IA Numbers and Sets, Groups and Geometry

Andrew Kay

September 28, 2014

Abstract

These notes are adapted from my notes taken from Part IA of the Mathematical Tripos at the University of Cambridge in 2006-2007:

- *Numbers and Sets*, lectured by Prof. Imre Leader.
- *Algebra and Geometry*, "Groups and Geometry", lectured by Prof. Thomas Körner.

The two modules are consolidated in this text as each contain proofs which depend on results from the other. Readers of Mathematics at Cambridge should note that neither module is covered exhaustively, but the missing parts from each can be found in my notes on *Sets, Logic, Relations, and Functions* and *IA Analysis I*, and *IA Vectors and Matrices* respectively.

Z notation is used in many places; see my notes on *Sets, Logic, Relations, and Functions* for definitions of unfamiliar symbols and words.

1 Sets

1.1 Sets of Numbers

The set $\mathbb{N} = \{0, 1, 2, \ldots\}$ of **natural numbers** is defined by three important properties:

1. There is a "first" natural number 0.[1]
2. Every natural number n has a "next" number $n + 1$.
3. Every non-empty subset of $\mathbb{N}$ has a minimum element.

The set $\mathbb{Z} = \{\ldots -2, -1, 0, 1, 2, \ldots\}$ of **integers** is defined by introducing *additive inverses* $-n$ for each natural number n.

$\mathbb{Z}$ is a **ring**, meaning we can add, subtract and multiply according to the usual rules.

The set $\mathbb{Q}$ of **rational numbers** is defined by introducing *multiplicative inverses* $\frac{1}{n}$ for each non-zero integer n.

The set $\mathbb{R}$ of **real numbers** is defined so that every non-empty bounded-above subset $S \subset \mathbb{R}$ has a *supremum* or *least upper bound* $\sup S$; i.e. every upper bound m of S must have $m \geqslant \sup S$.

The set $\mathbb{C}$ of **complex numbers** is defined by introducing i, the *imaginary unit*, which satisfies $\mathrm{i}^2 = -1$.

$\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are **fields**, meaning we can add, subtract and multiply and divide according to the usual rules.

$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

(See the Appendix for formal definitions.)

[1] In some texts, the first natural number is 1. We will write $\mathbb{N}_+ = \mathbb{N} \setminus \{0\} = \{1, 2, 3, \ldots\}$.

1.2 Induction

Suppose $P(n : \mathbb{N})$ is a predicate for which $P(0)$ is true. Suppose also that, for any n, the truth of $P(n)$ implies the truth of $P(n+1)$. In this case, we can conclude that $P(n)$ is true for *all* natural numbers n. This principle is known as **induction**.

Theorem 1.2.1 (Induction[2])**.**

$$\Big(P(0) \land \big(\forall\, n : \mathbb{N} \bullet P(n) \Rightarrow P(n+1)\big)\Big) \Rightarrow \big(\forall\, n : \mathbb{N} \bullet P(n)\big)$$

Proof. Suppose $\exists\, m : \mathbb{N} \bullet \neg P(m)$. Then let $m = \min\{\, n : \mathbb{N} \mid \neg P(n) \,\}$. $P(0)$ is true by assumption, so $m \geqslant 1$, and $m = n + 1$ for some $n : \mathbb{N}$. $n < m$, so $P(n)$ must be true. However, $P(n) \Rightarrow P(n+1) = P(m)$, contradicting $\neg P(m)$.[3] □

Therefore, we may prove a proposition $\forall\, n : \mathbb{N} \bullet P(n)$ by proving $P(0)$ (which is usually trivial) and the inductive step $\forall\, n : \mathbb{N} \bullet P(n) \Rightarrow P(n+1)$.

The principle of **strong induction** allows us to make a stronger assumption in the inductive step: we seek to prove $P(n)$, on the assumption that $P(k)$ is true for *all* natural numbers $k < n$.

Corollary 1.2.2 (Strong[4] Induction)**.**

$$\Big(\forall\, n : \mathbb{N} \bullet \big(\forall\, k : \mathbb{N} \mid k < n \bullet P(k)\big) \Rightarrow P(n)\Big) \Rightarrow \big(\forall\, n : \mathbb{N} \bullet P(n)\big)$$

Proof. Define $Q(n : \mathbb{N}) = \big(\forall\, k : \mathbb{N} \mid k < n \bullet P(k)\big)$. $Q(0)$ is a vacuous truth; also, $Q(n) \Rightarrow P(n)$ is equivalent to $Q(n) \Rightarrow Q(n+1)$. Therefore, the principle of induction applies to $Q(n)$, and so the result follows from Theorem 1.2.1. □

An "inductive proof" is one which makes use of either of these principles. Such a proof is "by induction on n" (or "by strong induction on n").

An "inductive definition" of a function $f : \mathbb{N} \to X$ is one for which the predicate "f is defined at $n : \mathbb{N}$" can be proven by induction; e.g. $f(0)$ is defined, and the definition of $f(n)$ depends on values of $f(k)$ for $k < n$. Such a function f is "defined inductively".

[2]Literally, "If $P(0)$ is true, and for all n, $P(n)$ implies $P(n+1)$, then for all n, $P(n)$ is true." Metaphorically, if we can step onto the first rung of a ladder, and climb from each rung to the next, then we can reach any rung.

[3]Metaphorically, if there is an unreachable rung, there is a lowest one, in which case we can reach the one below it. But then we can climb one more rung, contradicting its unreachability.

[4]The corollary is ostensibly *weaker*, as the premise is stronger.

1.3 Binomial Coefficients

Definition 1.3.1. *For $n : \mathbb{N}$, $n! = \prod_{k=1}^{n} k$ is the **factorial** of n.*

Definition 1.3.2.

1. *If X is a set, and $k : \mathbb{N}$, $X^{(k)} = \{ S : \mathbb{P}\, X \mid \#S = k \}$.*
2. *$C : \mathbb{N}^2 \to \mathbb{N}$ is given by $C(n,k) = \#\{1, \ldots n\}^{(k)}$. We write $\binom{n}{k}$ to mean $C(n,k)$. Values of C are **binomial coefficients**.*

Note that by symmetry,[5] each element $a : X$ appears in the same number of sets $S : X^{(k)}$; i.e. $\forall\, a, b : X \bullet \#\{ S : X^{(k)} \mid a \in S \} = \#\{ S : X^{(k)} \mid b \in S \}$.

Proposition 1.3.3. *$\forall\, n, k : \mathbb{N}$,*

1. $\binom{n}{k} = \dfrac{n!}{k!(n-k)!}$.
2. $\binom{n}{0} = \binom{n}{n} = 1$, $\binom{n}{1} = n$, *and if* $k > n$, *then* $\binom{n}{k} = 0$.
3. $\binom{n}{k} = \binom{n}{n-k}$.
4. $\binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}$.[6]
5. $\sum_{k=0}^{n} \binom{n}{k} = 2^n$.

Proof.

1. If the first k elements in an ordering of the set n determine a subset of cardinality k, then there are $k!$ possible orderings of the first k elements, and $(n-k)!$ orderings of the remaining elements; hence, each subset is given by $k!(n-k)!$ of the $n!$ orderings of the set n.
2. Follows immediately from (1), and the fact that $\{1, \ldots n\}$ has no subsets of cardinality $k > n$.

[5] I.e. $\mathrm{Sym}(X)$ acts **transitively** on X and $X^{(k)}$.

[6] Hence, "Pascal's triangle" computes the binomial coefficients.

3. Follows immediately from (1).

4. $$\frac{n!}{k!(n-k)!} + \frac{n!}{(k+1)!(n-k-1)!} = \frac{(n-k)n! + (k+1)n!}{(k+1)!(n-k)!} = \frac{(n+1)!}{(k+1)!(n-k)!}$$

5. Let $N = \{1, \ldots n\}$, then $\{\, k : \mathbb{N} \mid k \leqslant n \bullet N^{(k)} \,\}$ is a partition of $\mathbb{P}\, N$, so $2^n = \#\,\mathbb{P}\, N = \#\bigcup_{k=0}^{n} N^{(k)} = \sum_{k=0}^{n} \#N^{(k)} = \sum_{k=0}^{n} \binom{n}{k}$.

□

Theorem 1.3.4 (The Binomial Theorem)**.** $\forall\, n : \mathbb{N}$*, the polynomial*

$$(X + Y)^n = \sum_{k=0}^{n} \binom{n}{k} X^k\, Y^{n-k}$$

Proof. By induction on n; $n = 0$ is trivial. Then, □

$$\begin{aligned}
&(X + Y)^{n+1} = (X + Y)(X + Y)^n \\
&= (X + Y) \sum_{k=0}^{n} \binom{n}{k} X^k\, Y^{n-k} \\
&= \left[\sum_{k=0}^{n} \binom{n}{k} X^{k+1}\, Y^{n-k}\right] + \left[\sum_{k=0}^{n} \binom{n}{k} X^k\, Y^{n+1-k}\right] \\
&= \binom{n}{0} Y^{n+1} + \left[\sum_{k=1}^{n} \left(\binom{n}{k-1} + \binom{n}{k}\right) X^k\, Y^{n+1-k}\right] + \binom{n}{n} X^{n+1} \\
&= \binom{n+1}{0} Y^{n+1} + \left[\sum_{k=1}^{n} \binom{n+1}{k} X^k\, Y^{n+1-k}\right] + \binom{n+1}{n+1} X^{n+1} \\
&= \sum_{k=0}^{n+1} \binom{n}{k} X^k\, Y^{n+1-k}.
\end{aligned}$$

1.4 The Inclusion-Exclusion Principle

Lemma 1.4.1. $\forall\, n : \mathbb{N} \bullet \sum_{k=1}^{n} (-1)^{k+1} \binom{n}{k} = 1.$

Proof. By Theorem 1.3.4, $\sum_{k=0}^{n} (-1)^k \binom{n}{k} = (1 + (-1))^n = 0$. Therefore, $1 = (-1)^0 \binom{n}{0} = \sum_{k=0}^{n} (-1)^k \binom{n}{k} - \sum_{k=1}^{n} (-1)^k \binom{n}{k} = 0 + \sum_{k=0}^{n} (-1)^{k+1} \binom{n}{k}$. □

Theorem 1.4.2 (Inclusion-Exclusion Principle)**.**
If X is a finite set, and $S : \mathbb{P}\,\mathbb{P}\, X$, then

$$\#\bigcup S = \sum_{k=1}^{\#S} (-1)^{k+1} \sum_{B : S^{(k)}} \#\bigcap B$$

Equivalently, for $A_1, \ldots A_n : \mathbb{P}\, X$,

$$\#\bigcup_{i=1}^{n} A_i = \sum_{J : \mathbb{P}\{1,\ldots n\}} (-1)^{1+\#J} \#\bigcap_{i:J} A_i$$

Equivalently,

$$\#(A_1 \cup \cdots A_n) = \sum_{k=1}^{n} (-1)^{k+1} \sum_{1 \leqslant i_1 < \ldots i_k \leqslant n} \#(A_{i_1} \cap \ldots A_{i_k})$$

Proof. Given $x : \bigcup S$, suppose $x \in A$ for exactly m of the $A : S$.

By symmetry, $x \in \bigcap B$ for exactly $\binom{m}{k}$ of the $B : S^{(k)}$. Also, the terms for $k > m$ are all 0. Hence, x is counted exactly $\sum_{k=1}^{m} (-1)^{k+1} \binom{m}{k} = 1$ time by Lemma 1.4.1. □

In particular, e.g. $\#(X \cup Y) = \#X + \#Y - \#(X \cap Y)$.

1.5 Irrational and Transcendental Numbers

Definition 1.5.1. *An **irrational number** is a number which is not rational; i.e. it is not in* $\mathbb{Q}$.

Proposition 1.5.2. e *is irrational.*

Proof. Suppose $\mathrm{e} = \frac{p}{q} \in \mathbb{Q}$ with $q \geqslant 1$.

$$\mathbb{Z} \ni p(q-1)! = q!\mathrm{e} = q! \sum_{n=0}^{\infty} \frac{1}{n!} = \left[\sum_{n=1}^{q} \frac{q!}{n!}\right] + \left[\sum_{n=q+1}^{\infty} \frac{q!}{n!}\right]$$

where the first term is an integer.[7] Thererefore, the second term is an integer.

However, for $k \geqslant 1$, $\dfrac{q!}{(q+k)!} \leqslant \dfrac{1}{(q+1)^k}$ with strict inequality for $k > 1$, so

$$0 < \sum_{n=q+1}^{\infty} \frac{q!}{n!} = \sum_{k=1}^{\infty} \frac{q!}{(q+k)!} < \sum_{k=1}^{\infty} \frac{1}{(q+1)^k} = \frac{1}{q} \leqslant 1$$

and hence this term is not an integer; a contradiction. □

Definition 1.5.3. *For* $R : \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\}$,

1. *A **monomial** in variables* $X_1, \ldots X_m$ *is of the form* $aX_1^{k_1} \cdots X_m^{k_m}$ *for* $a : R, k_1, \ldots k_m : \mathbb{N}$.[8]

2. *A **polynomial** in one variable* X *is a sum of monomials in* X.

   In general, a polynomial f *in one variable* X *has* $f = \sum_{k=0}^{n} a_k X^k$ *for* $a_1, \ldots a_n : R \mid a_n \neq 0$, *or* $f = 0$.

3. *If* f *is a polynomial in one variable,* $\deg f = n$ *is the **degree**[9] of* f, *and* $\deg 0 = -\infty$.[10]

4. $R[X]$ *is the set of all polynomials in* X *with coefficients in* R.

5. *For* $f : R(X)$, $z : \mathbb{C}$ *is a **root** of* f *if* $f(z) = 0$.

[7] For $n \leqslant q$, $q!$ is a multiple of $n!$, so the first term is a sum of integers.
[8] For convenience, we will take X^0 to be 1 even when $X = 0$.
[9] More generally, the degree of a polynomial in m variables is the largest of the $\sum k_i$.
[10] $-\infty$ is not a number, but $-\infty < n$ for any number n.

Proposition 1.5.4. *For $z : \mathbb{C}$, z is a root of a non-zero polynomial in $\mathbb{Z}[X]$ iff it is a root of a non-zero polynomial in $\mathbb{Q}[X]$; i.e.*

$$\big(\exists f : \mathbb{Z}[X] \setminus \{0\} \bullet f(z) = 0\big) \Leftrightarrow \big(\exists g : \mathbb{Q}[X] \setminus \{0\} \bullet g(z) = 0\big)$$

Proof. Given $g = \sum_{k=0}^{n} \frac{p_k}{q_k} X^k$, let $f = \left[\prod_{k=0}^{n} q_k\right] \cdot g$. Then $f \neq 0$, $f \in \mathbb{Z}[X]$, and $f(z) = 0$.

The converse is trivial. □

Definition 1.5.5.

