x^{n-1} y$ have none.

⊛ **Example 11.18**

Consider necklaces with 8 beads, with 4 Blue, 2 Green, 2 Red. How many combinations, up to D_8 symmetries, exist?

Proof. We will approach this using the C-F formula; we have $N = \frac{1}{16} \sum_{g \in D_8} \operatorname{Fix} g$. Note first that $\operatorname{Fix} 1 = \sharp$ designs $= \binom{8}{4}\binom{4}{2} = 420$.

First, we claim that for $a = 1, 3, 5, 7$, $\operatorname{Fix} x^a = 0$; indeed, any x^a for these a would necessitate every bead to be of the same color.

Next, we claim that $\operatorname{Fix} x^2 = \operatorname{Fix} x^6 = 0$; indeed, we have two disjoint cycles of order 4, so any element in these "gaps" would have to be of the same color, hence, suppose one of these were green, then all 4 would be green; this is possible.

Next, $\operatorname{Fix} x^4 = \binom{4}{2}$ (that is, we choose which of the four pairs of 2 elements we take to be blue) times $\cdot 2$ (which of the 2 remain pairs are green), which gives $\operatorname{Fix} x^4 = 12$.

Now, take $\sigma =$ reflection, with no fixed vertices; there exist 4 such σ. $\operatorname{Fix} \sigma = \binom{4}{2}$ (which of the four vertices are blue) $\cdot 2$ (which of the 2 remaining vertices are red (or green, wlog)) $= 12$.

Now, take $\sigma =$ reflection with 2 fixed vertices; there exist 4. We have $\operatorname{Fix} \sigma = 3 + 3 + 6 = 12$.

Thus, $N = \frac{1}{16}(420 + 9 \cdot 12) = 33$. ■