§1 Set Theory

We start with the undefined concepts set and element, and the undefined relation "is a member of" between elements and sets. We adopt the convention that there is just one set with no members, the empty set Φ.

The "set of all x such that $P(x)$ holds" is written $\{x \mid P(x)\}$

Defn 1: Two sets A, B are ~~equal~~ if $(\forall x)(x \in A \Leftrightarrow x \in B)$

Defn 2: A is a subset of B iff $(\forall x)(x \in A \Rightarrow x \in B)$
We write $A \subseteq B$ (or $A \subset B$ if $A \neq B$ (a proper subset))

Note: $\Phi \subseteq A$ for any set A.
$A = B \Leftrightarrow A \subseteq B \wedge B \subseteq A$ (Prove)

Defn 3: The powerset of a set S is the set of all subsets of S, written 2^S.

Complement, Union, Intersection & Difference

Defn 4: The complement of a set A is $A' := \{x \mid x \notin A\}$

Defn 5: The difference between two sets A and B is
$$A \setminus B := \{x \mid x \in A \wedge x \notin B\}$$

Defn 6: The union of two sets A and B is
$$A \cup B := \{x \mid x \in A \vee x \in B\}$$

Defn 7: The intersection of two sets A and B is
$$A \cap B := \{x \mid x \in A \wedge x \in B\}$$

Defn 8: Two sets A, B are *disjoint* if $A \cap B = \phi$

Important Laws of Set Algebra

1	Commutative	$A \cup B = B \cup A$	$A \cap B = B \cap A$
2	Associative	$A \cup (B \cup C) = (A \cup B) \cup C$	$A \cap (B \cap C) = (A \cap B) \cap C$
3	Distributive	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
4	Identity	$A \cup \phi = \phi \cup A = A$	$A \cap U = U \cap A = A$
5	Complement	$A \cup A' = U$	$A \cap A' = \phi$
6	Involution	$(A')' = A$	
7	Idempotent	$A \cup A = A$	$A \cap A = A$
8	Null	$A \cup U = U$	$A \cap \phi = \phi$
9	Absorption	$A \cup (A \cap B) = A$	$A \cap (A \cup B) = A$
10	De Morgan	$(A \cup B)' = A' \cap B'$	$(A \cap B)' = A' \cup B'$

Indexed Sets

Suppose we have a collection of sets $\{A_\alpha\}_{\alpha \in K}$ where K is some set called the *index set*.

Then:

Defn 9: $\bigcup_{\alpha \in K} A_\alpha = \{x \mid x \in A_\alpha, \text{ some } \alpha \in K\}$

$\bigcap_{\alpha \in K} A_\alpha = \{x \mid x \in A_\alpha, \text{ all } \alpha \in K\}$

§2 Relations

Defn 2: Let $A_1, \ldots, A_n$ be sets. The *Cartesian Product* of these sets is:

$$A_1 \times A_2 \times \ldots \times A_n := \{x \mid x = (a_1, a_2, \ldots, a_n);\ a_i \in A_i,\ 1 \overset{i \in \mathbb{Z}}{\leq} i \leq n\}$$

Defn 2: - A *unary relation* over a set A is a subset of A
- a *binary relation* over sets A, B is a subset of $A \times B$
- an *n-ary relation* over sets $A_1, A_2, \ldots, A_n$ is a subset of $A_1 \times A_2 \times \ldots \times A_n$

Note: we will deal almost exclusively with binary relations

Defn 3: Let ρ be a relation $\rho \subseteq A \times B$. Then:

- the *domain* of ρ is $\{a \mid (a,b) \in \rho, \text{ some } b \in B\}$
- the *range* of ρ is $\{b \mid (a,b) \in \rho, \text{ some } a \in A\}$

We write $a \rho b$ if $(a,b) \in \rho$.

Defn 5: The *inverse* (or *converse*) of a relation $\rho \subseteq A \times B$ is the relation ρ^{-1} such that

$$(b,a) \in \rho^{-1} \Leftrightarrow (a,b) \in \rho.$$

Note: $\rho^{-1} \subseteq B \times A$

Relation Matrix

Defn 6: If A, B are finite sets, $\#A = m$, $\#B = n$, we define the *relation matrix* R associated with each relation $\rho \subseteq A \times B$ and each listing $A = \{a_1, a_2, \ldots a_m\}$, $B = \{b_1, b_2, \ldots, b_n\}$ by:

$$(R)_{ij} = \begin{cases} 1 & \text{if } (a_i, b_j) \in \rho \\ 0 & \text{if } (a_i, b_j) \notin \rho \end{cases}$$

Note R is not unique, but depends on how we construct our listings (as the sets A, B themselves are unordered).

DEFN 7: – If $\rho \subseteq A \times A$, ρ is a relation on A
– $U_A = A \times A$ is called the universal relation on A
– $I_A = \{(a,a) \mid a \in A\}$ is the identity relation on A

GRAPH OF A RELATION

We can represent a relation by a graph, provided the relation is on a finite set A. The elements of A are called vertices (written in circles). If $a \rho b$ then a and b should be joined by a line with an arrow pointing from a to b. Such a line is called an edge.

COMPOSITION OF RELATIONS

DEFN 8: Let $\rho_1 \subseteq A_1 \times A_2$ and $\rho_2 \subseteq A_2 \times A_3$. We define the composition of ρ_1 and ρ_2, written $\rho_1\rho_2$ or $\rho_1 \circ \rho_2$, as the relation on $A_1 \times A_3$ such that

$$a(\rho_1\rho_2)c \Leftrightarrow (\exists b \in A_2 : a \rho_1 b \wedge b \rho_2 c)$$

Note: $I_A \rho = \rho I_B = \rho$ for $\rho \subseteq A \times B$

$\rho\rho^{-1} \supseteq I_{\text{domain}\,\rho}$

$\rho^{-1}\rho \supseteq I_{\text{range}\,\rho}$

} for any $\rho \subseteq A \times B$.

To find the graph of composition for a relation ρ on A (ie $\rho \subseteq A \times A$), we use $(a,b) \in \rho^k \Leftrightarrow$ there is a path of length k from a to b.

It can also be constructed inductively, $\rho^3 = \rho^2 \rho$, $\rho^4 = \rho^3 \rho$, etc.

The matrix of composition can be found by performing the usual matrix multiplication but with the rules:

$0 + 0 = 0$ $\qquad$ $0 \cdot 0 = 0$

$1 + 0 = 0 + 1 = 1$ $\qquad$ $0 \cdot 1 = 1 \cdot 0 = 0$

$1 + 1 = 1 \leftarrow$ (≠) NB $\qquad$ $1 \cdot 1 = 1$

TYPES OF RELATIONS

DEFN 9: Let ρ be a relation on A, and domain $\rho = A$, range $\rho = A$. Then

- ρ is reflexive if $(\forall a \in A)(a \rho a)$
- ρ is symmetric if $(\forall a,b \in A)(a \rho b \Rightarrow b \rho a)$
- ρ is antisymmetric if $(\forall a,b \in A)(a \rho b \wedge b \rho a \Rightarrow a = b)$
- ρ is transitive if $(\forall a,b,c \in A)(a \rho b \wedge b \rho c \Rightarrow a \rho c)$

DEFN 10: The transitive closure ρ^+ of a relation ρ on A is $\rho^+ := \bigcup_{i=1}^{\infty} \rho^i$

THEOREM 1: Let ρ be a relation on A. Then

(a) ρ^+ is transitive

(b) if $\rho \subseteq \sigma$ and σ is transitive, then $\rho^+ \subseteq \sigma$

PROOF: (a) $a\rho^+ b$ and $b\rho^+ c \Rightarrow \exists\, p, q$ such that $a\rho^p b$ and $b\rho^q c$. But then $a\rho^{p+q} c \Rightarrow a\rho^+ c$

(b) If $a\rho^+ b$ then $\exists\, p$ such that $a\rho^p b$
i.e. $a\rho a_1, a_2\rho a_2, \ldots, a_{p-1}\rho b$
for some $a_1, a_2, \ldots, a_{p-1}$

Since $\rho \subseteq \sigma$, we have $a\sigma a_1, a_1\sigma a_2, \ldots, a_{p-1}\sigma b$
By transitivity of σ, $a\sigma b$
$\therefore \forall a, b \in A,\ a\rho^+ b \Rightarrow a\sigma b$
$\Rightarrow \rho^+ \subseteq \sigma$

Note: We have just shown that ρ^+ is the smallest transitive relation containing ρ.

EQUIVALENCE RELATIONS

DEFN 11: A relation ρ on A is an equivalence relation if ρ is reflexive, symmetric and transitive.