1. *$z : \mathbb{C}$ is an **algebraic number** if it is a root of a non-zero polynomial in $\mathbb{Z}[X]$.*[11]
2. *$z : \mathbb{C}$ is a **transcendental number** if it is not algebraic.*
3. *$\mathbb{A}$ is the set of algebraic numbers.*

Proposition 1.5.6. *Every rational number is algebraic.*

Proof. Given $a : \mathbb{Q}$, a is a root of $(X - a) \in \mathbb{Q}[X]$. □

Theorem 1.5.7. *Liouville's constant $x = \sum_{n=1}^{\infty} 10^{-n!}$ is transcendental.*

Proof. Suppose $\sum_{k=0}^{d} a_k x^k = 0$ for some $a_1, \ldots a_d : \mathbb{Z} \mid a_d \neq 0$. For $n : \mathbb{N}_+$, let

$$A_n = \sum_{i=1}^{n-1} 10^{-i!},\ B_n = 10^{-n!}, \text{ and } C_n = \sum_{i=n+1}^{\infty} 10^{-i!}$$

so that $\forall\, n : \mathbb{N}_+$,

1. $A_n + B_n + C_n = x$.
2. A_n is an integer multiple of B_n, and if $n > 1$, $B_n < A_n < 1$.
3. If $n \geqslant d$, then $C_n < 2 \cdot 10^{-(n+1)!} < 2B_n^d \cdot 10^{n!d-(n+1)!} < B_n^d$.

[11] Or equivalently, $\mathbb{Q}[X]$.

$(A_n + B_n + C_n)^d$ is a sum of terms of the form $A_n^p B_n^q C_n^r$, where $p, q, r : \mathbb{N} \mid p + q + r = d$.[12]

- One term is B_n^d,
- Each term with $r > 0$ has $A_n^p B_n^q C_n^r < C_n$,
- The remaining terms are integer multiples of $A_n B_n^{d-1} = B_n^d \cdot 10^{n!-(n-1)!}$.

Similarly, for $k : \mathbb{N} \mid k < d$, $(A_n + B_n + C_n)^k$ is a sum of terms each of which is either an integer multiple[13] of $B_n^{d-1} = B_n^d \cdot 10^{n!}$, or less than C_n.

Hence, for sufficiently large n,

$$0 = 10^{n!d} \sum_{i=0}^{d} a_i x^i = \frac{1}{B_n^d} \sum_{i=0}^{d} a_i (A_n + B_n + C_n)^i = S_n \cdot 10^{n!-(n-1)!} + a_d + \epsilon_n$$

where $S_n \in \mathbb{Z}$. It follows that $a_d + \epsilon_n$ is an integer multiple of $10^{n!-(n-1)!}$.

$|\epsilon_n| < MT \cdot 2 \cdot 10^{n!d-(n+1)!}$, where $M = \max_{0 \leqslant k \leqslant d} |a_k|$ and $T = 3^d(d+1)$ is an upper bound for the number of terms in the expansion. Therefore, for sufficiently large n, $|\epsilon_n| < |a_d| < \frac{1}{2} \cdot 10^{n!-(n-1)!}$, and so $a_d + \epsilon_n$ is not an integer multiple of $10^{n!-(n-1)!}$, a contradiction. □

A similar proof shows that for $x : \mathbb{R}$, if

$$\forall\, n : \mathbb{N} \bullet \exists\, \frac{p}{q} : \mathbb{Q} \bullet 0 < \left| x - \frac{p}{q} \right| < \frac{1}{q^n}$$

then x is transcendental.[14]

1.6 Countability

Definition 1.6.1.

1. *A set S is **countable** if $\exists f : \mathbb{N} \twoheadrightarrow S$.*[15]
2. *S is **uncountable** if S is not countable.*

Equivalently, $\exists f : S \rightarrowtail \mathbb{N}$. Equivalently, either S is finite or $\exists f : \mathbb{N} \rightarrowtail S$.

Note that for X countable, if $\exists f : X \twoheadrightarrow Y$ or $\exists f' : Y \rightarrowtail X$ then Y is countable.

[12] E.g. by applying Theorem 1.3.4 twice.

[13] Since for $k < d$, B_n^k is an integer multiple of B_n^{d-1}.

[14] Such an x is a **Liouville number**, and this result is *Liouville's theorem on diophantine approximation.*

[15] I.e. S can be enumerated, or "counted", by the natural numbers, although the list may be infinitely long.

Theorem 1.6.2.

1. $\mathbb{N}^2$ *is countable.*
2. *If* $A_1, \dots A_n$ *are countable, then* $A_1 \times \cdots A_n$ *is countable.*
3. *A countable union of countable sets is countable.*

Proof.

1. Let $f : \mathbb{N} \to \mathbb{N}^2$ be defined inductively by $f(0) = (0, 0)$, and

$$f(k) = (a, b) \Rightarrow f(k+1) = \begin{cases} (a+1, b-1) & (b > 0) \\ (0, a+1) & (b = 0) \end{cases}$$

   Then $\forall (a, b) : \mathbb{N}^2 \bullet f\left(\left[\sum_{j=1}^{a+b+1} j\right] + a\right) = (a, b)$, hence f is surjective.[16]

2. By strong induction on n; $n = 0, 1$ are trivial, and $n = 2$ follows immediately from (1).

   For $n > 2$, given $A_1, \dots A_{n+1}$ countable, $A_1 \times \cdots A_n$ is countable by the inductive assumption, and hence $A_1 \times \cdots A_{n+1} = (A_1 \times \cdots A_n) \times A_{n+1}$ is countable by the inductive assumption.

3. Let $(A_i)_{i:I}$ be a countable family of countable sets, with $c_I : I \rightarrowtail \mathbb{N}$ and for $i : I$, $f_i : A_i \rightarrowtail \mathbb{N}$. Define $\pi : \bigcup_{i:I} A_i \to I$ so that $a \in A_{\pi(a)}$, and $F : \bigcup_{i:I} A_i \to \mathbb{N}^2$ by $F(a) = (c_I \pi(a), f_{\pi(a)}(a))$.

   Given $a, b : \bigcup_{i:I} A_i$, if $F(a) = F(b)$ then since c_I is an injection, $\pi(a) = \pi(b)$, and so since $f_{\pi(a)} = f_{\pi(b)}$ is an injection, $a = b$. Hence F is injective.

   The result follows by (1).

□

Corollary 1.6.3.

1. $\mathbb{Q}$ *is countable.*
2. $\mathbb{Q}[X]$ *is countable.*
3. $\mathbb{A}$ *is countable.*

[16] I.e. "rotate $\mathbb{N}^2$ clockwise by $\frac{3\pi}{4}$ and read it like a book".

Proof.

1. Define $f : \mathbb{Q} \rightarrowtail \mathbb{N}^2$ by $f(\frac{p}{q}) = (p, q)$.
2. For $n : \mathbb{N}$, $P_n = \{ f : \mathbb{Q}[X] \mid \deg f \leqslant n \}$ is countable,[17] hence $\mathbb{Q}[X] = \bigcup_{n:\mathbb{N}} P_n$ is a countable union of countable sets.
3. For $f : \mathbb{Q}[X] \setminus \{0\}$, $R_f = \{ z : \mathbb{C} \mid f(z) = 0 \}$ is finite,[18] hence $\mathbb{A} = \bigcup_{f:\mathbb{Q}[X]\setminus\{0\}} R_f$ is a countable union of finite sets.

□

Theorem 1.6.4. $\mathbb{R}$ *is uncountable.*

Proof (Cantor's Diagonal Argument). Given $f : \mathbb{N} \to \mathbb{R}$,

$$\text{for } i : \mathbb{N} \text{ let } c_i = \begin{cases} 4 & \text{if the } i\text{th decimal place of } f(i) \text{ is } 5, \\ 5 & \text{otherwise.} \end{cases}$$

and define $x : \mathbb{R}$ by $x = c_0.c_1c_2\cdots$. $\forall\, i : \mathbb{N} \bullet f(i) \neq x$, as they differ in the ith decimal place. Therefore, f is not surjective. □

Corollary 1.6.5. *There are uncountably many transcendental numbers.*

Proof. Otherwise, $\mathbb{R} = (\mathbb{R} \cap \mathbb{A}) \cup (\mathbb{R} \setminus \mathbb{A})$ is a finite union of countable sets, contradicting Proposition 1.6.2.3 or Theorem 1.6.4. □

Theorem 1.6.6 (Cantor's Theorem)**.** *For any set X, $\nexists f : X \twoheadrightarrow \mathbb{P}\, X$.*

Proof. Given $f : X \to \mathbb{P}\, X$, let $S = \{ x : X \mid x \notin f(x) \}$. Note that $S \in \mathbb{P}\, X$. By construction, $\forall\, x : X$, $x \in f(x) \Leftrightarrow x \notin S$. Therefore, $\nexists\, x : X \bullet f(x) = S$, and f is not surjective. □

Hence, $\#X < \#\,\mathbb{P}\, X < \#\,\mathbb{P}\,\mathbb{P}\, X < \ldots$

Corollary 1.6.7. $\mathbb{P}\,\mathbb{N}$ *is uncountable.*

Proof. Follows immediately from Theorem 1.6.6. □

In particular, if we define $X_0 = \mathbb{N}$ and $X_{n+1} = \bigcup_{k:\mathbb{N}} \mathbb{P}^k\, X_n$, then $\forall\, n, k : \mathbb{N} \bullet \#X_{n+1} > \#\,\mathbb{P}^k\, X_n$.

[17] P_n has a natural injection to $\mathbb{Q}^{n+1}$, which is countable by (1) and Theorem 1.6.2.2.
[18] $\#R_f \leqslant \deg f$. E.g. see Theorem 3.9.6.

2 Numbers

2.1 Euclid's Algorithm

Definition 2.1.1. *For $d, n : \mathbb{Z}$, $d \mid n$ if $\exists\, k : \mathbb{Z} \bullet n = kd$.*

Proposition 2.1.2. *For $a, b, c : \mathbb{Z}$,*

1. *$a \mid 0$, $1 \mid a$, $a \mid a$, and $0 \mid a \Leftrightarrow a = 0$.*
2. *$(a \mid b \land a \mid c) \Rightarrow a \mid (b + c)$.*
3. *$a \mid b \Rightarrow a \mid bc$.*
4. *$(a \mid b \land b \mid c) \Rightarrow a \mid c$.*
5. *$a \mid b \Rightarrow |a| \leqslant |b|$.*
6. *$(a \mid b \land b \mid a) \Rightarrow a = \pm b$.*

Proof.

1. $0 = 0 \cdot a$, $a = a \cdot 1$, $a = 1 \cdot a$, and $\forall\, k : \mathbb{Z} \bullet k \cdot 0 = 0$.
2. $(b = ka \land c = k'a) \Rightarrow b + c = (k + k')a$.
3. $b = ka \Rightarrow bc = (kc)a$.
4. By (3), $a \mid b \Rightarrow a \mid k'b = c$.
5. If $b = ka$, then $|b| = |k|\,|a|$ with $|k| \geqslant 1$, or $a = b = 0$.
6. By (5), $|a| = |b|$.

□

Lemma 2.1.3. $\forall\, n, k : \mathbb{Z} \mid k > 0 \bullet \exists!\, q, r : \mathbb{Z} \mid 0 \leqslant r < k \bullet n = qk + r$.

Proof.

1. Existence: when $n = 0$, $q = r = 0$ is a solution.

   Suppose $n = qk + r$. Then $n + 1 = qk + r + 1$. If $r < k - 1$, then $n + 1 = qk + (r + 1)$ is a solution. Otherwise $r = k - 1$ and so $n = (q + 1)k + 0$ is a solution.

   By induction on n, the result holds for $n \geqslant 0$. For $n < 0$, write $-n = qk + r$. If $r = 0$ then $n = (-q)k + 0$, otherwise $n = (-1 - q)k + (k - r)$.

2. Uniqueness: suppose $qk + r = q'k + r'$, $0 \leqslant r, r' < k$. $(q - q')k + (r - r') = 0$ and so $k \,|\, (r - r')$. It follows that $r - r' = 0$ and then $q = q', r = r'$.

□

This is division with remainders.

Definition 2.1.4. *For $a, b, c : \mathbb{Z}$, c is a **highest common factor**[19] of a and b if:*

1. $c \mid a \wedge c \mid b$.[20]
2. $\forall\, d : \mathbb{N} \bullet (d \mid a \wedge d \mid b) \Rightarrow d \mid c$.[21]

Proposition 2.1.5.

1. *0 is a highest common factor of 0 and 0.*
2. *$\forall\, a : \mathbb{Z}$, a is a highest common factor of a and 0.*

Proof.

1. $0 \mid 0 \wedge 0 \mid 0 \wedge \forall\, d : \mathbb{Z} \bullet \big(d \mid 0 \wedge d \mid 0\big) \Rightarrow d \mid 0$.
2. $a \mid a \wedge a \mid 0 \wedge \forall\, d : \mathbb{Z} \bullet \big(d \mid a \wedge d \mid 0\big) \Rightarrow d \mid a$.

□

Proposition 2.1.6. *$a, b : \mathbb{Z}$ have at most one highest common factor (up to a change of sign).*

Proof. Suppose c and d are both highest common factors of a and b. Then $c \mid d$ and $d \mid c$, so $c = kd$ for some natural number k, and $d = k'c$ for some natural number k'. Hence, $c = kk'c$, so either $k = k' = \pm 1$ and $c = \pm d$, or $c = d = 0$. □

[19] The highest common factor is unique, but we cannot *define* it to be unique.
[20] "A highest common factor divides both numbers,"
[21] "and any other common factor divides it."

Theorem 2.1.7. $\forall\, a, b : \mathbb{N}_+$, *$a$ and b have a highest common factor.*

Proof (Euclid's Algorithm). Wlog $a \geqslant b$.

Let $r_0 = a$ and $r_1 = b$, and for $i \geqslant 2$, define $q_i, r_i : \mathbb{N}$ such that $r_i < r_{i-1}$ and $r_{i-2} = q_i r_{i-1} + r_i$, so long as $r_{i-1}, r_{i-2} > 0$.

Since r_i is a decreasing sequence of natural numbers, $\exists\, n : \mathbb{N} \bullet r_n = 0$ (and thus r_{n+1} is not defined). Let $c = r_{n-1}$.

Claim: $c \mid a \wedge c \mid b$.

Proof of claim: Since $r_n = 0$, $c \mid r_n \wedge c \mid r_{n-1}$.

Also, since $r_{i+2} = r_i - q_i r_{i+1}$ for $i \leqslant n-2$, $\big(c \mid r_{i+2} \wedge c \mid r_{i+1}\big) \Rightarrow c \mid r_i$.

By *backwards* strong induction on i, it follows that $\forall\, i : \mathbb{N} \mid i \leqslant n \bullet c \mid r_i$, and hence $c \mid a \wedge c \mid b$.

Claim: If $d \mid a \wedge d \mid b$ for some natural number d, then $d \mid c$.

Proof of claim: By assumption, $d \mid r_0 \wedge d \mid r_1$.

Also, since $r_{i+2} = r_i - q_i r_{i+1}$ for $i \leqslant 2$, $\big(d \mid r_i \wedge d \mid r_{i+1}\big) \Rightarrow d \mid r_{i+2}$.

By strong induction on i, it follows that $\forall\, i : \mathbb{N} \mid i \leqslant n \bullet d \mid r_i$, and hence $d \mid c$ (as $c = r_{n-1}$).

Therefore, c is a highest common factor of a and b.[22] □

Corollary 2.1.8. $\forall\, a, b : \mathbb{Z}$ *there is a unique non-negative highest common factor of a and b.*

Proof. We already know the result for $a, b \geqslant 0$. Then, it is enough that a highest common factor of $|a|$ and $|b|$ is also a highest common factor of a and b. Uniqueness follows from Proposition 2.1.6. □

Definition 2.1.9. *For $a, b : \mathbb{Z}$,*

1. $\mathrm{HCF}(a) = |a|$.
2. $\mathrm{HCF}(a, b)$ *is the (non-negative) highest common factor of a and b.*
3. *For $n \geqslant 2$, $a_i : \mathbb{Z}$,* $\mathrm{HCF}(a_1, \ldots a_{n+1}) = \mathrm{HCF}(\mathrm{HCF}(a_1, \ldots a_n), a_{n+1})$.