DEFN 12: A partition of a set A is a family $\{A_\alpha\}_{\alpha\in K}$ of subsets of A, such that:

- $A = \bigcup_{\alpha\in K} A_\alpha$
- For $\alpha, \beta \in K$, $A_\alpha \cap A_\beta = \phi$ or $A_\alpha = A_\beta$
- $A_\alpha \neq \phi$, $\forall \alpha \in K$

DEFN 13: Let ρ be an equivalence relation on A.
The equivalence class of $a \in A$ is:
$$E_\rho(a) := \{x \mid x \in A \wedge a\rho x\}$$

THEOREM 2: The family of equivalence classes $\{\xi_\rho(a)\}_{a\in A}$ is a partition of A.

PROOF (iii) $a \rho a \Rightarrow a \in \xi_\rho(a) \Rightarrow \xi_\rho(a) \neq \phi$, all $a \in A$.

(i) since $a \in \xi_\rho(a), \forall a \in A$, $A = \bigcup_{a\in A} \xi_\rho(a)$

(iii) Let $a, b \in A$. We show $\xi_\rho(a) \cap \xi_\rho(b) = \phi$, or $\xi_\rho(a) = \xi_\rho(b)$.

Suppose $c \in \xi_\rho(a) \cap \xi_\rho(b)$ (ie $\xi_\rho(a) \cap \xi_\rho(b) \neq \phi$)
Then $a \rho c$ and $b \rho c$
By symmetry, $c \rho b \Rightarrow a \rho b$ by transitivity
Hence for any $d \in \xi_\rho(a)$, $a \rho d$.
and $a \rho b, \Rightarrow b \rho a \Rightarrow b \rho d \Rightarrow d \in \xi_\rho(b)$

Similarly, $d \in \xi_\rho(b) \Rightarrow d \in \xi_\rho(a) \Rightarrow \xi_\rho(d) = \xi_\rho(b)$

Those three together show that $\{\xi_\rho(a)\}_{a\in A}$ forms a partition.

NOTATION: The family of equivalence classes of A w.r.t. an equivalence relation ρ is written A/ρ and is called the quotient (set) of A w.r.t ρ

THEOREM 3: Let $\{A_\alpha\}_{\alpha\in K}$ be a partition of A. Define ρ to be the relation on A such that $a \rho b$ iff both $a, b \in A_\alpha$ some α. Then ρ is an equivalence relation induced by the partition

PROOF: Exercise

Residue Arithmetic

We define a relation "$\equiv_p$" (called congruence mod p) on $\mathbb{Z}$ for each integer $p > 0$.

Defn 14: Let $a, b \in \mathbb{Z}$ and let $p \in \mathbb{N}^+$. Then $a \equiv_p b$ if $a - b = np$ for some $n \in \mathbb{Z}$.

We usually write $a \equiv_p b$ as $a \equiv b \pmod{p}$

Theorem 4: $\equiv_p$ is an equivalence relation on $\mathbb{Z}$.

Proof: Since $p > 0$ divides 0, we have $a \equiv a \pmod{p}$ for all $a \Rightarrow$ reflexive

If p divides $a - b$ then p divides $b - a$
$\Rightarrow$ symmetric

If $a \equiv b \bmod p$ and $b \equiv c \bmod p$, then
p divides $(a-b)$ and $(b-c)$
$\Rightarrow p$ divides $(a-b) + (b-c) = (a-c)$
$\Rightarrow a \equiv c \bmod p \Rightarrow$ transitive

Note $a \equiv 0 \pmod{p} \Leftrightarrow p$ divides a

Cor: There are p equivalence classes $(\bmod p)$. These are also called residue classes $(\bmod p)$

Proof: On division by p, any integer a leaves a remainder of one of $0, 1, \ldots, (p-1)$. Given a, let the remainder be r_a. Then $a - r_a = np$, some $n \Rightarrow a \equiv r_a \pmod{p}$. Hence each lies in at least one of the classes $\xi(0), \ldots, \xi(p-1)$

If $0 \le a \le p-1$ and $0 \le b \le p-1$, then $a \equiv b \pmod p \Leftrightarrow a = b$

$\Rightarrow$ none of these classes can be equal.

$\Rightarrow$ the equivalence classes are $\xi(0), \ldots, \xi(p-1)$

THEOREM 5: Suppose $a \equiv b \pmod p$ and $c \equiv d \pmod p$

Then: (a) $a + c \equiv b + d \pmod p$

(b) $ac \equiv bd \pmod p$

$ag \equiv bg \pmod p$, all $g \in \mathbb{Z}$.

PROOF: (a) p divides $(a-b)$ and $(c-d) \Rightarrow p$ divides $(a-b)+(c-d)$

– ie p divides $(a+c)-(b+d) \Rightarrow (a+c) \equiv (b+d) \bmod p$

(b) p divides $(a-b)c$ and p divides $b(d-c)$

$\Rightarrow p$ divides $(a-b)c - b(d-c) = ac - bd$

$\Rightarrow ac \equiv bd \bmod p$

Using this on $a \equiv b \bmod p$ and $g \equiv g \bmod p$

gives $ag \equiv bg \pmod p$.

THEOREM 6 (CANCELLATION LAW)

If p is prime and $c \not\equiv 0 \pmod p$ then

$ac \equiv bc \pmod p \Rightarrow a \equiv b \pmod p$

PROOF: p divides $ac - bc = (a-b)c$

$\Rightarrow p \mid (a-b)$ or $p \mid c$, since p is prime.

– but $p \nmid c$ (as $c \not\equiv 0 \pmod p$) $\Rightarrow p \mid (a-b)$

$\Rightarrow a \equiv b \pmod p$

COROLLARY (FERMAT'S THEOREM)

Let p be prime and $a \not\equiv 0 \pmod p$. Then $a^{p-1} \equiv 1 \pmod p$

PROOF: $1, 2, \ldots, (p-1)$ lie in different residue classes. Then so do $a.1, a.2, \ldots, a.(p-1)$ (by theorem 6, $aa_i \not\equiv a_j.a \pmod p \Rightarrow a_i \equiv a_j \pmod p$, which is false).

But then $a.1, a.2, \ldots, a.(p-1)$ are representatives of all possible residue classes except 0.

$\Rightarrow 1.2.\ldots.(p-1) \equiv (a.1)(a.2)\ldots a.(p-1) \pmod p$

$\Rightarrow 1.2.\ldots.(p-1) \equiv a^{p-1}(1.2.\ldots.(p-1)) \pmod p$

By theorem 6, $1 \equiv a^{p-1} \pmod p$.

PARTIAL ORDERINGS

DEFN 16: A partial ordering on a set A is a relation that is reflexive, antisymmetric and transitive, usually denoted by $\leq$

DEFN 17: (a) A partial ordering $\leq$ on A is said to be a total ordering if for each $a, b \in A$, either $a \leq b$ or $b \leq a$

(b) A partial ordering $\leq$ on A is said to be a well ordering if for every subset $S \subseteq A$, S has at least one number i.e. $\exists a_s \in S : (\forall x \in S)(a_s \leq x)$

Note: a well ordering must be total

§3 FUNCTIONS

DEFN 1: A *partial function* f from A to B is a binary relation $f \subseteq A \times B$: $\forall a \in A$ there is at most one b such that $(a,b) \in f$.

Note: a partial function is a single-valued relation.

DEFN 2: A *function* f from A to B is a partial function $f \subseteq A \times B$ with domain $(f) = A$, written $f : A \to B$

DEFN 3: If f is a function $f : A \to B$, then B is called the *codomain* of f. The range of f, written $f(A)$, is thus a subset of the codomain.

DEFN 4: Two functions $f : A \to B$ and $g : C \to D$ are *equal*, written $f = g$, if $A = B$, $C = D$ and the subsets f, g are equal

NOTATION: The set of all functions from A to B is written B^A

DEFN 5: Given $f : A \to B$, a function:

(a) If $\forall b \in B$, $\exists$ at most one $a \in A$ such that $(a,b) \in f$, then f is *one-one* or *injective*

(b) If $\forall b \in B$, $\exists a : (a,b) \in f$ then f is *onto* or *surjective* (ie $f(A) = B$) (range = codomain)

(c) If f is both one-one and onto, it is *bijective*

Defn 6: Let $f: A \to B$, $g: B \to C$ be functions. The composition of f and g (written $g \circ f$) is defined by: $g \circ f : A \to C$, $a \to g(f(a))$

Notation: The identity function I_A on a set A is defined by $I_A(a) = a$ for all $a \in A$

$I_A : A \to A$

I_A is bijective

Note: $f: A \to B$. Then $f \circ I_A = f$ and $I_B \circ f = f$

Defn 7: Let $f: A \to B$ and $g: B \to A$ be functions. Then: (a) If $f \circ g = I_B$, g is a right inverse of f

(b) If $g \circ f = I_A$, g is a left inverse of f

(c) If $f \circ g = I_B$ and $g \circ f = I_A$, g is an inverse of f written $g = f^{-1}$

Note: f always has an inverse which is a relation. It does not always have a function as an inverse.

Theorem 1: Let f be a function $f: A \to B$

(a) f has a left inverse iff f is an injection

(b) f has a right inverse iff f is a surjection

(c) f has an inverse iff f is a bijection.