$\mathrm{HCF}(a_1, \ldots a_n)$ is a true generalisation of $\mathrm{HCF}(a, b)$:

Proposition 2.1.10.

1. $\forall\, i : \mathbb{N} \mid 1 \leqslant i \leqslant n \bullet \mathrm{HCF}(a_1, \ldots a_n) \mid a_i$.

[22] Note that this proof is *constructive*, as it provides an algorithm for computing c. It is easy to see that the algorithm will terminate in at most b steps; in fact, the worst-case complexity of the algorithm is $\mathrm{O}(\log b)$, when a, b are consecutive Fibonacci numbers.

2. $\forall\, d : \mathbb{Z} \bullet \left(\forall\, i : \mathbb{N} \mid 1 \leqslant i \leqslant n \bullet d \,\middle|\, a_i\right) \Rightarrow d \,\middle|\, \mathrm{HCF}(a_1, \ldots a_n)$.

Proof. By induction on n. $n = 1$ is trivial, and $n = 2$ is Definition 2.1.4.2. Let $h = \mathrm{HCF}(a_1, \ldots a_n)$, and $h' = \mathrm{HCF}(a_1, \ldots a_{n+1})$. Suppose the result holds for n.

1. $h' \,\middle|\, h \wedge h' \,\middle|\, a_{n+1}$ by Definition 2.1.9. Then, for $1 \leqslant i \leqslant n$, $h' \,\middle|\, h \,\middle|\, a_i$ by the inductive assumption.

2. Given $d \,\middle|\, a_i$ for $1 \leqslant i \leqslant n+1$, $d \,\middle|\, h$ by the inductive assumption, and $d \,\middle|\, a_{n+1}$, hence by Definition 2.1.4, $d \,\middle|\, h'$.

□

Definition 2.1.11.

1. $a, b : \mathbb{Z}$ *are* ***coprime*** *(or* ***relatively prime****) if* $\mathrm{HCF}(a, b) = 1$.

2. $S : \mathbb{P}\,\mathbb{Z}$ *is coprime if* $\forall\, a, b : S \mid a \neq b$, a, b *are coprime.*[23]

Corollary 2.1.12. $\forall\, a, b : \mathbb{Z} \bullet \exists\, x, y : \mathbb{Z} \bullet ax + by = \mathrm{HCF}(a, b)$.

Proof (Extended Euclidean Algorithm). If a or b is 0, the result is trivial. Wlog $a, b > 0$.

Let r_i, n be defined as in the proof of Theorem 2.1.7. By definition, $r_0 = a \cdot 1 + b \cdot 0$ and $r_1 = a \cdot 0 + b \cdot 1$.

If $r_{i-2} = ax + by$ and $r_{i-1} = ax' + by'$ for some natural number $i \geqslant 2$ and integers x, y, x', y', then $r_i = r_{i-2} - q_k r_{i-1} = a(x - q_k x') + b(y - q_k y')$.

By strong induction on i, it follows that $\mathrm{HCF}(a, b) = r_{n-1}$ can be written in this form.[24] □

Theorem 2.1.13. [25]

$$\forall\, n : \mathbb{N}_+ \bullet \forall\, a_1, \ldots a_n : \mathbb{Z} \bullet \exists\, x_1, \ldots x_n : \mathbb{Z} \bullet \sum_{j=1}^{n} a_j x_j = \mathrm{HCF}(a_i)$$

[23] This is not the same as saying $\mathrm{HCF}(S) = 1$; besides not having defined HCF for infinite sets, $\mathrm{HCF}(2, 3, 6) = 1$ but $\mathrm{HCF}(2, 6) = 2$.

[24] Again, the proof is constructive.

[25] This is a direct generalisation of Corollary 2.1.12.

Proof. By induction on n. The result for $n = 1$ is trivial, and the result for $n = 2$ is Corollary 2.1.12.

Suppose that $\mathrm{HCF}(a_1, \dots a_n) = \sum_{i=1}^{n} a_i x_i$. By Corollary 2.1.12,

$$\exists\, x, y : \mathbb{Z} \bullet \mathrm{HCF}(\mathrm{HCF}(a_1, \dots a_n), a_{n+1}) = \mathrm{HCF}(a_1, \dots a_n) \cdot x + a_{n+1} y$$

And so

$$\mathrm{HCF}(a_1, \dots a_{n+1}) = \left(\sum_{i=1}^{n} a_i (x x_i) \right) + a_{n+1} y$$

□

2.2 Integer Linear Equations

An **integer linear equation** in one variable $x : \mathbb{Z}$ is of the form $ax = b$ for $a, b : \mathbb{Z} \mid a \neq 0$. This equation has a solution iff $a \,\big|\, b$, as this is precisely Definition 2.1.1. The solution is necessarily unique.[26]

We can give a similar condition for an integer linear equation $ax + by = c$ in two variables $x, y : \mathbb{Z}$, with constants $a, b, c : \mathbb{Z} \mid a, b \neq 0$, to have a solution.

Corollary 2.2.1.

$$\forall\, a, b, c : \mathbb{Z} \mid a, b \neq 0 \bullet (\exists\, x, y : \mathbb{Z} \bullet ax + by = c) \Leftrightarrow \mathrm{HCF}(a, b) \,\big|\, c$$

Proof. Negating x or y if necessary, wlog $a, b > 0$.

Suppose $\exists\, x, y : \mathbb{Z} \bullet c = ax + by$. Since $\mathrm{HCF}(a, b) \,\big|\, a \wedge \mathrm{HCF}(a, b) \,\big|\, b$, it follows that $\mathrm{HCF}(a, b) \,\big|\, c$.

Conversely, suppose $c = k \cdot \mathrm{HCF}(a, b)$ for some $k : \mathbb{Z}$. Then by Corollary 2.1.12, $\exists\, x, y : \mathbb{Z} \bullet a(kx) + b(ky) = k \cdot \mathrm{HCF}(a, b) = c$.[27] □

Note that a solution x, y cannot be unique, as $a(x + kb) + b(y - ka) = c$ is a distinct solution $\forall\, k : \mathbb{Z}$.

A similar result can be shown for integer linear equations in any number of variables.

Theorem 2.2.2. [28] $\forall\, n : \mathbb{N}_+ \bullet \forall\, a_1, \dots a_n, b : \mathbb{Z} \mid a_i \neq 0 \bullet$

$$\left(\exists\, x_1, \dots x_n : \mathbb{Z} \bullet \sum_{j=1}^{n} a_j x_j = b \right) \Leftrightarrow \mathrm{HCF}(a_i) \,\big|\, b$$

[26] Because a has a multiplicative inverse $\frac{1}{a} \in \mathbb{Q}$.

[27] And when this solution exists, we have an algorithm to construct it.

[28] "For all n, an integer linear equation in n variables has a solution iff the HCF of the coefficients divides the constant term."

Proof. Suppose the x_i exist. By Proposition 2.1.10.1, $\forall\, j \bullet \mathrm{HCF}(a_i) \,\big|\, a_j x_j$, and so it follows that $\mathrm{HCF}(a_i) \,\big|\, b$.

Conversely, suppose $b = k \cdot \mathrm{HCF}(a_i)$ for some $k : \mathbb{Z}$. Then by Theorem 2.1.13, $\exists\, x_i \bullet \sum_{j=1}^{n} a_j(kx_j) = b$. □

2.3 Congruence Modulo n

Definition 2.3.1. *For $a, b : \mathbb{Z}, n : \mathbb{N}_+$, $a \equiv b \pmod{n}$ if $n \,\big|\, (b - a)$.*

a and b are said to be "congruent modulo n."

Proposition 2.3.2. *$\equiv \pmod{n}$ is an equivalence relation.*

Proof. $\forall\, a, b, c : \mathbb{Z}$,

1. Refexivity: $n \,\big|\, (a - a)$.
2. Symmetry: $n \,\big|\, (b - a) \Rightarrow n \,\big|\, (a - b)$.
3. Transitivity: $\big(n \,\big|\, (b - a) \wedge n \,\big|\, (c - b)\big) \Rightarrow n \,\big|\, \big((c - b) - (a - b)\big)$.

□

Definition 2.3.3. *$\mathbb{Z}_n$ is the set of equivalence classes for $\equiv \pmod{n}$.*

These equivalence classes are all of the form $[a]_n = \{\, k : \mathbb{Z} \bullet a + kn \,\}$. By Lemma 2.1.3, $\mathbb{Z}_n = \{[0]_n, \ldots [n-1]_n\}$, and $\#\mathbb{Z}_n = n$.

Proposition 2.3.4. *For $a, b, c, d : \mathbb{Z}$, $n : \mathbb{N}_+$, if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then:*

1. *$a + c \equiv b + d \pmod{n}$.*
2. *$ac \equiv bd \pmod{n}$.*
3. *$\forall\, k : \mathbb{N}_+ \bullet a^k \equiv b^k \pmod{n}$.*

Proof. Let $b = a + pn$, $d = c + qn$ for $p, q : \mathbb{Z}$.

1. $b + d = a + c + (p + q)n$.
2. $bd = ac + (pc + qa + pqn)n$.
3. By Theorem 1.3.4, $b^k = (a + pn)^k = a^k + \left(\sum_{i=0}^{k-1} \binom{k}{i} a^i p^{k-i} n^{k-i-1} \right) n$.

□

Definition 2.3.5. $\forall [a]_n, [b]_n : \mathbb{Z}_n, k : \mathbb{N}_+$,

1. $[a]_n + [b]_n = [a+b]_n$.
2. $[a]_n \cdot [b]_n = [ab]_n$.
3. $[a]_n^k = [a^k]_n$

These are well-defined[29] by Proposition 2.3.4. Associativity, commutativity and distributivity follow immediately from the same properties in $\mathbb{Z}$.[30]

Where it is clearer, we will write $a : \mathbb{Z}_n$ to mean $[a]_n : \mathbb{Z}_n$ and $a : \mathbb{Z}$ interchangeably.

Proposition 2.3.6. *if* $a \equiv b \pmod{n}$, *then* $\mathrm{HCF}(a, n) = \mathrm{HCF}(b, n)$.[31]

Proof. Let $h = \mathrm{HCF}(a, n), h' = \mathrm{HCF}(b, n)$ and $b = a + kn$. $h \mid a \wedge h \mid n$, so $h \mid (a + kn)$. Similarly, $h' \mid a$. $(h \mid b \wedge h \mid n) \Rightarrow h \mid h'$, and $(h' \mid a \wedge h' \mid n) \Rightarrow h' \mid h$. Therefore $h = h'$. □

It follows that for $[a]_n : \mathbb{Z}_n$, $\mathrm{HCF}(a, n)$ is well-defined.

Definition 2.3.7. $\mathbb{Z}_n^* = \{\, a : \mathbb{Z}_n \mid \mathrm{HCF}(a, n) = 1 \,\}$.

Proposition 2.3.8. *For* $a : \mathbb{Z}_n$,

1. $ab \equiv 1 \pmod{n}$ *has a unique solution* $b : \mathbb{Z}_n^*$ *iff* $a \in \mathbb{Z}_n^*$.
2. $ab \equiv 0 \pmod{n}$ *has a solution* $b \not\equiv 0 \pmod{n}$ *iff* $a \notin \mathbb{Z}_n^*$.

Proof.

1. By Corollary 2.1.12, a solution exists iff $\mathrm{HCF}(a, n) = 1$.

   If $ab_1 \equiv ab_2 \equiv 1 \pmod{n}$ then $b_1 \equiv ab_2b_1 \equiv ab_1b_2 \equiv b_2 \pmod{n}$, so the solution is unique modulo n.

2. Let $f(x : \mathbb{Z}_n) = ax$. By Corollary 2.1.12, $1 \notin \operatorname{ran} f$, and so f is not surjective. Since $\mathbb{Z}_n$ is finite, f is not injective, so $\exists\, x, y : \mathbb{Z}_n \mid x \neq y \bullet ax = ay$. Hence, $a(y - x) \equiv 0 \pmod{n}$ but $y - x \not\equiv 0 \pmod{n}$.

   Conversely, suppose $ab \equiv 0 \pmod{n}$, with $b \not\equiv 0 \pmod{n}$. If $a \in \mathbb{Z}_n^*$ then $\exists\, p : \mathbb{Z}_n \bullet ap \equiv 1 \pmod{n}$, but then $p \cdot 0 \equiv pab \equiv b \not\equiv 0 \pmod{n}$. Therefore $a \notin \mathbb{Z}_n^*$.

□

[29] I.e. we get the same results even if we choose different representatives b, d from the equivalence classes $[a]_n, [c]_n$.

[30] Therefore, $\mathbb{Z}_n$ is a ring.

[31] In particular, a, n are coprime iff b, n are coprime.

2.4 Prime Numbers

Definition 2.4.1.

1. $p : \mathbb{N} \mid p > 1$ *is a* ***prime number*** *(or a* ***prime****) if*

$$\forall\, a, b : \mathbb{Z} \bullet p \,\big|\, ab \Rightarrow \big(p \,\big|\, a \vee p \,\big|\, b\big)$$

2. $n : \mathbb{N} \mid n > 1$ *is a* ***composite number*** *if* n *is not a prime number.*

We also say "p is prime" or "n is composite".

Lemma 2.4.2. *If* $p : \mathbb{N}$ *is prime, then* $\forall\, d : \mathbb{N} \bullet d \,\big|\, p \Leftrightarrow (d = 1 \vee d = p)$.

Proof. Suppose $d \,\big|\, p$ but $d \neq 1, p$. By Proposition 2.1.2.5, $1 < d < p$ and so $p = kd$ with $1 < k < p$. Now $p \,\big|\, kd \Rightarrow \big(p \,\big|\, k \vee p \,\big|\, d\big)$, contradicting $k, d < p$.
The converse is trivial. □

Proposition 2.4.3. *Distinct prime numbers are coprime.*

Proof. Let $p \neq q$ be primes, $h = \mathrm{HCF}(p, q)$. $h \,\big|\, p \Rightarrow (h = 1 \vee h = p)$, and $h \,\big|\, q \Rightarrow (h = 1 \vee h = q)$. Therefore $h = 1$. □

Proposition 2.4.4. *If* p *is a prime number, then*

$$\forall\, n : \mathbb{N}_+ \bullet \forall\, a_1, \ldots a_N : \mathbb{Z} \bullet \left(p \,\Big|\, \prod_{j=1}^{N} a_j \Rightarrow \exists\, i : \mathbb{N} \mid 1 \leqslant i \leqslant N \bullet p \,\big|\, a_i \right)$$

Proof. By induction on N. $N = 1$ is trivial, $N = 2$ is Definition 2.4.1.
Suppose $p \,\big|\, \prod_{j=1}^{N+1} a_j$. By Definition 2.4.1, $\left(p \,\big|\, \prod_{j=1}^{N} a_j\right) \vee p \,\big|\, a_{N+1}$. □

Corollary 2.4.5. $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$.

Proof. Follows immediately from Lemma 2.4.2. □

Therefore, $\mathbb{Z}_p$ is a field.

Proposition 2.4.6. *Every natural number* $n > 1$ *has a prime factor.*

Proof. Let $F = \{\, k : \mathbb{N} \mid k \,\big|\, n \,\}$. $F \supsetneq \{1\}$, and so let $p = \min(F \setminus \{1\})$. $\forall\, d : \mathbb{N} \mid 1 < d < p \bullet d \nmid p$, as $d \,\big|\, p \Rightarrow d \,\big|\, n$ and p is minimal. Therefore, by Lemma 2.4.2, p is prime. □

In particular, every composite n has a factorisation $n = pk$, with $1 < p, k < n$.[32]

[32] Hence for composite n, $\mathbb{Z}_n$ is not an **integral domain**.

Corollary 2.4.7. *For $a, b, c : \mathbb{N}_+$, if a, c and b, c are coprime, then ab, c are coprime.*

Proof. Suppose $\text{HCF}(ab, c) > 1$. By Proposition 2.4.6, $\text{HCF}(ab, c)$ has a prime factor p, with $p \mid ab \land p \mid c$. It follows from Definition 2.4.1 that $p \mid a \lor p \mid b$, and so either a, c are not coprime, or b, c are not coprime. □

Theorem 2.4.8. *There are infinitely many prime numbers.*

Proof. Suppose there are finitely many primes $p_1, \ldots p_N$, for some $N : \mathbb{N}$.[33] Let $P = 1 + \prod_{i=1}^{N} p_i$. By Proposition 2.4.6,[34] P has a prime factor q. However, $\forall\, i : \mathbb{N} \mid 1 \leqslant i \leqslant N \bullet p_i \nmid P$, and so the list was not complete, as it did not contain the prime number q. □

Theorem 2.4.9 (Fundamental Theorem of Arithmetic)**.** $\forall\, n : \mathbb{N}_+$, *$n$ has a unique*[35] *representation as a product of primes.*[36]

Proof. By strong induction on n. $n = 1$ has a unique representation as the empty product.

1. Existence: for $n > 1$, by Proposition 2.4.6 n has a prime factor p_0, and so $n = kp_0$ for some $k : \mathbb{N}_+ \mid k < n$. By the inductive assumption, $k = p_1 \cdots p_N$ for some $N : \mathbb{N}$, and so $n = p_0 p_1 \cdots p_N$.

2. Uniqueness: suppose $n = p_1 \cdots p_N = q_1 \cdots q_N$ for p_i, q_i prime. By Proposition 2.4.4, $p_N \mid q_j$ for some j. By Proposition 2.4.3, $p_N = q_j$ and by renumbering the q_i, $p_N = q_N$ and $p_1 \cdots p_{N-1} = q_1 \cdots q_{N-1} < n$. By the inductive assumption, $p_1, \ldots p_{N-1}$ and $q_1, \ldots q_{N-1}$ are the same (up to re-numbering).

□

[33] Note that this proof *does* work for $N = 0$, as $1 +$ the empty product $= 2$ has a prime factor not in the empty list.

[34] Note that $P > 1$ by definition.

[35] The representation is unique up to re-ordering the primes.

[36] Therefore, $\mathbb{Z}$ is a **unique factorisation domain**.

2.5 Linear Congruence Equations

A **linear congruence equation** in m variables x_i is of the form

$$\sum_{j=1}^{m} a_j x_j \equiv b \pmod{n}$$

Proposition 2.5.1.

1. *$ax \equiv b \pmod{n}$ has a solution iff $\mathrm{HCF}(a, n) \mid b$.*
2. *$ax \equiv b \pmod{n}$ has a unique solution iff $a \in \mathbb{Z}_n^*$.*
3. *A linear congruence equation in m variables x_i has a solution iff $\mathrm{HCF}(a_1, \ldots a_m, n) \mid b$.*

Proof.

1. By Corollary 2.2.1.
2. Suppose $a \in \mathbb{Z}_n^*$. By Proposition 2.3.8.1, a has a multiplicative inverse $p : \mathbb{Z}_n$, and so $x = pb$ is a solution. Also, if $ax \equiv ax' \equiv b \pmod{n}$, then $x \equiv apx \equiv apx' \equiv x' \pmod{n}$.

   Otherwise, suppose $a \notin \mathbb{Z}_n^*$. By Proposition 2.3.8.2, $\exists\, p : \mathbb{Z}_n \bullet ap \equiv 0 \pmod{n} \land p \not\equiv 0 \pmod{n}$. It follows that if x is a solution, $x + p$ is a distinct solution modulo n.
3. The congruence has a solution iff the corresponding integer linear equation $\left(\sum_{j=1}^{m} a_j x_j\right) + nx_{m+1} = b$ in $m + 1$ variables x_i has a solution.

   The result follows from Theorem 2.2.2.

□

Lemma 2.5.2. *For $a_1, a_2, b_1, b_2 : \mathbb{Z}, n_1, n_2 : \mathbb{N}_+ \mid \mathrm{HCF}(n_1, n_2) = 1$, the simultaneous congruences $a_i x \equiv b_i \pmod{n_i}$ have a solution x iff each congruence individually has a solution.*

Proof. Suppose for $i = 1, 2$, $\exists\, x_i : \mathbb{Z} : a_i x_i \equiv b_i \pmod{n_i}$. By Corollary 2.5.1.2, $\exists\, p_1, p_2 : \mathbb{Z} \bullet p_1 n_1 \equiv 1 \pmod{n_2} \land p_2 n_2 \equiv 1 \pmod{n_1}$. Then $x = p_2 n_2 x_1 + p_1 n_1 x_2$ has $x \equiv x_1 \pmod{n_1} \land x \equiv x_2 \pmod{n_2}$, solving both equations simultaneously.

The converse is trivial. □

If x_1, x_2 are unique modulo n_1, n_2 respectively, it follows that x is unique modulo $n_1 n_2$.

Theorem 2.5.3 (Chinese Remainder Theorem)**.** *A set of $m : \mathbb{N}_+$ simultaneous linear congruence equations $a_i x \equiv b_i \pmod{n_i}$ in one variable x, with n_i coprime, has a solution iff each congruence individually has a solution.*

Proof. By induction on m. $m = 1$ follows from Proposition 2.5.1.1, and $m = 2$ is Lemma 2.5.2.

Given m simultaneous congruences, we can replace two of them with the single congruence $x \equiv p_2 n_2 x_1 + p_1 n_1 x_2 \pmod{n_1 n_2}$, as in the proof of Lemma 2.5.2. By Corollary 2.4.7, for $i > 2$, $n_1 n_2, n_i$ are coprime. By the inductive assumption, the resulting $m - 1$ simultaneous congruences have a solution.

The converse is trivial. □

By Proposition 2.5.1.2, if the individual solutions the solutions x_i are unique modulo n_i, then x is unique modulo $\prod n_i$.[37]

[37] A practical application of this result is that if an army of N soldiers knows the remainders r_i when the soldiers are divided into groups of p_i (for sufficiently many primes that $\prod p_i > N$), then the exact size of the army can be computed from the simultaneous congruences $N \equiv r_i \pmod{p_i}$.

3 Groups

3.1 Groups

Definition 3.1.1 (Group Axioms)**.** *If G is a set, and $\_ \cdot \_ : G \times G \to G$ is a binary operator on G, then the pair $(G, \cdot)$ is a **group** if:*

1. $\forall\, a, b, c : G \bullet (a \cdot b) \cdot c = a \cdot (b \cdot c)$.
2. $\exists\, e : G \bullet \forall\, g : G \bullet e \cdot g = g \cdot e = g$.
3. $\forall\, g : G \bullet \exists\, g^{-1} : G \bullet g^{-1} \cdot g = g \cdot g^{-1} = e$.

e is the **identity element**, and g^{-1} is the **inverse** of g. The binary operator is **group multiplication**, and the symbol $\cdot$ is usually omitted. For $k : \mathbb{Z}$ we will write g^k to mean the product of $|k|$ copies of g or g^{-1}, with $g^0 = e$.[38] Where it is clearer, we will write G to mean a set G and a group $(G, \cdot)$ interchangeably. We may write e_G to mean the identity element of a group G in particular.

Proposition 3.1.2.

1. $\forall\, g, h : G \bullet gh = g \Leftrightarrow hg = g \Leftrightarrow h = e$.[39]
2. $\forall\, g, h : G \mid gh = e \Leftrightarrow hg = e \Leftrightarrow h = g^{-1}$.[40]

Proof.

1. $gh = g \Rightarrow g^{-1}gh = g^{-1}g \Rightarrow h = e$. $hg = g$ is similar.
2. $gh = e \Rightarrow ghg = g$. By (1), $hg = e$.

   Suppose $h_1, h_2 : G$ are inverses of g. Then $h_1 = h_1 e = h_1 g h_2 = e h_2 = h_2$.

□

Note that for $g, h : G$, $(h^{-1}g^{-1})(gh) = h^{-1}(g^{-1}g)h = h^{-1}h = e$, and so $(gh)^{-1} = h^{-1}g^{-1}$.

If G is Abelian, where it is clearer we will write 0 to mean e, $g + h$ to mean $g \cdot h$, and kg to mean g^k.

[38] The usual exponent rules follow.

[39] I.e. the identity element is unique, and is the only **left-identity** and the only **right-identity**.

[40] I.e. the inverse of g is unique, and is the only **left-inverse** and the only **right-inverse**.

Definition 3.1.3. $\mathbb{1} = (\{e\}, \cdot)$, *with* $e \cdot e = e$, *is the* ***trivial group****.*

Definition 3.1.4.

1. *For* $g : G$, $\langle g \rangle = \{\, k : \mathbb{Z} \bullet g^k \,\}$.
2. G *is* ***cyclic*** *if* $\exists\, g : G \bullet \langle g \rangle = G$.
3. *For* $n : \mathbb{N}_+$, $C_n = (\mathbb{Z}_n, +)$.

If $G = \langle g \rangle$ then g is a **generator**.

3.2 Commutativity

Definition 3.2.1.

1. *If* $g, h : G \mid gh = hg$, *then* g, h ***commute****.*
2. *If* $\forall\, g, h : G \bullet gh = hg$, *then* G *is* ***Abelian****.*

Definition 3.2.2.

1. *For* $g : G$, $\mathrm{C}_G(g) = \{\, h : G \mid gh = hg \,\}$ *is the* ***centralizer*** *of* g.
2. *For* $H : \mathbb{P}\, G$, $\mathrm{C}_G(H) = \{\, g : G \mid (\forall\, h : H \bullet gh = hg) \,\}$.
3. $\mathrm{Z}(G) = \mathrm{C}_G(G)$ *is the* ***center*** *of* G.

Where it is clearer, we will write C to mean C_G.

3.3 Homomorphisms

Definition 3.3.1.

1. $\theta : G \to H$ *is a* ***homomorphism*** *if* $\forall\, a, b : G \bullet \theta(a \cdot b) = \theta(a) \cdot \theta(b)$.
2. *An* ***isomorphism*** *is a bijective homomorphism.*
3. $G \cong H$ *(*G, H *are* ***isomorphic****) if there is an isomorphism* $\theta : G \to H$.

Proposition 3.3.2. *For a homomorphism $\theta : G \to H$,*

1. $\theta(e_G) = e_H$,
2. $\forall\, g : G \bullet \theta(g^{-1}) = \theta(g)^{-1}$.

Proof. Given $g : G$,

1. $\theta(g) = \theta(e_G g) = \theta(e_G)\theta(g)$, so by Proposition 3.1.2.1 $\theta(e_G) = e_H$.
2. $e_H = \theta(e_G) = \theta(gg^{-1}) = \theta(g)\theta(g^{-1})$, and so by Proposition 3.1.2.2 $\theta(g^{-1}) = \theta(g)^{-1}$.

□

Proposition 3.3.3. $\cong$ *is an equivalence relation.*

Proof.

1. Reflexivity: $\mathrm{id}_G : G \to G$ is trivially an isomorphism.
2. Symmetry: suppose $\theta : G \to H$ is an isomorphism. Since θ is a bijection, θ^{-1} is a bijection. Given $a, b : H$, let $a = \theta(c)$ and $b = \theta(d)$. Then $\theta^{-1}(ab) = \theta^{-1}(\theta(c)\theta(d)) = \theta^{-1}(\theta(cd)) = cd = \theta^{-1}(a)\theta^{-1}(b)$. Hence, θ is a homomorphism.
3. Transitivity: suppose $\theta : G \to H$, $\phi : H \to K$ are isomorphisms. Then $\phi\theta$ is a bijection, and for $a, b : G$, $\phi\theta(ab) = \phi(\theta(a)\theta(b)) = \phi\theta(a)\phi\theta(b)$ and so $\phi\theta$ is a homomorphism.

□

Definition 3.3.4. *For a homomorphism $\theta : G \to H$, the* ***kernel*** *of θ is* $\ker\theta = \{\, g : G \mid \theta(g) = e_H \,\}$.

Proposition 3.3.5. *θ is injective iff* $\ker\theta \cong \mathbb{1}$.

Proof. Suppose $\ker\theta = \{e_G\}$. Then $\forall\, g, h : G \bullet \theta(g) = \theta(h) \Rightarrow \theta(gh^{-1}) = \theta(g)\theta(h)^{-1} = e_H \Rightarrow gh^{-1} = e_G \Rightarrow g = h$.

The converse is trivial. □

Definition 3.3.6. *A homomorphism $\theta : G \to H$ is* ***trivial*** *if* $\ker\theta = G$.

Equivalently, θ is trivial iff $\mathrm{ran}\,\theta \cong \mathbb{1}$.

3.4 Subgroups

Definition 3.4.1. *For $H : \mathbb{P}\, G$, $(H, \cdot)$ is a **subgroup** of $(G, \cdot)$ if:*

1. $e \in H$,
2. $\forall\, g : H \bullet g^{-1} \in H$,
3. $\forall\, g, h : H \bullet gh \in H$.

*We write $H \leqslant G$. If $H \neq G$, then H is a **proper subgroup** of G, and we write $H < G$.*

Note that if $H \leqslant G$, then H is a group. Where it is clearer, we will write $H \leqslant G$ if $H \cong H' \leqslant G$.

Definition 3.4.2. $G_{\leqslant} = \{\, H : \mathbb{P}\, G \mid H \leqslant G \,\}$.[41]

Proposition 3.4.3. $\langle g \rangle \leqslant G$.

Proof. For $k, k' : \mathbb{Z}$, $e = g^0$, $(g^k)^{-1} = g^{-k}$, and $g^k g^{k'} = g^{k+k'}$. □

Proposition 3.4.4. *If $\theta : G \to K$ is a homomorphism, $(H \lhd \theta) : H \to K$ is a homomorphism.*

Proof. Trivial. □

Proposition 3.4.5. *If $\theta : G \to H$ is a homomorphism,*

1. $\ker \theta \leqslant G$,
2. $\operatorname{ran} \theta \leqslant H$.

Proof.

1. $\theta(e_G) = e_H$, and for $g_1, g_2 : \ker \theta$, $\theta(g_1^{-1}) = \theta(g_1)^{-1} = e^{-1} = e$, and $\theta(g_1 g_2) = \theta(g_1)\theta(g_2) = e^2 = e$.
2. $e_H = \theta(e_G)$, for $h_1, h_2 : \operatorname{ran} \theta$, $\exists\, g_i : G \bullet \theta(g_i) = h_i$, so $h_1^{-1} = \theta(g_1^{-1})$, and $h_1 h_2 = \theta(g_1 g_2)$.

□

[41] Note that for $H, K : G_{\leqslant}$, $H \cong K \not\Rightarrow H = K$.

3.5 Cosets

Definition 3.5.1.