Proof (a) Suppose f has a left inverse $g: B \to A$. Then $g \circ f = I_A$. Suppose $f(a) = f(a')$. We must show that $a = a'$ (ie f is injective)

$a = I_a(a) = (g \circ f)(a) = g(f(a)) = g(f(a')) = (g \circ f)a' = I_a(a') = a'$

Suppose f is an injection. Then define $g: B \to A$ by

$$g(b) = \begin{cases} a & \forall b \in B : f(a) = b \\ a_0 & \text{otherwise, } a_0 \in A \text{ is fixed and arbitrary} \end{cases}$$

Since f is injective, there is exactly one $b \in B$ such that $f(a) = b \Rightarrow g$ is well-defined.
Also, $a \in A \Rightarrow (g \circ f)(a) = g(f(a)) = g(b) = a$
$\Rightarrow g \circ f = I_A$ (i.e. g is a left inverse of f)

(b) is similar to (a), (c) follows from (a) and (b).

§4 Countability and Cardinality

1 Equipotence and Finite Sets

1.1 **Defn**: Two sets A, B are *equipotent* (or *equivalent*) iff there is a bijection $h: A \to B$. We write $A \simeq B$

1.2 **Proposition**: For sets A, B, C we have:

(i) $A \simeq A$

(ii) $A \simeq B \Rightarrow B \simeq A$

(iii) $A \simeq B \wedge B \simeq C \Rightarrow A \simeq C$

Thus, on any collection of sets, equipotence is an equivalence relation.

1.3 We now wish to introduce the idea of *cardinality* of a set. It is difficult to do this precisely: we want for all sets A, B, $\#A = \#B \Leftrightarrow A \simeq B$

Before 1900 the method was to split the class of all sets into the equivalence classes induced by the relation $\simeq$. However, the Russel paradox makes it very awkward to handle this concept of cardinality within axiomatic set theory.

The modern method is to select one set as representative from each equivalence class of $\simeq$. We will not examine the details of selection here; we simply accept:

1.4 There is a procedure which assigns to each set A its cardinal number, written $\#A$, in such a way that $\#A = \#B \Leftrightarrow A \simeq B$

1.5 **DEFINITION** The set A is *finite* $\Leftrightarrow (\exists n \in \mathbb{N})(\#A = n)$
When A is not finite, we say A is *infinite*

1.6 We now give a construction of $\mathbb{N}$, a special case of the construction in 1.3.

1.6.1 **DEFN:** A set X is *inductive* iff
(i) $\forall x \in X$, x is a set
(ii) $\Phi \in X$
(iii) $\forall x \in X$, $x \cup \{x\} \in X$

1.6.2 **AXIOM OF INFINITY:** There exists at least one inductive set

1.6.3 **DEFN** $\mathbb{N} = \bigcap \{X \mid X \text{ is inductive}\}$
ie $\mathbb{N}$ is the intersection of all inductive sets.
(so $\mathbb{N}$ consists solely of sets of empty sets!)

Generally, $n+1 = n \cup \{n\}$, thus: $0 = \Phi$
$1 = \{\Phi\}$
$2 = \{\Phi, \{\Phi\}\}$
$3 = \{\Phi, \{\Phi\}, \{\Phi, \{\Phi\}\}\}$
$\vdots$

Thus n is the selected representative of the equivalence class of all sets with cardinality n.

1.7 **PROPOSITION** A is infinite $\Leftrightarrow \exists$ an injective function $f: \mathbb{N} \to A$

2 COUNTABILITY

2.2 PROPOSITION: A is infinite $\Leftrightarrow (\exists B)(B \subset A$ and $A \simeq B)$

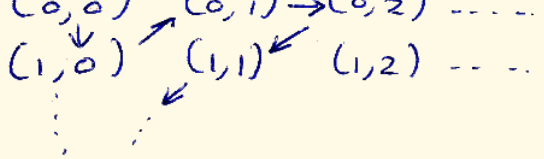
PROOF: Suppose A is infinite. By 1.7 we have an injection $f: \mathbb{N} \to A$. Then $A = C \cup D$, where $C = f[\mathbb{N}]$ and $D = A \setminus C$.
Let $B = f[\mathbb{N} - \{0\}] \cup D$
Clearly $B \subset A$ and a bijection can be constructed from A to B. We assume the converse is obvious.

2.3 PROPOSITION: Every infinite subset of $\mathbb{N}$ is equivalent to $\mathbb{N}$.

PROOF: The infinite subset A must have its elements arranged in order of magnitude, ie, say $A = \{m_0, m_1, m_2, \ldots\}$ where $m_0 < m_1 < \ldots m_i < \ldots$ Then we have a bijection $h: \mathbb{N} \to A$ given by $h(n) = m_n$.

2.4 THEOREM: $\mathbb{N} \times \mathbb{N} \simeq \mathbb{N}$

PROOF: Diagonal argument



or by $f(m,n) = 2^m 3^n$ with unique factorisation theorem.

2.5 **Theorem**: The set $\mathbb{Q} \simeq \mathbb{N}$

Proof: Diagonal argument:

$$\begin{array}{ccccc} \frac{1}{1} & \frac{2}{1} & \frac{3}{1} & \frac{4}{1} & \frac{5}{1} \cdots \\ \frac{1}{2} & \frac{2}{2} & \frac{3}{2} & \frac{4}{2} & \cdots \\ \frac{1}{3} & & & & \\ \vdots & & & & \end{array}$$

or define $f: \mathbb{Q} \to \mathbb{Z} \times \mathbb{N}$. Reduce each $q \in \mathbb{Q}$ to lowest terms $\frac{m}{n}$, $m \in \mathbb{Z}$, $n \in \mathbb{N}$. Then let $f(m/n) = (m, n) \in \mathbb{Z} \times \mathbb{N}$, which is clearly injective. By 2.1 we know $\mathbb{Z} \simeq \mathbb{N}$ so $g: \mathbb{Z} \times \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ is a bijection which exists. And by 2.4 we have $\mathbb{N} \times \mathbb{N} \simeq \mathbb{N}$.

2.6 $\#\mathbb{N} = \aleph_0$

2.7 **Defn**: A is <u>denumerable</u> $\Leftrightarrow A \simeq \mathbb{N}$ (also called <u>countably infinite</u>)

2.8 $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{N}^2$, $\mathbb{Z}^3$, etc are all denumerable

2.9 **Proposition**: If A, B are denumerable then $A \times B$ is denumerable (from $\mathbb{N} \times \mathbb{N} \simeq \mathbb{N}$).

2.10 **Theorem**: The union of denumerably many denumerable sets is denumerable.

Proof: ~~Diagonal argument~~ - enumerate the sets in rows

A_1 : a_{11} a_{12} a_{13} ……

A_2 : a_{21} a_{22} a_{23} ……

⋮

2.11 DEFN: A set A is called <u>countable</u> iff it is finite or denumerable.

Hence, A denumerable $\Leftrightarrow$ A is countable and infinite

2.12 PROPOSITION: A is countable $\Leftrightarrow$ $\exists$ a injection $f: A \to \mathbb{N}$
(consider 2.3)

2.13 PROPOSITION:- The product of two countable sets is countable
- The union of countably many countable sets is countable.

3 UNCOUNTABLE SETS.

3.1 DEFN: A set is <u>uncountable</u> iff it is not countable

3.2 THEOREM: The set $\mathbb{R}$ of all real numbers is uncountable.

PROOF: (Georg Cantor's diagonal argument 1874)
Suppose $\mathbb{R}$ is countable. Then $[0,1)$ is countable.
Then there is a bijection $f: \mathbb{N}^+ \to [0,1)$, ie, the elements of $[0,1)$ all occur in a list without repetitions.
We arrange the decimal expansions as:

$f(1) = 0, a_{11}\, a_{12}\, a_{13} \ldots$
$f(2) = 0, a_{21}\, a_{22}\, a_{23} \ldots$
$\ldots\ldots\ldots$

Then we construct $y = 0, b_1 b_2, \ldots$ by $\begin{cases} b_n = 2 & \text{when } a_{nn} = 1 \\ b_n = 1 & \text{when } a_{nn} \neq 1 \end{cases}$

Then $y \neq f(n)$ all n. But $y \in [0,1)$.

3.3 COROLLARY: There are uncountably many irrational numbers (we know $\mathbb{Q}$ is denumerable. If $\mathbb{R} - \mathbb{Q}$ was countable, then $\mathbb{Q} \cup (\mathbb{R} \setminus \mathbb{Q}) = \mathbb{R}$ would also be).

3.4 By this time we have a cardinal other than $\aleph_0$. It can be shown that $\mathbb{R} \times \mathbb{R} \simeq \mathbb{R}$ (and in fact $A \times A \simeq A$, any infinite set A).

3.5 DEFN $\#A \leq \#B \iff \exists$ injection $f: A \to B$

3.6 The relation $\leq$ is obviously reflexive and transitive. We shall now show that it is antisymmetric and hence a partial order.

3.7 SCHRÖDER - BERNSTEIN THEOREM (1897)

Given two injective functions $f: A \to B$, $g: B \to A$, we can construct a bijection $h: A \to B$.

PROOF: Let $C_A : \mathcal{P}A \to \mathcal{P}A$ be the function which takes complements in A, ie, $\forall X \in \mathcal{P}A$, $C_A(X) = A \setminus X$. Similarly we have $C_B : \mathcal{P}B \to \mathcal{P}B$

We have a function $\vec{f} : \mathcal{P}A \to \mathcal{P}B$ given by $\forall X \in \mathcal{P}A$, $\vec{f}(X) = f[X]$. Likewise $\vec{g} : \mathcal{P}B \to \mathcal{P}A$

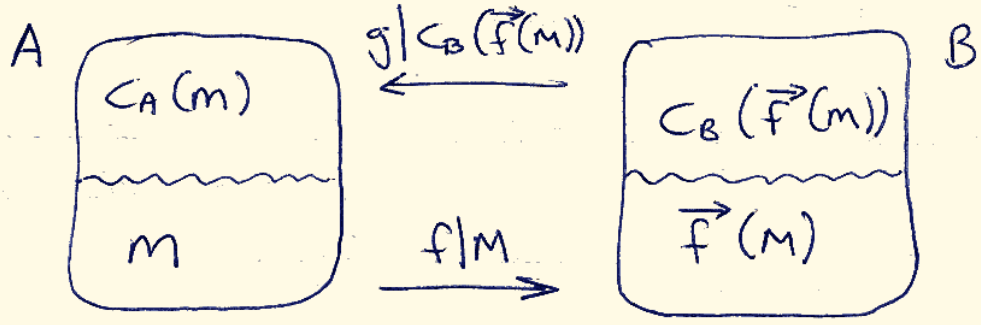
Below, we shall construct a set $M \subseteq A$ such that

① $C_A(M) = \vec{g}(C_B(\vec{f}(M)))$

Taking ① as true, we immediately have a bijective function $h: A \to B$ given by

② $h = (f|M) \cup (g|C_B(\vec{f}(M)))^{-1}$

Here the notation $f|M$ means the function which is the restriction of f to M –


A
$C_A(m)$
m
$g|C_B(\vec{f}(m))$
$f|M$
$C_B(\vec{f}(m))$
$\vec{f}(m)$
B

Bearing in mind that f and g are both injective, we can see that h is made up of two non-overlapping (by ①) injective "pieces"; the range of h is B, and the domain is A (again by ①)

It remains to construct M satisfying ①. Consider

$$\mathcal{P}A \xrightarrow{\vec{f}} \mathcal{P}B \xrightarrow{C_B} \mathcal{P}B \xrightarrow{\vec{g}} \mathcal{P}A \xrightarrow{C_A} \mathcal{P}A.$$

Call the composite of these four functions $\ell : \mathcal{P}A \to \mathcal{P}A$.

③ ℓ preserves inclusions because $\vec{f}$ and $\vec{g}$ both preserve inclusions while C_A and C_B reverse inclusions

④ Let $\mathcal{J} = \{X \in \mathcal{P}A \mid X \subseteq \ell(X)\}$
Observe that $\mathcal{J} \neq \emptyset$ because $\emptyset \in \mathcal{J}$

⑤ Let $M = \bigcup_{X \in \mathcal{J}} X$

Then clearly:

⑥ $\forall X \in \mathcal{J},\ X \subseteq M$

Applying ③ to ⑥ one has $\ell(X) \subseteq \ell(M)$
by ④ $X \subseteq \ell(X)$, hence:

⑦ $\forall X \in \mathcal{J} \quad X \subseteq \ell(M)$

From ⑦ and ⑤ we get:

⑧ $M \subseteq \ell(M)$

By ③ then, $\ell(M) \subseteq \ell(\ell(M))$, so that by ④, $\ell(M) \in \mathcal{J}$ and then by ⑥ $\ell(M) \subseteq M$. This, and ⑧ gives $\ell(M) = M$ i.e. $M = C_A(\vec{g}(C_B(\vec{f}(M))))$. Applying C_A to this gives ①, as $C_A(C_A(u)) = u$

3.8 COROLLARY: The relation $\leq$ in 3.5 is a partial order.

3.9 REMARK: It was a difficult problem for Cantor and others whether $\leq$ is a total ordering of the cardinals, ie whether given any two sets A and B one is always assured that there will be an injection $f: A \to B$ or $g: B \to A$. In 1904 E. Zermelo proved $\leq$ is a well-ordering of the cardinals, hence a total ordering, provided one accepts the axiom of choice. In 1915 F. Hartogs proved that $\leq$ is a total ordering $\Rightarrow$ Axiom of Choice. Zermelo's basic result was Axiom of Choice $\Leftrightarrow$ every set can be well-ordered.

3.10 CANTOR'S THEOREM (1892) $\quad \#A < \#\mathcal{P}A$

PROOF: This means ① $\#A \leq \#\mathcal{P}A$
and ② $\#A \neq \#\mathcal{P}A$.

To prove ① we need an injection $f: A \to \mathcal{P}A$. That is very easy: let $\forall x \in A$, $f(x) = \{x\}$, clearly an injection.

To prove ② we need to show that there can be no bijection between A and $\mathcal{P}A$. We shall in fact show that there cannot even be a surjection.

Suppose $g: A \to \mathcal{P}A$ is a surjection. Define $B = \{x \in A \mid x \notin g(x)\}$
Since g is surjective and $B \in \mathcal{P}A$, there exists an elt $a \in A$ such that $g(a) = B$. Thus $g(a) = \{x \in A \mid x \notin g(x)\}$
Hence $a \in g(a) \Leftrightarrow a \notin g(a)$, thus g cannot be surjective

3.11 **REMARK**: Cantor's Theorem tells us that there is no greatest cardinal, because for any cardinal, the cardinal of the corresponding power set is still greater. It also tells us that we have infinitely many different infinite cardinals, eg

$$\#\mathbb{N} < \#\mathcal{P}\mathbb{N} < \#\mathcal{P}\mathcal{P}\mathbb{N} < \dots$$

We now know that $\mathcal{P}\mathbb{N}$ is uncountable.

3.12 **DEFN**: For any sets A, B, $B^A = \{f \mid f: A \to B \text{ is a function}\}$

REMARK: Consider finite sets A, B; say $\#A = m$, $\#B = n$. It is easy to see there are n^m functions from A to B. In particular there are precisely 2^m functions from $A \to \{0,1\}$

3.13 **DEFN**: For any cardinals m, n, n^m is defined to be the cardinal of B^A where A, B are sets such that $\#A = m$ and $\#B = n$.

In particular $2^{\#A} = \#(\{0,1\}^A) = \#(2^A)$

3.14 **THEOREM**: For any set A, $\mathcal{P}A \simeq \{0,1\}^A$
Consequently $\#\mathcal{P}A = 2^{\#A}$

PROOF: To each $X \subseteq A$ we construct the function $\lambda_X : A \to \{0,1\}$ as follows:

$$\forall a \in A,\ \lambda_X(a) = \begin{cases} 1 & \text{if } a \in X \\ 0 & \text{if } a \notin X \end{cases}$$

This gives us a function $\lambda: \mathcal{P}A \to \{0,1\}^A$ given by $\lambda(X) = \lambda_X$, all $X \in \mathcal{P}A$. We show that λ is bijective:

Injective: Suppose $X \neq Y$. There is some $a \in X$ with $a \notin Y$ (or vice-versa). Then $\lambda_X(a) = 1$ but $\lambda_Y(a) = 0$, so $\lambda_X \neq \lambda_Y$. Thus λ is injective

Surjective: Consider any $f \in \{0,1\}^A$, ie $f: A \to \{0,1\}$
We have to find $X \in \mathcal{P}A$ with $f = \lambda_X$
Let $X = \{a \in A \mid f(a) = 1\}$. Clearly $\lambda_X = f$.

3.15 An infinite sequence $(x_1, x_2, \ldots)$ of elts $x_n \in A$ is defined to be the function $f: \mathbb{N}^+ \to A$ given by $\forall n \in \mathbb{N}^+ \quad f(n) = x_n$. Thus $A^{\mathbb{N}^+}$ is the set of all (infinite) sequences of elts of A. In particular, $2^{\mathbb{N}^+} = \{0,1\}^{\mathbb{N}^+}$ is the set of all (infinite) sequences of zeroes and ones.

3.16 LEMMA: $[0,1) \simeq \mathbb{R}$

PROOF: $x \mapsto x$ is an injection from $[0,1)$ to $\mathbb{R}$
Also $\mathbb{R} \simeq (0,1)$, hence we have an injection from $\mathbb{R}$ into $[0,1)$. Then by Schröder-Bernstein (3.7) $[0,1) \simeq \mathbb{R}$.