1. *For* $A : \mathbb{P}\, G, g : G$, $gA = \{\, a : A \bullet ga \,\}$, *and* $Ag = \{\, a : A \bullet ag \,\}$.
2. *For* $A, B : \mathbb{P}\, G, g : G$, $AB = \{\, a : A, b : B \bullet ab \,\}$.
3. *For* $H \leqslant G$, ${}_GH = \{\, g : G \bullet gH \,\}$ *is the set of* ***left-cosets*** *of* H.
4. *For* $H \leqslant G$, $H_G = \{\, g : G \bullet Hg \,\}$ *is the set of* ***right-cosets*** *of* H.

Proposition 3.5.2. *For* $A, B : \mathbb{P}\, G$, $g, h : G$,

1. $eA = Ae = A$.
2. $(gh)A = g(hA)$, $(Ag)h = A(gh)$, *and* $(gA)h = g(Ah)$.
3. $(gA)B = g(AB)$, $(AB)g = A(Bg)$, *and* $(Ag)B = A(gB)$.
4. $\#A = \#gA = \#Ag$.

Proof. By associativity and inverses in G. □

Lemma 3.5.3. *For* $H \leqslant G$, ${}_GH$ *and* H_G *are partitions of* G.

Proof. Let $R : G \leftrightarrow G$ be defined by gRh iff $g \in hH$. R is an equivalence relation, as for $a, b, c : G$,

1. Reflexivity: $e \in H \Rightarrow a = ae \in aH$.
2. Symmetry: $a \in bH \Rightarrow (\exists\, g : H \bullet a = bg)$
   $\Rightarrow \left(\exists\, g^{-1} : H \bullet b = ag^{-1}\right) \Rightarrow b \in aH$.
3. Transitivity: $(a \in bH \land b \in cH)$
   $\Rightarrow (\exists\, g, h : H \bullet a = bg \land b = ch)$
   $\Rightarrow (\exists\, hg : H \bullet a = c(hg)) \Rightarrow a \in cH$.

H_G is similar. □

Corollary 3.5.4. *For $H \leqslant G$, $a, b : G$, the following are equivalent*[42]*:*

1. $a \in bH$,
2. $b^{-1}a \in H$,
3. $aH = bH$,
4. $b^{-1}aH = H$.

Proof.

- (1) $\Leftrightarrow$ (2): $a \in bH \Leftrightarrow b^{-1}a \in b^{-1}bH = H$.
- (1) $\Rightarrow$ (3): By Lemma 3.5.3, $a \in bH \Rightarrow aH \cap bH \neq \emptyset \Rightarrow aH = bH$.
- (3) $\Leftrightarrow$ (4): $aH = bH \Leftrightarrow b^{-1}aH = b^{-1}bH = H$.
- (3) $\Rightarrow$ (1): $a = ae \in aH$, and $aH = bH$, so $a \in bH$.

□

In particular, for $a : G$, $aH = eH = H$ iff $a \in H$.

Proposition 3.5.5. *For $H \leqslant G$,*

$$\forall\, A : \mathbb{P}\, G \mid A \neq \emptyset \bullet AH = H \Leftrightarrow HA = H \Leftrightarrow A \subseteq H$$

Proof. If $A \subseteq H$, then for $a : A, h : H$, $a \in H$ and so $\forall\, ah : AH \bullet ah \in H$. Also, given $h : H$, choose $a : A$, then $a^{-1}h \in H$ and so $h = aa^{-1}h \in AH$.

Otherwise, $\exists\, a : A \mid a \notin H$, so $a = ae \in AH$ and $AH \neq H$.

Similarly for $HA = A$. □

In particular, $HH = H$.

3.6 Orders

Definition 3.6.1. *For $g : G$, $|g|$ is the least $n : \mathbb{N}_+$ such that $g^n = e$. If there is no such n, $|g| = \infty$.*[43]

$|g|$ is the **order** of g.

Proposition 3.6.2. $\forall\, g : G, n : \mathbb{Z} \mid |g| \neq \infty \bullet g^n = e \Leftrightarrow |g| \,\big|\, n$.

Proof. Suppose $g^n = e$. By Lemma 2.1.3, $n = q\,|g| + r$ for $0 \leqslant r < |g|$ and $e = g^n = (g^{|g|})^q g^r = e^q g^r = g^r$. It follows that $r = 0$.

Conversely, if $n = k\,|g|$ then $g^n = (g^{|g|})^k = e$. □

[42] Similarly for right-cosets.

[43] ∞ is not a number, but $\infty > n$ for any number n.

Proposition 3.6.3. $|g| = \#\langle g \rangle$.

Proof. If $|g| \neq \infty$, the result follows by Lemma 2.1.3 and Proposition 3.6.2. If $|g| = \infty$, then $g^a = g^b \Rightarrow e = g^{b-a} \Rightarrow a = b$ and so $f(k : \mathbb{Z}) = g^k$ is a bijection.[44] □

In particular, $\forall\, g : G,\ g^0, g^1, \ldots g^{|g|-1}$ are distinct, and G is cyclic iff $\exists\, g : G \bullet |g| = \#G$.

Proposition 3.6.4. *G is cyclic iff $G \cong \mathbb{Z}$ or $G \cong C_n$ for some $n : \mathbb{N}_+$.*

Proof. Suppose $G = \langle g \rangle$.

If $|g| = \infty$, let $f(k : \mathbb{Z}) = g^k$. Otherwise, let $f(k : \mathbb{Z}_{|g|}) = g^k$. Either way, by Proposition 3.6.3 f is an isomorphism.

Conversely, $\mathbb{Z} = \langle 1 \rangle$ and $\mathbb{Z}_n = \langle [1]_n \rangle$. □

Note that f depends on the choice of the generator g, which is not unique for $n > 2$.

Lemma 3.6.5. *If $a, b : G$ commute, with $|a|, |b|$ coprime, then $|ab| = |a|\,|b|$.*

Proof. Let $m = |a|, n = |b|$. $(ab)^{mn} = (a^m)^n (b^n)^m = e$, and so $|ab| \leqslant mn$.

Conversely, if $|ab| = d$, $e = (ab)^{nd} = a^{nd}(b^n)^d = a^{nd}$ so $m \mid nd$ and by Theorem 2.4.9, $m \mid d$. Similarly, $n \mid d$, and so $mn \mid d$. Hence, $mn \leqslant d$. □

Theorem 3.6.6. *If G is Abelian, and $\{\, g : G \bullet |g| \,\}$ is bounded above, then $\exists\, g : G \bullet \forall\, h : G \bullet |h| \mid |g|$.*

Proof. Let $|g|$ be maximal. Suppose $\exists\, h : G \bullet |h| \nmid |g|$. By Theorem 2.4.9, $|h| = pk$ for some prime $p \nmid |g|$. It follows that $\left|h^k\right| = p$ and so by Lemma 3.6.5, $\left|h^k g\right| = p\,|g| > |g|$, a contradiction. □

3.7 Group Actions

Definition 3.7.1.

1. *For a set X,* $\mathrm{Sym}(X) = X \rightarrowtail\!\!\!\!\twoheadrightarrow X$.
2. *For $n : \mathbb{N}_+$,* $S_n = \mathrm{Sym}(\{1, \ldots n\})$.

[44] ∞ is not really a cardinal, but here $\#\mathbb{Z} = \infty$ is used as a shorthand for "$\mathbb{Z}$ is infinite".

Proposition 3.7.2. *For a set X, $(\mathrm{Sym}(X), \circ)$ is a group.*

Proof.

1. $\forall \sigma, \tau : X \rightarrowtail\!\!\!\!\twoheadrightarrow X \bullet \sigma \circ \tau \in X \rightarrowtail\!\!\!\!\twoheadrightarrow X$.
2. $\circ$ is associative.
3. $\mathrm{id}_X : X \rightarrowtail\!\!\!\!\twoheadrightarrow X$.
4. $\forall \sigma : X \rightarrowtail\!\!\!\!\twoheadrightarrow X \bullet \exists \sigma^{-1} : X \rightarrowtail\!\!\!\!\twoheadrightarrow X \bullet \sigma^{-1} \circ \sigma = \sigma \circ \sigma^{-1} = \mathrm{id}_X$.

□

$\mathrm{Sym}(X)$ is the "permutation group of X", or the "symmetric group on X". S_n is the "symmetric group on n elements".

Definition 3.7.3.

1. *A **group action** on X is a homomorphism $\theta : G \to \mathrm{Sym}(X)$.*
2. *θ is a **faithful** group action if it is injective.*
3. *θ is a **trivial** group action if it is a trivial homomorphism.*

We say "G acts on X", "G acts faithfully on X", or "G acts trivially on X". Where G is presented as a subgroup of $\mathrm{Sym}(X)$, the inclusion map gives the **natural** group action on X, and we say "G acts naturally on X".

Where it is clearer, we will write gx to mean $\theta(g)(x)$.

Proposition 3.7.4. *If G acts on X,*

1. *$\forall g, h : G, x : X \bullet g(hx) = (gh)x$.*
2. *$\forall x : X \bullet ex = x$.*
3. *The action is faithful iff $\forall g : G \bullet (\forall x : X \bullet gx = x) \Rightarrow g = e$.*

Proof.

1. $\theta(g)(\theta(h)(x)) = (\theta(g) \circ \theta(h))(x)$.
2. $\theta(e) = \mathrm{id}_X$.
3. By Proposition 3.3.5, θ is faithful iff $\ker \theta \cong \mathbb{1}$.

□

Proposition 3.7.5. *If G acts on X, and $H \leqslant G$, then H acts on X.*

Proof. If $\theta : G \to \mathrm{Sym}(X)$ is a homomorphism, then by Proposition 3.4.4, $(H \lhd \theta) : H \to \mathrm{Sym}(X)$ is also a homomorphism. □

Definition 3.7.6.

1. *The* ***orbit*** *of x,* $\mathrm{Orb}_G(x) = \{\, g : G \bullet gx \,\}$.
2. *The* ***stabiliser*** *of x,* $\mathrm{Stab}_G(x) = \{\, g : G \mid gx = x \,\}$.

Where it is clearer, we will write Orb to mean Orb_G, and Stab to mean Stab_G.

Proposition 3.7.7. $\{\, x : X \bullet \mathrm{Orb}(x) \,\}$ *is a partition of X.*

Proof. Let $R : X \leftrightarrow X$ be defined as xRy iff $x \in \mathrm{Orb}(y)$. R is an equivalence relation, as for $x, y, z : X$,

1. Reflexivity: $x \in \mathrm{Orb}(x)$ as $x = ex$.
2. Symmetry: $x \in \mathrm{Orb}(y) \Rightarrow (\exists\, g : G \bullet x = gy)$
   $\Rightarrow \left(\exists\, g^{-1} : G \bullet y = g^{-1}x\right) \Rightarrow y \in \mathrm{Orb}(x)$.
3. Transitivity: $(x \in \mathrm{Orb}(y) \land y \in \mathrm{Orb}(z))$
   $\Rightarrow (\exists\, g, h : G \bullet x = gy \land y = hz)$
   $\Rightarrow (\exists\, gh : G \bullet x = (gh)z) \Rightarrow x \in \mathrm{Orb}(z)$.

□

Proposition 3.7.8. $\forall\, x : X \bullet \mathrm{Stab}(x) \leqslant G$.

Proof. $ex = x$, and $\forall\, g, h : \mathrm{Stab}(x)$, $gx = x \Rightarrow x = g^{-1}x$, and $(gh)x = g(hx) = gx = x$. □

Theorem 3.7.9 (Cayley's Theorem)**.** *Every group is isomorphic to a subgroup of a permutation group.*

Proof. Let $\theta(g : G) = \phi_g : \mathrm{Sym}(G)$, where $\phi_g(h : G) = gh$.

1. ϕ_g is injective, as $gh = gh' \Rightarrow g^{-1}gh = g^{-1}gh' \Rightarrow h = h'$.
2. θ is injective, as $\phi_g = \phi_h \Rightarrow g = \phi_g(e) = \phi_h(e) = h$.
3. $\forall\, g, h : G \bullet \phi_g \circ \phi_h = \phi_{gh}$.

Hence, $G \cong \mathrm{ran}\,\theta \leqslant \mathrm{Sym}(G)$. □

I.e. every group acts naturally and faithfully on itself by left-multiplication.[45]

[45] Or by right-multiplication of inverses, with $\phi'_g(h) = hg^{-1}$.

Proposition 3.7.10. *For $H \leqslant G$, $\theta : G \to \mathrm{Sym}({}_G H)$ defined by $\theta(a)(bH) = (ab)H$ is a homomorphism.*

Proof. If $bH = cH$ then $(ab)H = a(bH) = a(cH) = (ac)H$. Therefore, θ is well-defined. Also, $\forall\, g, h : G \bullet g(hH) = (gh)H$. Therefore θ is a homomorphism. □

I.e. every group acts on left-cosets[46] of its subgroups.

3.8 Lagrange's Theorem

Theorem 3.8.1 (Lagrange's Theorem)**.** *If G is a finite[47] group, and $H \leqslant G$,*

1. *$\#G = \#_G H \cdot \#H$. In particular, $\#H \,\big|\, \#G$.*
2. *$\forall\, g : G \bullet |g| \,\big|\, \#G$.*

Proof.

1. By Proposition 3.5.2.3 and Lemma 3.5.3, G has a partition into $\#_G H$ sets of cardinality $\#H$.
2. By Proposition 3.6.3, Proposition 3.4.3, and (1), $|g| = \#\langle g \rangle \,\big|\, \#G$.

□

Corollary 3.8.2. *$C_k \leqslant C_n$ iff $k \,\big|\, n$.*

Proof. Suppose $n = kd$ for some $d : \mathbb{N}_+$. Let $g : C_n$ be a generator, then $(g^d)^k = e$ but for $1 \leqslant k' < k$, $dk' < n$ and so $(g^d)^{k'} \neq e$. Hence $\left|g^d\right| = k$ and $\left\langle g^d \right\rangle \cong C_k$.

The converse follows immediately from Theorem 3.8.1.2. □

Theorem 3.8.3 (Orbit-Stabiliser Theorem)**.** *If G is a finite[47] group acting on a set X, then $\forall\, x : X \bullet \#\,\mathrm{Orb}(x) \cdot \#\,\mathrm{Stab}(x) = \#G$. In particular, $\mathrm{Orb}(x) \,\big|\, \#G$.*

Proof. Let $H = \mathrm{Stab}(x)$. By Proposition 3.7.8 and Lemma 3.5.3, ${}_G H$ is a partition of G. Let $f : \mathrm{Orb}(x) \to {}_G H$ be defined by $f(gx) = gH$.

1. f is well-defined: if $gx = hx$, then $x = g^{-1}hx \Rightarrow g^{-1}h \in H$. By Corollary 3.5.4, $gH = hH$.

[46] Or, similarly, right-cosets.

[47] In fact, the proof does extend to infinite groups.

2. f is injective: by Corollary 3.5.4, $gH = hH \Rightarrow g^{-1}h \in H \Rightarrow g^{-1}hx = x \Rightarrow gx = hx$.

3. f is surjective: given $gH : {}_GH$, $f(gx) = gH$.

Therefore, f is a bijection. The result follows by Theorem 3.8.1.1. □

3.9 The Group $\mathbb{Z}_n^*$

Definition 3.9.1. *Euler's totient function* $\phi(n : \mathbb{N}_+) = \#\mathbb{Z}_n^*$.