3.17 THEOREM: $\mathbb{R} \simeq 2^{\mathbb{N}^+}$, that is, $\#\mathbb{R} = 2^{\aleph_0}$

PROOF: Express $x \in [0,1)$ in base 2, giving a binary expansion
If x has a terminating expansion we use this and ignore the non-terminating expansion. We thus get a injection from $[0,1)$ into $2^{\mathbb{N}^+}$

On the other hand, starting with any sequence of 0's

and 1's, we can map this into $\mathbb{R}$ by using binary expansions in $[0,1)$, except in the case of non-terminating 1111.... sequences, which we map into $[1,2)$ instead. We thus have a map from $\{0,1\}^{\mathbb{N}^+}$ into $\mathbb{R}$. We know $\mathbb{R} \simeq [0,1)$, so by Schröder-Bernstein, $2^{\mathbb{N}^+} \simeq [0,1) \simeq \mathbb{R}$.

3.18 ADDITION OF CARDINALS is defined by

$$\#A + \#B = \#(A \cup B) \quad \text{provided } A \cap B = \phi.$$

Given any two cardinals m and n, we simply have to find sets A, B with $A \cap B = \phi$ and $\#A = m$, $\#B = n$., and then we form $m+n = \#(A \cup B)$.

If A and B are not disjoint, we can make them disjoint as $A \simeq A \times \{0\}$, $B \simeq B \times \{1\}$ and $(A \times \{0\}) \cap (B \times \{1\}) = \phi$.

Since the union of two (disjoint) denumerable sets is denumerable, we have:

$$\aleph_0 + \aleph_0 = \aleph_0$$

It is easy to see that $\aleph_0 + 2^{\aleph_0} = 2^{\aleph_0} + 2^{\aleph_0} = 2^{\aleph_0}$

MULTIPLICATION OF CARDINALS is defined by

$$\#A \times \#B = \#(A \times B)$$

If $X \cap Y = \phi$, then $B^X \times B^Y \simeq B^{X \cup Y}$ (prove this) and this gives a useful identity for cardinal numbers:

$$k^m \cdot k^n = k^{m+n}$$

In particular $2^{\aleph_0} \cdot 2^{\aleph_0} = 2^{\aleph_0 + \aleph_0} = 2^{\aleph_0}$. This proves Cantor's

result of 1874, namely

3.19 COROLLARY : $\mathbb{R} \times \mathbb{R} \simeq \mathbb{R}$

3.20 We now try to bring it all together :

3.20.1 $\aleph_0$ is the least infinite cardinal

Proof : Given any infinite set A, there is an injective function $f : \mathbb{N} \to A$. Then $\aleph_0 \leq \#A$ by defn 3.5

3.20.2 For any set A

A is countable $\Leftrightarrow \#A \leq \aleph_0$

A is uncountable $\Leftrightarrow \aleph_0 < \#A$

PROOF: The first is 2.12 with 3.5

To prove the second : A is uncountable means A is infinite but not denumerable. Now, A is infinite $\Leftrightarrow \aleph_0 \leq \#A$ (by 3.20.1) Also, A is not denumerable $\Rightarrow \aleph_0 \neq \#A$.

3.203 $m < 2^m$ for every cardinal number m.

PROOF: This is just 3.10 with 3.14 and 3.13.

3.204 $\mathbb{R} \simeq 2^{\mathbb{N}} \simeq \mathcal{P}\mathbb{N} \simeq \mathbb{R} \times \mathbb{R}$

PROOF : This is just 3.17, 3.14 & 3.19

3.20.5 $\aleph_0 < 2^{\aleph_0} = \#\mathbb{R}$ is a second proof that $\mathbb{R}$ is uncountable.

4 Two Mind Boggers

4.1 Cantor's Paradox

Take any set S of cardinal numbers, say $S = \{k_\alpha \mid \alpha \in J\}$. Say $k_\alpha = \# A_\alpha$. Take $A = \bigcup_{\alpha \in J} A_\alpha$. Take $m = \# A$.

There is a trivial injection from A_α into A, so $k_\alpha \leq m < 2^m$. Thus $\forall \alpha \in J$, $k_\alpha < 2^m$. Therefore we have:

(4.1.2) Given any set of cardinal numbers, we can construct a cardinal number properly larger than every cardinal number in that set.

Thus the notion "set of all cardinal numbers" is impossible. Mathematics could only deal with this paradox once axiom systems were developed which restricted the collections which could be admitted as sets.

4.2 The Continuum Hypothesis.

We have mentioned (3.9) Zermelo's result that $\leq$ is a well-ordering of the cardinals. This implies that for any cardinal m, there is a least cardinal amongst all those that are greater than m. In order of magnitude, the cardinals have the following names:

$$0, 1, 2, \ldots \aleph_0, \aleph_1, \aleph_2, \ldots \aleph_\omega, \aleph_{\omega+1}, \aleph_{\omega+2}, \ldots$$

but there are many more than indicated here. (The subscripts used are the ordinals).

The axiom of Choice implies that the progression of all the alephs coincides with the class of all infinite cardinals (which is not a set, cf 4.1). In particular, the cardinal $2^{\aleph_0}$ must be one of the alephs.

In this case, $\aleph_0 < 2^{\aleph_0} \Rightarrow \aleph_1 \leq 2^{\aleph_0}$. Cantor guessed that $2^{\aleph_0} = \aleph_1$. (the Continuum Hypothesis). Strenuous research over 70 years could not prove it. In 1963 P. J. Cohen proved that the CH is independent of the other axioms of set theory, ie, we can decide whether or not we want $2^{\aleph_0} = \aleph_1$ in a particular set theory or not.

§ 5 Numbers and Polynomials

5.2 The Basic Axioms

For every $a, b, c \in \mathbb{Z}$:

A1 :	$a+b = b+a$	Commutative	M1 $a.b = b.a$
A2 :	$(a+b)+c = a+(b+c)$	Associative	M2 : $(a.b).c = a.(b.c)$
A3 :	$0+a = a+0 = a$	Identity	M3 $a.1 = 1.a = a$
A4 :	$a+(-a) = 0$	Inverse	
D :	$a.(b+c) = a.b + a.c$	Distributive	$(a+b).c = ac + bc$

P : $\mathbb{Z}$ contains a non-empty subset $\mathbb{N}$ such that

(i) $\forall x \in \mathbb{Z}$ belong to exactly one of $\mathbb{N}$, $\{0\}$, $-\mathbb{N}$
where $-\mathbb{N} = \{-x \mid x \in \mathbb{N}\}$

(ii) for all $a, b \in \mathbb{N}$, $a+b \in \mathbb{N}$ and $a.b \in \mathbb{N}$

I If U is a subset of $\mathbb{N}$ such that $1 \in U$ and such that $a \in U \Rightarrow a+1 \in U$, then $U = \mathbb{N}$
(Principle of Mathematical Induction)

5.2.1 Lemma: For all $a, b, c \in \mathbb{Z}$:

(i) $0.c = 0$

(ii) $(-a).b = -(a.b)$

(iii) $-(-c) = c$

5.2.2 Theorem: $\forall a, b \in \mathbb{Z}$, $(-a).(-b) = a.b$

5.2.4 Defn: The (unique) subset $\mathbb{N}$ of $\mathbb{Z}$ is the set of positive integers, $-\mathbb{N}$ the set of negative integers. If $a, b \in \mathbb{Z}$, we say that $a < b$ iff $b-a \in \mathbb{N}$ (a is less than b)

$a \leq b$ iff $b-a \in \mathbb{N} \cup \{0\}$

5.2.5 THEOREM: If $a, b, c \in \mathbb{Z}$, and $a < b$, $b < c$ then $a < c$

5.2.6 THEOREM: If $a, b, c \in \mathbb{Z}$ and $a < b$ and $0 < c$ then $ac < bc$

PROOF: We are given $b - a \in N$, $c \in N$. Hence by axiom P(ii) $(b-a)c \in N$. Hence $bc - ac \in N$, thus $ac < bc$.

5.2.7 DEFN: Let $a \in \mathbb{Z}$. We define $|a|$, called the modulus of a, by:

$$|a| = \begin{cases} a & \text{iff } 0 < a \\ 0 & \text{iff } 0 = a \\ -a & \text{iff } a < 0 \end{cases}$$

5.3 DIVISIBILITY, IRREDUCIBLES AND PRIMES IN $\mathbb{Z}$

5.3.1 DEFN: Let $a, b \in \mathbb{Z}$. We say a divides b, write $a | b$ iff $\exists c \in \mathbb{Z} : b = ac$. If a does not divide b we write $a \nmid b$

5.3.3 DEFN: If $a, b, d \in \mathbb{Z}$ such that $d | a$ and $d | b$, then d is a common divisor of a and b.

5.3.4 LEMMA: If $d | a$ and $d | b$, and if $s, t \in \mathbb{Z}$, then $d | sa + tb$

PROOF: Since $d | a$, $\exists u \in \mathbb{Z} : du = a$
Since $d | b$, $\exists v \in \mathbb{Z} : dv = b$
Then $sa + tb = sdu + tdv = d(su + tv)$
$\Rightarrow d | sa + tb$

5.3.5 **DEFN**: (i) If $u \in \mathbb{Z}$ and $u \mid 1$ then u is a *unit*

(ii) If $a \in \mathbb{Z}$ is neither 0 nor a unit, we say a is *irreducible* $\Leftrightarrow$ whenever a is expressed as a product $a = bc$, $b, c \in \mathbb{Z}$, it follows that either b or c is a unit.

(iii) If $a \in \mathbb{Z}$ is neither 0 nor a unit we say that a is *prime* $\Leftrightarrow$ whenever $a \mid bc$, $b, c \in \mathbb{Z}$, then $a \mid b$ or $a \mid c$ or both.

(iv) If $a, b \in \mathbb{Z}$ are such that $a = bu$ where u is a unit, then a and b are *associates*.

5.3.7 **THEOREM**: Every prime element in $\mathbb{Z}$ is irreducible.

PROOF: Let a be a prime in $\mathbb{Z}$. Then by 5.3.5(iii), $a \neq 0$ and a is not a unit. Suppose $a = bc$, $b, c \in \mathbb{Z}$. Then certainly $a \mid bc$. But a is prime, $\Rightarrow a \mid b$ or $a \mid c$ or both. Suppose $a \mid b$. Then $\exists s \in \mathbb{Z} : as = b$, $\Rightarrow asc = bc = a$

$\Rightarrow sc = 1$, thus c is a unit.

5.3.9 **LEMMA**: Let $a \in \mathbb{Z}$, $a > 1$. Then a can be expressed as a product of finitely many positive irreducibles (ie primes)

PROOF: Let S be the collection of all integers greater than 1, if any, which are *not* expressible in this form. If $S = \phi$, the result is immediate. If not, S has a least member as it is well-ordered.

m cannot be irreducible, so it can be expressed as a product, say $m = m_1 m_2$. But, since m is the least elt of S, and $1 < m_1 < m$, $1 < m_2 < m$, $m_1, m_2 \notin S$. Thus both m_1, m_2 can be expressed as products of (positive) irreducibles, and it follows that so can m. Thus $m \notin S$. Hence $S = \phi$.

5.3.10 THEOREM: There are infinitely many primes.

PROOF: Assume there are a finite number of primes, $p_1, p_2, \ldots, p_n$. Consider $N_n = (p_1 p_2 \ldots p_n) + 1$.

By 5.3.9, this can be written as a product of finitely many primes, $N_n = t_1 t_2 t_3 \ldots t_r$ say, where each t_i must be in the list $p_1, p_2, \ldots, p_n$.

Suppose $t_1 = p_m$

Then $p_m \mid p_1 p_2 \ldots p_n$ and $p_m = t_1 \mid N_n$.

Hence, by 5.3.4 with $s = 1$, $t = -1$ we get

$$p_m \mid N_n - (p_1 p_2 \ldots p_n), \text{ ie } p_m \mid 1$$

5.4 GCD's

5.4.1 DEFN: Let $a, b \in \mathbb{Z}$. An integer $c \in \mathbb{Z}$ is termed a greatest common denominator (gcd) or highest common factor (hcf) of a and b, written (a, b), iff:

(i) $c \mid a$ and $c \mid b$

(ii) if $d \mid a$ and $d \mid b$ then $d \mid c$

5.4.4 **THEOREM** Any two integers a, b, not both zero, have a unique positive gcd. Furthermore, if $c = (a,b)$, $\exists s, t \in \mathbb{Z} : c = sa + tb$.

5.4.5 **THEOREM – THE DIVISION ALGORITHM**

Let $a, b \in \mathbb{Z}$ with $b \neq 0$. Then there exist unique $m, r \in \mathbb{Z}$ such that $a = mb + r$ where $0 \leq r < |b|$

PROOF: Let $S = \{x : x = a - mb \in \mathbb{Z}^+, m \in \mathbb{Z}\}$ (i.e. $a \geq 0$)

S is not empty as $a \in S$, so S has a least member, say r. Then $r = a - m_1 b$ for some $m_1 \in \mathbb{Z}$.

We claim: $r < b$ (as r is the least member, and...)

[Otherwise $0 < b \leq r$, and $a - (m_1 + 1)b = r - b \in S$
i.e., we have a smaller elt than the smallest elt, an absurdity]

Thus we have $a = m_1 b + r$, where $0 \leq r < b$.

If $a < 0$ we can find m, r : $-a = mb + r$, $0 \leq r < b$
$\Rightarrow a = (-m)b - r$ where $-b < -r \leq 0$
but then $-a = (-m-1)b + (b - r)$
clearly $(-m-1) \in \mathbb{Z}$, and $0 < b - r < b$ if $r > 0$
(if $r = 0$, $a = (-m)b$ immediately)

The case for $b < 0$, and the proof of uniqueness is left as an exercise.

5.4.6 **PROOF OF THEOREM 5.4.4.**

Let $S = \{x \mid x = ma + nb \in \mathbb{Z}^+;\ m, n \in \mathbb{Z}\}$ (so S is non-empty)
As S is non-empty, it has a least member, say c.
We assert c is the required (unique) g.c.d of a and b.

Let $w \in S$, then by the division algorithm (for $* w, c$)

$$w = kc + r \quad ; k, r \in \mathbb{Z},\ 0 \leq r < c.$$

If $r = 0$, then we have $c \mid w$
else $(r > 0)$:

$$\text{say } \left.\begin{array}{l} w = u(a) + v(b) \in S \\ c = m(a) + n(b) \in S. \end{array}\right\} u, v, m, n \in \mathbb{Z}$$

Then $r = (u - km)a + (v - kn)b. \in S.$
but as $r \in S$ and $0 \leq r < c$, c the least member of S
we have a contradiction.
$\Rightarrow r = 0$, $w = kc$ i.e. $c \mid w$
It follows (letting $w = a$ and $w = b$) that $c \mid a$, $c \mid b$
so c is a common denominator

Say $d \mid a$ and $d \mid b$, some d.
Then $d \mid ma + nb = c$ so $d \mid c$. (i.e. $d \leqslant c$)
Thus c is the greatest common denominator
and is unique

5.4.8 **DEFN:** Two integers a, b are relatively prime or coprime
iff $(a, b) = 1$

5.4.9 **THEOREM:** Let $a, b \in \mathbb{Z}$. Then a and b are relatively prime iff $\exists\, s, t \in \mathbb{Z} : sa + tb = 1$.

5.4.10 **THEOREM:** If $a \in \mathbb{Z}$ is irreducible, then a is prime in $\mathbb{Z}$.

PROOF: Suppose $b, c \in \mathbb{Z}$ and $a \mid bc$
We want to show that $a \mid b$ or $a \mid c$, or both.

If $a \mid b$ we are finished, so suppose $a \nmid b$.
It follows that $(a, b) = 1$, (as a is irreducible, its only divisors are $\pm 1, \pm a$. As $a \nmid b$, the only common divisors can be ± 1.), ~~so we do as follows~~
So $\exists\, s, t \in \mathbb{Z} : sa + tb = 1$
which means $sac + tbc = c$
Now $a \mid sac$ obviously,
and $a \mid tbc$ (as $a \mid bc$)
so $a \mid sac + tbc = c$
ie $a \mid c$.

5.5 THE UNIQUE FACTORISATION THEOREM
(also called THE FUNDAMENTAL THEOREM OF ARITHMETIC)

Every non-zero element $a \in \mathbb{Z}$ is either a unit or can be expressed as the product of a unit and finitely many positive primes.

If $a = u p_1 p_2 p_3 \dots p_r = v q_1 q_2 \dots q_s$ where u, v are units and the p, q's the primes, then $u = v$, $r = s$ and the p_i's and q_i's can be paired off in such a manner that paired primes are equal.

PROOF: Lemma 5.3.9 (Every $a \in \mathbb{Z}$, $a > 1$ can be expressed as a product of finitely many positive primes) gives the proof of the first half (for $|a| > 1$)

Suppose there exists an integer a with decompositions as above but in which the p_i's and q_j's don't pair off.
If $a < 0$, then $|a|$ still retains this property.
Let S be the set of all such positive numbers (which we assume to be non-empty) which contains a smallest element, say (WLOG) $|a|$.

Now $|a| = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$

Also p_1 is prime, we deduce $p_1 \mid q_1 q_2 \cdots q_s$.
But the q's are irreducible so $p_1 \mid q_i$, some i

So we get $p_2 p_3 \cdots p_r = q_1 q_2 \cdots q_{i-1} q_{i+1} \cdots q_s < |a|$
But $|a|$ is the smallest elt of S, so the above does not lie in S. So it has a prime factorisation, and the $p_2, p_3, \ldots, p_r$ can be paired off with the $q_1, q_2, \ldots, q_{i-1}, q_{i+1}, \ldots, q_s$ Also $r-1 = s-1$, so $r = s$
Thus $|a|$ can be factored uniquely into primes, ie $|a| \notin S$
So S is empty.