$\phi(n)$ counts how many of $1, \ldots n$ are coprime to n.

Proposition 3.9.2. *For p prime,*

1. $\phi(1) = 1$.
2. $\phi(p) = p - 1$.
3. $\forall\, k : \mathbb{N}_+ \bullet \phi(p^k) = p^{k-1}(p-1)$.
4. $\forall\, m, n : \mathbb{N}_+ \mid \mathrm{HCF}(m,n) = 1 \bullet \phi(mn) = \phi(m)\phi(n)$.[48]

Proof.

1. Trivial.

2. Follows immediately from Lemma 2.4.2.

3. Let $1 \leqslant a \leqslant p^k$. By Theorem 2.4.9, every such a which is not coprime to p^k has $a = pd$ for some $1 \leqslant d \leqslant p^{k-1}$. Therefore, $\#\mathbb{Z}_{p^k} - \#\mathbb{Z}_{p^k}^* = p^{k-1}$ and so $\#\mathbb{Z}_{p^k}^* = p^k - p^{k-1} = p^{k-1}(p-1)$.

4. By Lemma 2.5.2, $ax \equiv 1 \pmod m$ and $bx \equiv 1 \pmod n$ have a unique simultaneous solution $x_{(a,b)} : \mathbb{Z}_{mn}^*$ for each $(a,b) : \mathbb{Z}_m^* \times \mathbb{Z}_n^*$.

   Conversely, by Proposition 2.3.8.1 each $x : \mathbb{Z}_{mn}^*$ has a unique $c : \mathbb{Z}_{mn}^*$ with $cx \equiv 1 \pmod{mn}$. Letting $a \equiv c \pmod m, b \equiv c \pmod n$, it follows that $a \in \mathbb{Z}_m^*$ and $b \in \mathbb{Z}_n^*$, and so $x = x_{(a,b)}$. Therefore, $\#\mathbb{Z}_{mn}^* = \#\left(\mathbb{Z}_m^* \times \mathbb{Z}_n^*\right) = \#\mathbb{Z}_m^* \cdot \#\mathbb{Z}_n^*$.

□

[48] By Theorem 2.4.9, it follows that $\phi(n)$ can be computed relatively easily, i.e. we don't actually have to find all of the HCFs.

Proposition 3.9.3. $\left(\mathbb{Z}_n^*, \cdot\right)$ *is a group.*

Proof. Follows immediately from Proposition 2.3.8.1. □

Theorem 3.9.4 (Fermat-Euler Theorem)**.** $\forall\, a : \mathbb{Z}_n^* \bullet a^{\phi(n)} = 1$.

Proof. Follows immediately from Theorem 3.8.1.2. □

Corollary 3.9.5 (Fermat's Little Theorem)**.** *If p is prime, then* $\forall\, a \in \mathbb{Z}_p \bullet a^p \equiv a \pmod{p}$.

Proof. $a = 0$ is trivial. By Corollary 2.4.5, if $a \neq 0$ then $a \in \mathbb{Z}_p^*$, and so by Theorem 3.9.4 and Proposition 3.9.2.2, $a^p \equiv a^{p-1}a \equiv 1 \cdot a \pmod{p}$. □

Theorem 3.9.6. *For p prime, a polynomial of degree $k : \mathbb{N}$ in one variable has at most k roots in $\mathbb{Z}_p$.*

Proof. By induction on k. $k = 0, 1$ are trivial.

Suppose r is a root of $f(X) \equiv \sum_{i=0}^{k+1} a_i X^i \pmod{p}$, with $a_{k+1} \neq 0$.[49]

Let $g(X) \equiv \sum_{i=0}^{k} b_i X^i \pmod{p}$ where $b_k = a_{k+1} \neq 0$, and for $0 < i \leqslant k$, $b_{i-1} \equiv a_i + rb_i \pmod{p}$.

$$\begin{aligned}
(X - r)g(X) &\equiv \sum_{i=0}^{k} b_i \left(X^{i+1} - rX^i\right) \\
&\equiv b_k X^{k+1} + \left[\sum_{i=1}^{k} \left(b_{i-1} - rb_i\right) X^i\right] - rb_0 \\
&\equiv a_{k+1} X^{k+1} + \left[\sum_{i=1}^{k} a_i X^i\right] - rb_0 \\
&\equiv f(X) - a_0 - rb_0 \pmod{p}
\end{aligned}$$

By evaluating at $X = r$, it follows that $a_0 + rb_0 \equiv 0 \pmod{p}$ and $f(X) = (X - r)g(X)$. By Proposition 2.3.8.2 and Corollary 2.4.5, if $f(x) = 0$, either $x = r$ or $g(x) = 0$. By the inductive assumption, $g(X)$ has at most k roots, and so $f(X)$ has at most $k + 1$.[50] □

[49] Since $\deg f \in \mathbb{N}$, f is not the zero polynomial.

[50] The only fact we used about $\mathbb{Z}_p$ was that $ab = 0 \Rightarrow a = 0 \vee b = 0$, so this proof also works for $\mathbb{Z}[X]$, $\mathbb{Q}[X]$, $\mathbb{R}[X]$ and $\mathbb{C}[X]$. See *IB Groups, Rings and Modules.*

Corollary 3.9.7. *For p prime,*

1. *$\forall\, a : \mathbb{Z}_p$, a has at most two square roots.*
2. *$\forall\, a : \mathbb{Z}_p^* \bullet a = a^{-1} \Leftrightarrow a \equiv \pm 1 \pmod{p}$.*

Proof.

1. By Theorem 3.9.6, $X^2 - a \pmod{p}$ has at most two roots.[51]
2. a is a root of $X^2 - 1 \pmod{p}$. By (1), there are no more roots.

□

Theorem 3.9.8. *For p prime, $\mathbb{Z}_p^*$ is cyclic.*

Proof. By Theorem 3.6.6, $\exists\, g : \mathbb{Z}_p^* \bullet \forall\, a : \mathbb{Z}_p^* \bullet |a| \,\big|\, |g|$, and so $\forall\, a : \mathbb{Z}_p^* \bullet a^{|g|} \equiv 1 \pmod{p}$. It follows that $X^{|g|} - 1$ has $p - 1$ roots in $\mathbb{Z}_p$ and so by Theorem 3.9.6, $p-1 \leqslant |g|$. By Theorem 3.8.1.2, $|g| = p-1$ and $\langle g \rangle = \mathbb{Z}_p^*$. □

A generator of $\mathbb{Z}_p^*$ is also called a **primitive root** modulo p.

Corollary 3.9.9 (Wilson's Theorem)**.**

1. *For p prime, $(p-1)! \equiv -1 \pmod{p}$.*
2. *For n composite, $(n-1)! \equiv 0 \pmod{n}$.*

Proof.

1. $p = 2$ is trivial. Suppose $p = 2k + 1$ is prime.[52]

   Let $g : \mathbb{Z}_p^*$ be a generator. Since $(g^k)^2 \equiv 1 \pmod{p}$ but $|g| \neq k$, by Corollary 3.9.7.1 $g^k \equiv -1 \pmod{p}$.

   By Corollary 2.4.5 and Corollary 3.9.5,

   $$(p-1)! \equiv \prod_{a:\mathbb{Z}_p^*} a \equiv \prod_{i=1}^{p-1} g^i \equiv g^{\frac{p(p-1)}{2}} \equiv (g^p)^k \equiv g^k \equiv -1 \pmod{p}$$

2. By Proposition 2.4.6, n has a factorisation $n = ab$ with $1 < a, b < n$, so $ab \equiv 0 \pmod{n}$, and the product $(n-1)!$ includes a, b.

□

[51] For $p > 2$, if $b \neq 0$ is a square root, $-b$ is a distinct square root, and it follows that exactly half of $\mathbb{Z}_p^*$ are squares.

[52] 2 is the only even prime number. It is often a special case because $\mathbb{Z}_2^* \cong \mathbb{1}$.

Corollary 3.9.10. *For p prime, $\mathbb{Z}_p^*$ contains a primitive nth root of 1 iff $p \equiv 1 \pmod{n}$.*

Proof. Follows immediately from Corollary 3.8.2. □

Corollary 3.9.11. *For p prime, -1 is a square modulo p iff $p = 2$ or $p \equiv 1 \pmod{4}$.*

Proof. $p = 2$ is trivial. If $p > 2$, $-1 \not\equiv 1 \pmod{p}$ and so if $a : \mathbb{Z}_p^* \mid a^2 \equiv -1 \pmod{p}$, then $|a| = 4$. The result follows by Corollary 3.9.10. □

3.10 Conjugation

Definition 3.10.1.

1. *For $a, g : G$, $a^g = g^{-1}ag$.*
2. *For $A : \mathbb{P}\, G$, $g : G$, $A^g = g^{-1}Ag$.*
3. *For $a, b : G$, $a \sim b$ if $\exists\, g : G \bullet a = b^g$.*
4. *For $A, B : \mathbb{P}\, G$, $A \sim B$ if $\exists\, g : G \bullet A = B^g$.*

We say a^g is the "**conjugation** of a by g", and "a,b are **conjugate**".

Definition 3.10.2. *For $g : G$, $\mathrm{ccl}_G(g) = \{\, h : G \mid h \sim g \,\}$ is the **conjugacy class** of g.*

Where it is clearer, we will write ccl to mean ccl_G.

Proposition 3.10.3. *For $a, b, g, h : G$, and $A, B : \mathbb{P}\, G$,*

1. *$a^e = a$, and $A^e = A$.*
2. *$a = a^g$ iff a, g commute.*
3. *$(a^{-1})^g = (a^g)^{-1}$, and $(A^{-1})^g = (A^g)^{-1}$.*
4. *$(a^g)^h = a^{gh}$, and $(A^g)^h = A^{gh}$.*
5. *$(ab)^g = a^g b^g$.*
6. *If a, b commute, then a^g, b^g commute.*

Proof.

1. $e^{-1}ae = a$.

2. $ag = ga \Leftrightarrow g^{-1}ag = g^{-1}ga = a$.

3. $g^{-1}a^{-1}g = (g^{-1}ag)^{-1}$.

4. $h^{-1}(g^{-1}ag)h = (gh)^{-1}a(gh)$.

5. $g^{-1}(ab)g = (g^{-1}ag)(g^{-1}bg)$.

6. $a^g b^g = (ab)^g = (ba)^g = b^g a^g$.

Similarly for $A, B : \mathbb{P}\, G$. □

Proposition 3.10.4. $\sim$ *is an equivalence relation.*

Proof.

1. Reflexivity: $a = a^e$.

2. Symmetry: $a = b^g \Rightarrow b = a^{g^{-1}}$.

3. Transitivity: $(a = b^g \wedge b = c^h) \Rightarrow a = (c^h)^g = c^{hg}$.

Similarly for $A, B : \mathbb{P}\, G$. □

It follows that $\{\, g : G \bullet \mathrm{ccl}(g) \,\}$ is a partition of G.

Theorem 3.10.5. *For $g : G$,*

1. *$\phi_g(a : G) = a^g$ is an isomorphism.*

2. *$\psi_g(A : \mathbb{P}\, G) = A^g$ is a bijection.*

3. *$(G_\leqslant \lhd \psi_g) \in \mathrm{Sym}(G_\leqslant)$, i.e. if $H \leqslant G$, then $H^g \leqslant G$.*

4. *$\theta : G \to \mathrm{Sym}(G)$ given by $\theta(g) = \phi_g$ is a homomorphism.*

5. *$\Theta : G \to \mathrm{Sym}(\mathbb{P}\, G)$ given by $\Theta(g) = \psi_g$ is a homomorphism.*

6. *$\Theta' : G \to \mathrm{Sym}(G_\leqslant)$ given by $\Theta(g) = (G_\leqslant \lhd \psi_g)$ is a homomorphism.*

Proof.

1. ϕ_g is a homomorphism by Proposition 3.10.3.5.
   ϕ_g is injective: $a^g = b^g \Rightarrow (a^g)^{g^{-1}} = (b^g)^{g^{-1}} \Rightarrow a = b$.
   ϕ_g is surjective: given $a : G$, $\phi_g(a^{g^{-1}}) = (a^{g^{-1}})^g = a$.

2. Similarly, $\psi_g \in \mathrm{Sym}(\mathbb{P}\, G)$ is injective and surjective.

3. If $H \leqslant G$, $e = e^g \in H^g$, $a^g \in H^g \Rightarrow (a^g)^{-1} = (a^{-1})^g \in H^g$, and $a^g, b^g \in H^g \Rightarrow a^g b^g = (ab)^g \in H$. Therefore, $\psi_g(H) \leqslant G$.

4. By Proposition 3.10.3.4, $\phi_g \circ \phi_h = \phi_{gh}$.

5. Similarly, Θ is a homomorphism.

6. Similarly, Θ' is a homomorphism.

□

I.e. G acts on G, $\mathbb{P}\, G$ and $G_{\leqslant}$ by conjugation.[53]

Corollary 3.10.6.

1. $\forall\, a : G \bullet \mathrm{C}(a) \leqslant G$.

2. $\forall\, A : \mathbb{P}\, G$, $\mathrm{C}(A) \leqslant G$.

Proof.

1. G acts on itself by conjugation. By Proposition 3.10.3.2, $\mathrm{Stab}(a) = \mathrm{C}(a)$. The result follows by Proposition 3.7.8.

2. Similarly, G acts on $\mathbb{P}\, G$ by conjugation, and $\mathrm{Stab}(A) = \mathrm{C}(A)$.

□

Corollary 3.10.7. $\forall\, g : G \bullet \#\,\mathrm{ccl}(g) \cdot \#\,\mathrm{C}(g) = \#G$. *In particular,* $\#\,\mathrm{ccl}(g) \,|\, \#G$.

Proof. When G acts on itself by conjugation, $\mathrm{Orb}(g) = \mathrm{ccl}(g)$. The result follows by Theorem 3.8.3. □

3.11 Normal Subgroups

Definition 3.11.1. $H \trianglelefteq G$ *if* $H \leqslant G$ *and* $\forall\, g : G \bullet H^g = H$.

We say "H is a **normal subgroup** of G" or "H is normal in G". If $H < G$ is normal, we write $H \triangleleft G$.

[53] Also, if $H \leqslant G$, then H also acts on G, $\mathbb{P}\, G$ and $G_{\leqslant}$ by Proposition 3.7.5.

Theorem 3.11.2. *For $H \leqslant G$, the following are equivalent:*

1. $\forall\, g : G \bullet H^g = H$ *(i.e. $H \trianglelefteq G$).*
2. $\forall\, g : G \bullet H^g \subseteq H$.
3. $\forall\, g : G \bullet gH = Hg$.
4. *If $K \leqslant G$, then $K \sim H \Rightarrow K = H$.*
5. *If $K \leqslant G$, then $K \sim H \Rightarrow KH = H$*
6. $\forall\, a, b, g : G \mid aH = bH \bullet agH = bgH$.
7. $\forall\, a, b : G \bullet aHbH = abH$.

Proof.