5.6 POLYNOMIALS

5.6.1 DEFN (a) A polynomial with coefficients in S is simply an infinite sequence $(a_0, a_1, a_2, \ldots)$
in which $a_i \in S$, $i = 0, 1, 2, \ldots$
and $\exists N \in \mathbb{Z}$: $\forall n \in \mathbb{Z}, n > N \Rightarrow a_n = 0$
The set of all such polynomials is denoted $S[x]$

(b) Two polynomials $(a_0, a_1, a_2, \ldots)$ and $(b_0, b_1, \ldots, b_2)$ are <u>equal</u> iff $a_i = b_i$, all $i \in \mathbb{Z}^+ \cup \{0\}$

5.9 Divisibility, Irreducibility, & Primes in $\mathbb{Q}[x]$

5.9.1 Let $f, g \in \mathbb{Q}[x]$. Then f divides g $(f|g)$ iff $\exists\, h \in \mathbb{Q}[x]$ such that $g = fh$.

5.9.3 <u>Defns</u> (a) If $u \in \mathbb{Q}[x]$ and $u|1$ $(u \in \mathbb{Q})$ then u is a <u>unit</u>

(b) If $f \in \mathbb{Q}[x]$ is neither the zero polynomial nor a unit, then f is <u>irreducible</u> iff whenever f is expressed as a product $f = gh$ with $g, h \in \mathbb{Q}[x]$, then either g or h is a unit

(c) If $f \in \mathbb{Q}[x]$ is neither zero nor a unit, then f is <u>prime</u> iff whenever $f|gh$, some $g, h \in \mathbb{Q}[x]$, then $f|g$ or $f|h$ or both.

(d) If $f, g \in \mathbb{Q}[x]$ and $f = gu$, u a unit in $\mathbb{Q}[x]$, then f and g are <u>associates</u>.

5.9.5 <u>Defn</u>: A polynomial $F = z_0 + z_1 x + \cdots + z_n x^n \in \mathbb{Z}[x]$ is <u>primitive</u> iff $(z_0, z_1, \ldots, z_n) = 1$

5.9.8 <u>Lemma</u>: If $f \in \mathbb{Q}[x]$ then $\exists\, F \in \mathbb{Z}[x]$, F primitive such that $F = \alpha f$ is an associate of f, $\alpha \in \mathbb{Q}^+$

5.9.10 <u>Theorem</u> 1.9.10: If $F, G \in \mathbb{Z}[x]$ are both primitive, then so is FG

Examples

$4x+1 \mid x^2 - \frac{1}{12}x - \frac{1}{12}$ since $(4x+1)\cdot\frac{1}{4}\left(x-\frac{1}{3}\right) = x^2 - \frac{1}{12}x - \frac{1}{12}$

$x+2 \nmid x^3+2x^2-4x+12$

$10x^2+15x+6$ is primitive, $72x^3+2x^2-42x+8$ is not.

If $f = \frac{3}{5} - 9x + \frac{18}{7}x^2 - \frac{12}{11}x^3 = \frac{3}{385}\left[77 - 1155x + 330x^2 - 140x^3\right]$
then $F = 77 - 1155x + 330x^2 - 140x^3$ and $\alpha = \frac{3}{385}$, a unit in $\mathbb{Q}[x]$

* Is x^3+1 irreducible in $\mathbb{Z}_2[x]$?
Apparently so, but note $\hat{2} = \hat{0}$ in $\mathbb{Z}_2$, so
$x^3+\hat{1} = x^3+\hat{2}x^2+\hat{2}x+\hat{1} = (x^2+x+\hat{1})(x+\hat{1})$
so it is reducible.

PROOF: Let $FG = c_0 + c_1 x + \dots + c_{m+n} x^{m+n}$. If FG is not primitive then $c_0, c_1, \dots, c_{m+n}$ have a common divisor (other than 1 or -1) in $\mathbb{Z}$ and hence some common prime divisor p, say. Now p doesn't divide all the y's nor all the z's. Let s, t be the least integers such that $p \nmid y_s$ and $p \nmid z_t$.

Consider $c_{s+t} = y_0 z_{s+t} + y_1 z_{s+t-1} + \dots + y_s z_t + \dots + y_{s+t} z_0$.
Now $p \nmid y_s z_t$ as p is prime. But p does divide every other term in the above equality, including c_{s+t} itself – contradiction.

5.9.11 DEFN: Let $F = z_0 + z_1 x + \dots + z_n x^n \in \mathbb{Z}[x]$
The $\gcd(z_0, z_1, \dots, z_n)$ is called the content of F.

5.9.13 DEFN: Let $f = a_0 + a_1 x + \dots + a_n x^n$ where $a_n \neq 0$.
Then n is called the degree of f. We write $\deg f = n$.
(The zero polynomial has no degree)

5.9.14 THEOREM (Gauss): If $F \in \mathbb{Z}[x]$ and if we can write $F = gh$ where $g, h \in \mathbb{Q}[x]$, then we can write $F = GH$ where $G, H \in \mathbb{Z}[x]$, $\deg G = \deg g$ and $\deg H = \deg h$

PROOF: (i) We first suppose that F is primitive and write $g = \frac{a}{b} G$ and $h = \frac{c}{d} H$ where $a, b, c, d \in \mathbb{Z}^+$ are such that $(a, b) = (c, d) = 1$, where $G, H \in \mathbb{Z}[x]$ are primitive and where $\deg g = \deg G$ and $\deg h = \deg H$.
Thus $F = gh = \frac{ac}{bd} GH$. Hence $bdF = ac\,GH$ in $\mathbb{Z}[x]$

Examples

① The content of $-18x^2 + 45x - 30$ is $(-18, 45, 30) = 3$.

Now F and GH are both primitive polynomials and so the content of $bd\,F$ is bd, while the content of $ac\,GH$ is ac. Thus $ac = bd$ and $F = GH$ follows.

(ii) If F is not primitive, write $F = z F_1$ where z is the content of F and where F_1 is primitive. Then, from $F = gh$ we get $F_1 = \frac{g}{z} h$.

Hence, by (i), $F_1 = G_1 H_1$ and consequently $F = (zG_1) H_1$ where G_1, zG_1 and $H_1 \in \mathbb{Z}[x]$

5.9.15 COROLLARY If $F \in \mathbb{Z}[x]$ is reducible in $\mathbb{Q}[x]$ then it is already reducible in $\mathbb{Z}[x]$, otherwise it is prime (in $\mathbb{Z}[x]$). (Proof omitted)

5.9.16 THEOREM (EISENSTEIN'S TEST): Let $F = a_0 + a_1 x + \dots + a_n x^n \in \mathbb{Z}[x]$

If there exists a prime p in $\mathbb{Z}$ such that:

(i) $p \mid a_0$, $p \mid a_1$, $\dots$, $p \mid a_{n-1}$, $p \nmid a_n$

(ii) $p^2 \nmid a_0$

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

PROOF: Supposing F is reducible in $\mathbb{Q}[x]$, we may assume that $F = GH$, where $G = b_0 + b_1 x + \dots + b_r x^r \in \mathbb{Z}[x]$

and $H = c_0 + c_1 x + \dots + c_s x^s \in \mathbb{Z}[x]$

and where $r < n$, and $s < n$.

We have: $a_0 = b_0 c_0$

$a_1 = b_0 c_1 + b_1 c_0$ etc.

Since $p \mid a_0$ we know that $p \mid b_0$ or $p \mid c_0$, but not both ($p^2 \nmid a_0$)

Suppose WLOG that $p \mid b_0$ and $p \nmid c_0$. Now, not all the b_i are divisible by p or else all the a_i, would be (contrary to $p \nmid a_n$) Let k be the smallest suffix for which $p \nmid b_k$. Then $0 < k \leq r < n$.
Now $a_k = b_0 c_k + \dots + b_k c_0$ and $p \mid a_k$ since $k < n$.
Also, p divides all the terms $b_i c_{k-i}$ except the last [since $p \nmid b_k$, and $p \nmid c_0$] - contradiction.

5.9.18 THEOREM (UNIQUE FACTORISATION THEOREM FOR POLY'S)

Let f be a non-zero elt of $\mathbb{Q}[x]$. Then either f is a unit or f can be expressed as a product of a unit and finitely many monic* irreducible polynomials. Furthermore, this factorisation is unique.
(Proof in 6.7.13)

* MISSING: ROOTS & THE REMAINDER THEOREM
TEXT BOOK pp 51-55

* ie coeff of greatest power of x is $+1$.