- (1) $\Rightarrow$ (2): Trivial.
- (1) $\Leftrightarrow$ (3): $g^{-1}Hg = H \Leftrightarrow Hg = gH$.
- (1) $\Rightarrow$ (4): $K \sim H \Rightarrow K = H^g \Rightarrow K = H$.
- (2) $\Rightarrow$ (1): $H^{g^{-1}} \subseteq H \Rightarrow H \subseteq H^g$. Also, $H^g \subseteq H$, so $H^g = H$.
- (3) $\Rightarrow$ (6): $aH = bH \Rightarrow aHg = bHg \Rightarrow agH = bgH$.
- (3) $\Rightarrow$ (7): $Hb = bH \Rightarrow aHbH = abHH = abH$.
- (4) $\Rightarrow$ (1): $H^g \sim H \Rightarrow H^g = H$.
- (4) $\Rightarrow$ (5): $K \sim H \Rightarrow K = H \Rightarrow KH = HH = H$.
- (5) $\Rightarrow$ (2): $H^g \sim H \Rightarrow H^g H = H$. By Proposition 3.5.5, $H^g \subseteq H$.
- (6) $\Rightarrow$ (2): $\forall\, h : H \bullet g^{-1}hH = g^{-1}H \Rightarrow g^{-1}hgH = g^{-1}gH = H$. By Proposition 3.5.5, $h^g \in H$, and so $H^g \subseteq H$.
- (7) $\Rightarrow$ (5): Let $K = H^g$, then $KH = g^{-1}HgH = gg^{-1}HH = H$.

□

Definition 3.11.3.

1. *For $a : G$, $\mathrm{N}_G(a) = \{\, g : G \mid a^g = a \,\}$ is the **normalizer** of a.*
2. *For $A : \mathbb{P}\, G$, $\mathrm{N}_G(A) = \{\, g : G \mid A^g = A \,\}$.*

Where it is clearer, we will write N to mean N_G. Note that although by Proposition 3.10.3.2, $\forall\, a : G \bullet \mathrm{N}(a) = \mathrm{C}(a)$, this is not true for $A : \mathbb{P}\, G$.

3.12 Quotient Groups

Definition 3.12.1. *For $H \trianglelefteq G$, $G/H = ({}_G H, \cdot)$, with $aH \cdot bH = aHbH$.*

G/H is "the **quotient** of G over H".

Proposition 3.12.2. *G/H is a group.*

Proof.

1. $\cdot$ is well-defined: by Theorem 3.11.2.7, $aHbH = abH \in {}_G H$.
2. Associativity: follows immediately from associativity in G.
3. Identity: $e_{G/H} = eH = H$. $\forall\, gH : {}_G H \bullet H \cdot gH = gH \cdot H = gH$.
4. Inverses: $(gH)^{-1} = g^{-1}H$. $\forall\, gH : {}_G H \bullet gH \cdot g^{-1}H = gg^{-1}H = H$.

□

Since Theorem 3.11.2.7 is *equivalent* to Theorem 3.11.2.1, $H \trianglelefteq G$ is precisely the condition on which $\cdot$ is well-defined.

Theorem 3.12.3 (The Isomorphism Theorem)**.**

1. *If $\theta : G \to H$ is a homomorphism, then $\ker\theta \trianglelefteq G$.*
2. *If $\theta : G \to H$ is a homomorphism, then $G/\ker\theta \cong \operatorname{ran}\theta$.*
3. *If $H \trianglelefteq G$, then $\pi : G \to G/H$ given by $\pi(g) = gH$ is a homomorphism, and $\ker\pi = H$.*

Proof. Let $K = \ker\theta$.

1. $K \leqslant G$ by Proposition 3.4.5.1. Given $g : G, a : K$, $\theta(a^g) = \theta(a)^{\theta(g)} = e_H$. Hence, $\forall\, a : K \bullet a^g \in K$ and so $K^g = K$.
2. Define $\phi : G/K \to \operatorname{ran}\theta$ by $\phi(aK) = \theta(a)$. $aK = bK \Leftrightarrow a^{-1}b \in K$, so $\theta(a) = \theta(a)\theta(a^{-1}b) = \theta(b)$ and hence ϕ is well-defined.

   $\phi(aK \cdot bK) = \phi(abK) = \theta(ab) = \theta(a)\theta(b) = \phi(aK)\phi(bK)$, and so ϕ is a homomorphism.

   $\phi(aK) = \phi(bK) \Rightarrow \theta(a) = \theta(b) \Rightarrow \theta(a^{-1}b) = e_H \Rightarrow a^{-1}b \in K \Rightarrow aK = bK$, and so ϕ is injective.

   Given $h = \theta(a) : \operatorname{ran}\theta$, $\phi(aK) = h$, and so ϕ is surjective.
3. By Theorem 3.11.2.7, $\pi(ab) = abH = aHbH = \pi(a)\pi(b)$, and so π is a homomorphism.

   $\pi(a) = e_{G/H} = H \Leftrightarrow aH = H \Leftrightarrow a \in H$, and so $\ker\pi = H$.

□

3.13 The Group S_n

Definition 3.13.1.

1. $\sigma : S_n$ *is a* ***cycle*** *of length* $k : \mathbb{N}_+$ *if* $\exists\, a_1, \ldots a_k : \{1, \ldots n\} \bullet \sigma(a_j) = a_{j+1}$ *for* $1 \leqslant j < k$, $\sigma(a_k) = a_1$, *and for* $x \notin \{a_1, \ldots a_k\}$, $\sigma(x) = x$.

2. *If* σ, τ *are cycles, and* $\forall\, x : \{1, \ldots n\} \bullet$ *either* $\sigma(x) = x$ *or* $\tau(x) = x$, *then* σ, τ *are* ***disjoint****.*

3. *A* ***transposition*** *is a cycle of length* 2.

We will write $\sigma = (a_1\, a_2 \cdots a_k)$.

Proposition 3.13.2.

1. *For* $a_1, \ldots a_k : \{1, \ldots n\}$, $(a_1\, a_2 \cdots a_k) = (a_2\, a_3 \cdots a_k\, a_1)$.

2. *If* $\sigma, \tau : S_n$ *are disjoint cycles, then* σ, τ *commute.*

3. $\forall\, a : \{1, \ldots n\} \bullet (a) = \iota$ *is the identity of* S_n.

Proof.

1. $\sigma(a_i) = a_{i+1}$ for $2 \leqslant i < k$, $\sigma(a_k) = a_1$, and $\sigma(a_1) = a_2$.

2. $\forall\, x : \{1, \ldots n\} \bullet$ wlog $\tau(x) = x$. If $\sigma(x) \neq x$, then $\sigma^2(x) \neq \sigma(x)$, so $\tau(\sigma(x)) = \sigma(x) = \sigma(\tau(x))$. As S_n acts faithfully on $\{1, \ldots n\}$, $\sigma\tau = \tau\sigma$.

3. $(a)a = a$, and for $x \neq a$, $(a)x = x$.

□

Theorem 3.13.3. $\forall\, \sigma : S_n \bullet \sigma$ *is a product of disjoint cycles.*

Proof. Define $m(\sigma) = \#\{\, x : \{1, \ldots n\} \bullet \sigma(x) \neq x \,\}$. We proceed by strong induction on $m(\sigma)$. $m(\sigma) = 0$ is trivial.

Given $x : \{1, \ldots n\} \mid \sigma(x) \neq x$, let $k = \min\{\, i : \mathbb{N}_+ \bullet \sigma^i(x) = x \,\}$.[54] For $1 \leqslant i, j \leqslant k$, if $\sigma^i(x) = \sigma^j(x)$ then $\sigma^{|j-i|}(x) = x$ so $i = j$. Hence the $\sigma^i(x)$ are distinct, $\sigma(\sigma^i(x)) = \sigma^{i+1}(x)$, and $\sigma(\sigma^{k-1}(x)) = x$.

Therefore, $\gamma = (x\, \sigma(x)\, \sigma^2(x) \cdots \sigma^{k-1}(x))$ is a cycle of length $k > 1$, and $m(\sigma\gamma^{-1}) = m(\sigma) - k < m(\sigma)$, so $\sigma\gamma^{-1}$ is a product of disjoint cycles which are disjoint to γ, hence $\sigma = (\sigma\gamma^{-1})\gamma$ is a product of disjoint cycles. □

[54] The set is non-empty as $\sigma^{\#S_n} = \iota$.

Corollary 3.13.4. *$\forall \sigma : S_n \bullet \sigma$ is a product of transpositions.*

Proof. By Theorem 3.13.3, it is sufficient to show that every cycle is a product of transpositions. By induction on the length of the cycle k, $k = 1, 2$ are trivial, and $(a_1\, a_2 \cdots a_{k+1}) = (a_1\, a_{k+1})(a_1\, a_2 \cdots a_k)$. □

Lemma 3.13.5. *For $\sigma : S_n$,*

1. *For $\alpha = (a_1\, a_2 \cdots a_k)$, $\alpha^\sigma = (\sigma^{-1}(a_1)\, \sigma^{-1}(a_2) \cdots \sigma^{-1}(a_k))$.*
2. *For disjoint cycles $\alpha_1, \ldots \alpha_m : S_n$, $\alpha_1^\sigma, \ldots \alpha_m^\sigma$ are disjoint cycles, and*
$$\left(\prod_{i=1}^{m} \alpha_i\right)^\sigma = \prod_{i=1}^{m} \alpha_i^\sigma$$
3. *$\tau : S_n$ is conjugate to σ iff σ, τ are each products of the same number of disjoint cycles of the same lengths.*[55]

Proof.

1. For $1 \leqslant i < k$, $\alpha^\sigma(\sigma^{-1}(a_i)) = \sigma^{-1}(a_{i+1})$, $\alpha^\sigma(\sigma^{-1}(a_k)) = \sigma^{-1}(a_1)$, and for $x \notin \{\sigma^{-1}(a_1), \ldots \sigma^{-1}(a_k)\}$, $\sigma(x) \notin \{a_1, \ldots a_k\}$, so $\alpha(\sigma(x)) = \sigma(x)$, so $\alpha^\sigma(x) = x$.
2. By (1), Proposition 3.13.2.2, and Proposition 3.10.3.6.
3. By Theorem 3.13.3, (1), and (2).

□

Theorem 3.13.6. *For $n \geqslant 2$,*

1. *There is a homomorphism $\zeta : S_n \to C_2 \cong (\{1, -1\}, \cdot)$ which, for any transposition $\alpha : S_n$, $\zeta(\alpha) = -1$.*
2. *If $\theta : S_n \to C_2$ is a non-trivial homomorphism, then $\theta = \zeta$.*

[55] Not counting trivial cycles (a).

Proof.

1. Define $\zeta : S_n \to \mathbb{Q}$ by $\zeta(\sigma) = \prod_{i=1}^{n-1} \prod_{j=i+1}^{n} \frac{\sigma(j) - \sigma(i)}{j - i}$.

   $\forall\, \sigma : S_n \bullet \sigma$ is a bijection, so $|\zeta(\sigma)| = 1$, hence $\operatorname{ran} \zeta = \{1, -1\}$.

   Also, $\forall\, \sigma, \tau : S_n \bullet$

   $$\begin{aligned}
   \zeta(\sigma\tau) &= \prod_{i=1}^{n-1} \prod_{j=i+1}^{n} \frac{\sigma\tau(j) - \sigma\tau(i)}{j - i} \\
   &= \left[\prod_{i=1}^{n-1} \prod_{j=i+1}^{n} \frac{\sigma\tau(j) - \sigma\tau(i)}{\tau(j) - \tau(i)}\right] \cdot \left[\prod_{i=1}^{n-1} \prod_{j=i+1}^{n} \frac{\tau(j) - \tau(i)}{j - i}\right] \\
   &= \left[\prod_{i=1}^{n-1} \prod_{j=i+1}^{n} \frac{\sigma(j) - \sigma(i)}{j - i}\right] \cdot \left[\prod_{i=1}^{n-1} \prod_{j=i+1}^{n} \frac{\tau(j) - \tau(i)}{j - i}\right] = \zeta(\sigma) \cdot \zeta(\tau)
   \end{aligned}$$

   as τ is a bijection, so the product is over the same terms.[56] Hence, ζ is a homomorphism.

   For transpositions $\alpha_1, \alpha_2 : S_n$, by Lemma 3.13.5.3 $\exists\, \sigma : S_n \bullet \alpha_2 = \alpha_1^\sigma$. C_2 is Abelian, so $\zeta(\alpha_2) = \zeta(\alpha_1)^{\zeta(\sigma)} = \zeta(\alpha_1)$. It is easy to check that $\zeta(1\,2) = -1$, and the result follows.

2. As before, for transpositions $\alpha_1, \alpha_2 : S_n$, $\theta(\alpha_1) = \theta(\alpha_2)$.

   By Corollary 3.13.4, $\forall\, \sigma : S_n \bullet \sigma$ is a product of transpositions $\alpha_1, \ldots \alpha_m$, so $\theta(\sigma) = \theta(\alpha_1)^m$. Therefore, if $\theta(\alpha_1) = 1$ then θ is trivial, otherwise $\theta(\alpha_1) = -1$ and $\theta = \zeta$.

□

Definition 3.13.7. *For $\sigma : S_n$, $\zeta(\sigma)$ is the **signature** of σ.*

Corollary 3.13.8. *A product of an even number of transpositions cannot be written as a product of an odd number of transpositions, and vice versa.*

Proof. If $\sigma : S_n$ is a product of m transpositions, then $\zeta(\sigma) = (-1)^m$. □

Definition 3.13.9. *For $n \geqslant 2$, $A_n = \ker \zeta$ is the **alternating group** on n elements.*

By Theorem 3.12.3, $A_n \lhd S_n$, and $S_n / A_n \cong C_2$.

[56] Where $i < j$ but $\tau(i) > \tau(j)$, $\frac{\sigma\tau(j) - \sigma\tau(i)}{\tau(j) - \tau(i)} = \frac{\sigma\tau(i) - \sigma\tau(j)}{\tau(i) - \tau(j)}$.

A Appendix

A.1 The Natural Numbers

Definition A.1.1. *The set of* ***natural numbers*** $\mathbb{N}$ *is defined as follows:*

1. $\emptyset \in \mathbb{N}$.
2. $\forall\, n : \mathbb{N} \bullet (n \cup \{n\}) \in \mathbb{N}$.
3. $\forall\, S : \mathbb{P}\,\mathbb{N} \bullet \big(\emptyset \in S \land \forall\, n : S \bullet (n \cup \{n\}) \in S\big) \Rightarrow S = \mathbb{N}$.

Note that by this definition, $0 = \emptyset$, $\#n = n$, and "$n + 1$" $= n \cup \{n\}$.

Definition A.1.2.

1. $\mathbb{N}_+ = \mathbb{N} \setminus \{0\}$.
2. $\_ + \_ : \mathbb{N}^2 \to \mathbb{N}$ *is defined as* $\forall\, m, n : \mathbb{N},\ n + 0 = n,\ n + 1 = (n \cup \{n\})$, *and* $n + (m + 1) = (n + m) + 1$.
3. $\_ \cdot \_ : \mathbb{N}^2 \to \mathbb{N}$ *is defined as* $\forall\, m, n : \mathbb{N},\ n \cdot 0 = 0$, *and* $(n + 1) \cdot m = (n \cdot m) + m$.
4. $\_ < \_ : \mathbb{N} \leftrightarrow \mathbb{N}$ *is defined as* $m < n$ *iff* $m \in n$.

By strong induction on n, $+$ and $\cdot$ are defined for all natural numbers.

Note that $\forall\, n : \mathbb{N},\ n = \{\, k : \mathbb{N} \mid k < n \,\}$ and $n + 1 = \{\, k : \mathbb{N} \mid k \leqslant n \,\}$. Also, $m < n$ iff $m \subset n$.

We will write m^n to mean a product of n copies of m.

Definition A.1.3. *For* $S : \mathbb{P}\,\mathbb{N} \mid S \neq \emptyset$,

1. *If* $\exists\, m : \mathbb{N} \bullet \forall\, n : S \bullet n < m$,[57] *then* $\max S = \bigcup_{n:S} n$.
2. $\min S = \bigcap_{n:S} n$.

Where $\max S$ or $\min S$ are defined, they are natural numbers. In particular, every non-empty set $S \subseteq \mathbb{N}$ has a least element $\min S$.[58]

[57] I.e. S is non-empty and bounded-above.

[58] This is the *well-ordering principle*.

A.2 The Integers

Definition A.2.1. *Let* $R : \mathbb{N}^2 \leftrightarrow \mathbb{N}^2$ *be the equivalence relation generated by* $\forall\, a, b, k : \mathbb{N} \bullet (a, b)R(a + k, b + k)$.[59]

1. $\mathbb{Z} = \mathbb{N}^2/R$ *is the set of* ***integers****.*
2. $\mathbb{Z}^\times = \mathbb{Z} \setminus \{[(0, 0)]\}$.
3. $-_- : \mathbb{Z} \to \mathbb{Z}$ *is defined as* $-[(a, b)] = [(b, a)]$.[60]
4. $\_ + \_ : \mathbb{Z}^2 \to \mathbb{Z}$ *is defined as* $[(a, b)] + [(c, d)] = [(a + b, c + d)]$.[61]
5. $\_ \cdot \_ : \mathbb{Z}^2 \to \mathbb{Z}$ *is defined as* $[(a, b)] \cdot [(c, d)] = [(ac + bd, ad + bc)]$.[62]
6. $\_ < \_ : \mathbb{Z} \leftrightarrow \mathbb{Z}$ *is defined as* $[(a, b)] < [(c, d)]$ *iff* $a + d < b + c$.[63]

We will identify $\mathbb{N} \subset \mathbb{Z}$ by the inclusion map $\iota(n : \mathbb{N}) = [(n, 0)]$; i.e. we will write n to mean $\iota(n)$. Note that ι commutes with $+$, $\cdot$, and $<$,[64] and $[(a, b)] = \iota(a) + (-\iota(b))$. We will write $a - b$ to mean $a + (-b)$.

A.3 The Rational Numbers

Definition A.3.1. *Let* $R : (\mathbb{Z} \times \mathbb{Z}^\times) \leftrightarrow (\mathbb{Z} \times \mathbb{Z}^\times)$ *be the equivalence relation generated by* $\forall\, a : \mathbb{Z}, b, k : \mathbb{Z}^\times \bullet (a, b)R(ak, bk)$.[65]

1. $\mathbb{Q} = (\mathbb{Z} \times \mathbb{Z}^\times)/R$ *is the set of* ***rational numbers****.*
2. $\mathbb{Q}^* = \mathbb{Q} \setminus \{[(0, 1)]\}$*, and* $\mathbb{Q}_+ = \{\, [(a, b)] : \mathbb{Q} \bullet ab > 0 \,\}$.
3. $-_- : \mathbb{Q} \to \mathbb{Q}$ *is defined as* $-[(a, b)] = [(-a, b)]$.[66]
4. $\_ + \_ : \mathbb{Q}^2 \to \mathbb{Q}$ *is defined as* $[(a, b)] + [(c, d)] = [(ad + bc, bd)]$.[67]

[59] With equivalence classes $[(a, 0)] = \{\, k : \mathbb{N} \bullet (a + k, k) \,\}$ and $[(0, b)] = \{\, k : \mathbb{N} \bullet (k, b + k) \,\}$.

[60] This is well-defined, as $[(b + k, a + k)] = [(b, a)]$.

[61] This is well-defined, as $[(a + k, b + k)] + [(c + k', d + k')] = [(a + c + (k + k'), b + d + (k + k'))] = [(a + c, b + d)]$.

[62] Convince yourself that this is well-defined.

[63] This is well-defined, as $[(a+k, b+k)] < [(c+k', d+k')]$ iff $a+d+(k+k') < b+c+(k+k')$ iff $a + d < b + c$.

[64] I.e. $\iota(m + n) = \iota(m) + \iota(n)$, $\iota(m \cdot n) = \iota(m) \cdot \iota(n)$, and $\iota(m) < \iota(n)$ iff $m < n$.

[65] With equivalence classes $[(0, 1)] = \{\, k : \mathbb{Z}^\times \bullet (0, k) \,\}$ and $[(a, b)] = \{\, k : \mathbb{Z}^\times \bullet (ak, bk) \,\}$ for a, b coprime.

[66] This is well-defined, as $[(-ak, bk)] = [(-a, b)]$.

[67] Convince yourself that this is well-defined.

5. $\_ \cdot \_ : \mathbb{Q}^2 \to \mathbb{Q}$ *is defined as* $[(a,b)] \cdot [(c,d)] = [(ac, bd)]$.[68]

6. $\_^{-1} : \mathbb{Q}^* \to \mathbb{Q}^*$ *is defined as* $[(a,b)]^{-1} = [(b,a)]$.[69]

7. $\_ < \_ : \mathbb{Q} \leftrightarrow \mathbb{Q}$ *is defined as* $[(a,b)] < [(c,d)]$ *iff* $abd^2 < b^2cd$.[70]

We will identify $\mathbb{Z} \subset \mathbb{Q}$ by the inclusion map $\iota(a : \mathbb{Z}) = [(a,1)]$. Note that ι commutes with $+$, $\cdot$, and $<$, and $[(a,b)] = \iota(a) \cdot \iota(b)^{-1}$. We will write $\frac{a}{b}$ to mean $a \cdot b^{-1}$, and a^{-n} to mean $(a^{-1})^n$.

A.4 The Real Numbers

Definition A.4.1. *Let* $P(s : \mathbb{P}\,\mathbb{Q}, m : \mathbb{Q})$ *be the predicate* $\forall\, x : s \bullet x \leqslant m$,[71]

$$B = \{\, s : \mathbb{P}\,\mathbb{Q} \mid s \neq \emptyset \wedge (\exists\, m : \mathbb{Q} \bullet P(s,m)) \,\}$$

and $R : B \leftrightarrow B$ *be the equivalence relation defined by*

$$\forall\, s, t : B \mid (\forall\, m : \mathbb{Q} \bullet B(s,m) \Leftrightarrow B(t,m)) \bullet sRt$$

1. $\mathbb{R} = B/R$ *is the set of* ***real numbers***.

2. $\mathbb{R}^* = \mathbb{R} \setminus \{[\{0\}]\}$, *and* $\mathbb{R}_+ = \{\, [s] : \mathbb{R} \mid \neg P(s,0) \,\}$.

3. $-\_ : \mathbb{R} \to \mathbb{R}$ *is defined as* $-[s] = [\{\, m : \mathbb{Q} \mid P(s,m) \bullet -m \,\}]$.[72]

4. $\_ + \_ : \mathbb{R}^2 \to \mathbb{R}$ *is defined as* $[s] + [t] = [\{\, x : s, y : t \bullet x + y \,\}]$.

5. $\_ - \_ : \mathbb{R}^2 \to \mathbb{R}$ *is defined as* $[s] - [t] = [s] + (-[t])$.

6. $\_ \cdot \_ : \mathbb{R}^2 \to \mathbb{R}$ *is defined for* $[s], [t] : \mathbb{R}_+$ *as*
   $[s] \cdot [t] = [\{\, x : s, y : t \mid x, y > 0 \bullet xy \,\}]$,
   $\pm[s] \cdot \pm[t] = \pm([s] \cdot [t])$,[73] *and* $[\{0\}] \cdot [s] = [s] \cdot [\{0\}] = [\{0\}]$.

7. $\_^{-1} : \mathbb{R}^* \to \mathbb{R}^*$ *is defined for* $[s] : \mathbb{R}_+$ *as*
   $[s]^{-1} = [\{\, m : \mathbb{Q} \mid P(s,m) \bullet m^{-1} \,\}]$, *and* $(-[s])^{-1} = -([s]^{-1})$.

8. $\_ < \_ : \mathbb{R} \leftrightarrow \mathbb{R}$ *is defined as* $[s] < [t]$ *iff* $[s] \neq [t]$ *and*
   $\forall\, m : \mathbb{Q} \bullet P(t,m) \Rightarrow P(s,m)$.

We will identify $\mathbb{Q} \subset \mathbb{R}$ by the inclusion map $\iota(a : \mathbb{Q}) = [\{a\}]$. Note that ι commutes with $+$, $\cdot$, $^{-1}$ and $<$.

[68] This is well-defined, as $[(ak, bk)] \cdot [(ck', dk')] = [(ac(kk'), bd(kk'))] = [(ac, bd)]$.

[69] This is well-defined, as $[(bk, ak)] = [(b, a)]$.

[70] This is well-defined, as $[(ak, bk)] < [(ck', dk')]$ iff $abd^2(kk')^2 < b^2c(kk')^2$ iff $abd^2 < b^2cd$.

[71] I.e. s is "bounded above" by m.

[72] These are all well-defined, as $[s] = [s'] \Rightarrow (P(s,m) \Leftrightarrow P(s',m))$.

[73] I.e. $[s] \cdot -[t] = -[s] \cdot [t] = -([s] \cdot [t])$, and $-[s] \cdot -[t] = [s] \cdot [t]$.

Definition A.4.2. *If* $S : \mathbb{P}\,\mathbb{R} \mid S \neq \emptyset$,

1. *If* $\exists\, m : \mathbb{R} \bullet P(S, m)$,[74] $\sup S = \left[\bigcup_{[s]:S} s\right]$ *is the* ***supremum*** *of* S.
2. *If* $\exists\, m : \mathbb{R} \bullet P(\{\, x : S \bullet -x \,\}, m)$, $\inf S = -\sup\{\, x : S \bullet -x \,\}$ *is the* ***infimum*** *of* S.

In particular, every non-empty bounded-above subset S of $\mathbb{R}$ has a least upper bound $\sup S$.[75]

A.5 The Complex Numbers

Definition A.5.1.

1. $\mathbb{C} = \mathbb{R}^2$ *is the set of* ***complex numbers***.
2. $\mathbb{C}^* = \mathbb{C} \setminus \{(0,0)\}$.
3. $\mathrm{Re}, \mathrm{Im} : \mathbb{C} \to \mathbb{R}$ *are defined as* $\mathrm{Re}(a,b) = a$, *and* $\mathrm{Im}(a,b) = b$.
4. $\_^* : \mathbb{C} \to \mathbb{C}$ *is defined as* $(a,b)^* = (a,-b)$.
5. $|\cdot| : \mathbb{C} \to \mathbb{R}$ *is defined as* $|(a,b)| = \sqrt{a^2+b^2}$.[76]
6. $-\_ : \mathbb{C} \to \mathbb{C}$ *is defined as* $-(a,b) = (-a,-b)$.
7. $\_ + \_ : \mathbb{C}^2 \to \mathbb{C}$ *is defined as* $(a,b)+(c,d) = (a+c, b+d)$.
8. $\_ - \_ : \mathbb{C}^2 \to \mathbb{C}$ *is defined as* $(a,b)-(c,d) = (a,b)+(-(c,d))$.
9. $\_ \cdot \_ : \mathbb{C}^2 \to \mathbb{C}$ *is defined as* $(a,b)\cdot(c,d) = (ac-bd, ad+bc)$.
10. $\_^{-1} : \mathbb{C}^* \to \mathbb{C}^*$ *is defined as* $(a,b)^{-1} = \left(\dfrac{a}{a^2+b^2}, \dfrac{-b}{a^2+b^2}\right)$.

$<$ is not defined.

We will identify $\mathbb{R} \subset \mathbb{C}$ by the inclusion map $\iota(a : \mathbb{R}) = (a, 0)$. Note that ι commutes with $+$, $\cdot$, and $^{-1}$. We define $\mathrm{i} \in \mathbb{C}$ as $\mathrm{i} = (0,1)$.

[74] Extend P to $(S : \mathbb{P}\,\mathbb{R}, m : \mathbb{R})$. I.e. S is a non-empty, bounded-above set of real numbers.

[75] Note that $\forall [s], [t] : \mathbb{R} \bullet (\sup s = \sup t) \Leftrightarrow ([s] = [t])$, and so $\mathbb{R} = \{\, s : B \bullet \sup s \,\}$.

[76] For $x : \mathbb{R} \mid x \geqslant 0$, we can define $\sqrt{x}$ e.g. as $\sup\{\, y : \mathbb{R} \mid y^2 \leqslant x \,\}$.

A.6 Arithmetic

Proposition A.6.1. *Over $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$, where they are defined,*

1. *$a + 0 = a$, and $1 \cdot a = a$.*
2. *$-a = (-1) \cdot a$, $-(-a) = a$, $a + (-a) = 0$, $(a^{-1})^{-1} = a$, and $a \cdot a^{-1} = 1$.*
3. *$(a \cdot b)^{-1} = a^{-1} \cdot b^{-1}$.*
4. *$+, \cdot$ are associative[77] and commutative,[78] and $\cdot$ distributes over $+$.[79]*
5. *$|\_|$ obeys the triangle inequality, i.e. $|a + b| \leqslant |a| + |b|$.*
6. *$a > b$ iff $b < a$, $a \leqslant b$ iff $(a < b) \vee (a = b)$, and $a \geqslant b$ iff $b \leqslant a$.*
7. *$<$ is transitive and antisymmetric,[80] and $<, =, >$ are a trichotomy.[81]*
8. *If $a < b$ then $-b < -a$, $a + c < b + c$, for $d > 0$, $ad < bd$, and if $a > 0$ then $b^{-1} < a^{-1}$. Also, $a \leqslant b$ iff $\exists\, c \geqslant 0 \bullet a + c = b$.*

Proof. Omitted. □

Definition A.6.2. *For a non-empty finite set or sequence $S = (x_1, \ldots x_n)$ of numbers (e.g. natural numbers, integers...),*

1. *$\sum S$ is the **sum** of the elements of S, i.e. $\sum S = x_1 + \cdots x_n$.*
2. *$\prod S$ is the **product** of the elements of S, i.e. $\prod S = x_1 \cdots x_n$.*
3. *$\sum \emptyset = 0$, and $\prod \emptyset = 1$.*[82]

These are all defined, by induction on n, and associativity and commutativity[83] of $+$ and $\cdot$.

We will write $\sum_{variables}$ *expression* to mean $\sum($ *variables* $\bullet$ *expression* $)$.[84] In particular, $\sum_{k=1}^{n}$ *expression* means $\sum_{k:\{1,\ldots n\}}$ *expression*.

(Similarly for $\prod$).

[77] I.e. $(a + b) + c = a + (b + c)$ and $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
[78] I.e. $m + n = n + m$ and $m \cdot n = n \cdot m$.
[79] I.e. $a \cdot (b + c) = a \cdot b + a \cdot c$.
[80] I.e. $(a < b) \Rightarrow \neg(b < a)$.
[81] I.e. exactly one of $a < b$, $a = b$, $a > b$ is true. Also, $((a \leqslant b) \wedge (a \geqslant b)) \Rightarrow (a = b)$.
[82] Hence, if $S = U \cup V$ and $U \cap V = \emptyset$, then $\sum S = \sum U + \sum V$ and $\prod S = \prod U \cdot \prod V$.
[83] I.e. the sum or product of a set S is independent of how it is enumerated.
[84] We use a sequence rather than a set, as e.g. $\sum(1, 1) = 2 \neq \sum\{1, 1\} = \sum\{1\} = 1$.