Examples

① $f = \frac{1}{5} - 3x + \frac{6}{5}x^2 - x^3 + \frac{4}{5}x^4 + \frac{2}{15}x^5$ is irreducible in $\mathbb{Q}[x]$

$f = \frac{1}{15}\{3 - 45x + 18x^2 - 15x^3 + 12x^4 + 2x^5\}$

Note: $3 \mid 3$, $3 \mid 45$, ..., $3 \nmid 2$, and $3^2 \nmid 3$, by Eisenstein the inside polynomial is irreducible in $\mathbb{Z}[x]$. Consequently so is f in $\mathbb{Q}[x]$.

6 Introduction to Rings

We shall be interested in the following set of axioms, defined on a set S with binary operations $+$, $\cdot$ (i.e., on triples $\langle S, +, \cdot \rangle$).

6.2.1 **The Axioms**: For any three elts $a, b, c \in S$, distinct or not:

A1	$a+b=b+a$	M1 : $a.b=b.a$
A2	$(a+b)+c=a+(b+c)$	M2: $(a.b).c=a.(b.c)$
A3	$\exists z \in S$: $z+a=a+z=a$	M3 : $\exists e \in S : e.a=a.e=a$
A4	$\forall a \in S, \exists a^* \in S : a+a^*=a^*+a=z$	M4 : $\forall_{a \neq z} a \in S \; \exists a' \in S : a.a'=a'.a=e$

A1 - commutative A2 - associative D - distributivity
A3 - identity A4 - inverse Z - zero divisors

D $a.(b+c)=a.b+a.c$ and $(a+b).c=a.c+b.c$

Z If $a.b=z$ then $a=z$ or $b=z$ (or both).

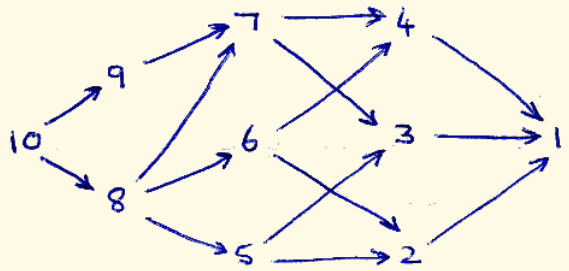
Any elt of S (including 0) for which there exists a non-zero elt of S such that $s.t=z$ or $t.s=z$ is a Zero Divisor

6.2.2 **Definitions** see opposite.

6.3 Ring Properties Deducible from the Axioms.

6.3.1 **Theorem**: Let $\langle R, +, \cdot \rangle$ be a ring. Then R contains exactly one elt satisfying A3 (existence of zero). Further, to each $a \in R$ there corresponds exactly one a' given by A4.

	If +, · satisfy: A1	A2	A3	A4	M2	D	M1	M3	M4	Z	$\langle S, +, \cdot \rangle$ Called a:
1	——		all		——						Ring
2			"				✓				Commutative Ring
3			"					✓			Ring with unity
4			"							✓	Ring with no zero divisors
5			"				✓	✓			Commutative ring with unity
6			"				✓			✓	" " with no ZD's
7			"					✓		✓	Ring with unity & no ZD's.
8			"				✓	✓		✓	INTEGRAL DOMAIN
9			"					✓	✓	✓	DIVISION RING (Skew field, S field, Non-commutative field)
10			"				✓	✓	✓	✓	FIELD



: Relationships

Eg.

1. $M_2(2\mathbb{Z})$
2. $\{\hat{0}, \hat{2}, \hat{4}, \hat{6}\}$ mod 8
3. $M_2(\mathbb{Z})$
4. All elts of $\mathbb{Q}[x]$ with zero constant term
5. $\mathbb{Z}_4$
6. $2\mathbb{Z}$
7. $\mathbb{Q}[x]$
8. $\mathbb{Z}$
9. $\mathbb{Q}$
10. $\mathbb{Q}$

where $M_2(\mathbb{C})$ is the set of all 2×2 matrices with coeffrents in $\mathbb{C}$

$\mathbb{Q} \subset M_2(\mathbb{C})$ - quaternions, ie, all 2×2 mats of form (with $s,t,u,v \in \mathbb{R}$)

$$\begin{pmatrix} s+it & u+iv \\ -u+iv & s-it \end{pmatrix}$$

PROOF: Suppose z and $z^* \in R$ both satisfy A3.
Then $z + z^* = z$ and $z + z^* = z^*$, hence $z = z^*$.

Say we have two inverses a^* and $a^{①}$ both satisfying A4.
Now $(a^{①} + a^*) + a^* = z + a^* = a^*$
and $a^{①} + (a + a^*) = a^{①} + z = a^{①}$
Hence $a^* = a^{①}$.

Similar results can be proved for M3 and M4.

6.3.2 THEOREM: Let $\langle R, +, . \rangle$ be a ring. Then, for any $a, b \in R$:

(i) $z . a = a . z = z$ (ii) $(a^*)^* = a$

(iii) $a^* . b = a . b^* = (a . b)^*$ (iv) $a^* . b^* = a . b$

If R has a unity elt e then:

(v) $e^* . b = b . e^* = b^*$ (vi) $e^* . e^* = e$.

(Proofs omitted - page 93). NOTE From now on we use $0, 1, -a, a^{-1}$ instead of z, e, a^*, a'.

6.3.4 THEOREM Every finite integral domain J is a field.

PROOF: (We need only show that M4 is satisfied).
Let the elts of J be labelled $a_0 (=0), a_1 (=1), a_2, \ldots, a_n$
Select any a_i other than a_0. Consider the list
$a_0 a_i, a_1 a_i, \ldots a_n a_i$ of elts, all in J.
Suppose, for suffices j, k (where $0 < j \leq k \leq n$) we have
$a_j a_i = a_k a_i$. Since J is a domain, it follows that $a_j = a_k$. This means that the list comprises $n+1$ distinct elts of J, that is, all of J. Since $1 \in J$ there is an l such that $a_l a_i = 1$.
But then $a_i a_l = a_l a_i = 1$, and a_i has a multiplicative inverse in J.

6.3.5 NOTE: A much deeper result is that every finite division ring is a field.

(96)

6.4 SUBRINGS, SUBFIELDS & IDEALS

6.4.1 DEFN: Let $\langle R, +, \cdot \rangle$ be a ring and suppose that S is a non-empty subset of R. We say that S is a subring of R iff (i) S is closed under $+, \cdot$.
(ii) $\langle S, +, \cdot \rangle$ is a ring.

6.4.2 THEOREM: Let S be a non-empty subset of a ring R. Then S is a subring of R iff:
(i) if $a, b \in S$ then $a+b \in S$ and $a.b \in S$.
(ii) if $a \in S$ then $-a \in S$

6.4.3 LEMMA: Let S be a subring of R. Letting 0_S and 0_R denote the zero elts of the rings $\langle S, +, \cdot \rangle$ and $\langle R, +, \cdot \rangle$ we have $0_S = 0_R$. Further, if $a \in S$ then $(-a)_S = (-a)_R$.

PROOF OF 6.4.3: Let $s \in S$. In S we have $s + 0_S = s$.
In R we have $s + 0_R = s$. Hence in R we have $s + 0_S = s + 0_R$.
Hence $0_S = 0_R$.
In S, $a + (-a)_S = 0_S$; in R, $a + (-a)_R = 0_R$
Hence, in R, $a + (-a)_S = 0_S = 0_R = a + (-a)_R$
$\Rightarrow (-a)_S = (-a)_R$.

PROOF OF 6.4.2: $\overset{\text{only if}}{\Rightarrow}$: Since S is a subring of R, $\langle S, +, \cdot \rangle$ is a ring
Hence for $a, b \in S$ we have $a+b \in S$, $a.b \in S$ and $(-a) \in S$
But $(-a)_S = (-a)_R = -a$.
$\overset{\text{if}}{\Leftarrow}$: (i) implies S is closed under $+, \cdot$.
Since $S \neq \phi$, $\exists\, s \in S$
By (ii), $(-s)_R \in S$. By (i) $0_R = s + (-s)_R \in S$
Clearly 0_R is the elt reqd by axiom A3 to be in S

Examples

1. Q is a subring of $\langle M_2(\mathbb{C}), \oplus, \odot \rangle$ (Q defined in pg 41 exc). For given $x, y \in Q$, it is easily seen that $x \oplus y$, $x \odot y$ and $\ominus x$ are also in Q.

2. On $2\mathbb{Z}$ define $+$ as usual, but $\odot$ by: $a \odot b = 0$, all $a, b \in 2\mathbb{Z}$. Then $\langle 2\mathbb{Z}, +, \odot \rangle$ is a ring, but it is not a subring of $\langle \mathbb{Z}, +, \cdot \rangle$ since $a \odot b \neq a$ all $a, b \in 2\mathbb{Z}$.

3. $S = \{\hat{0}, \hat{2}, \hat{4}, \hat{6}\}$ is a subring of $\mathbb{Z}_8$. Note that $1_{\mathbb{Z}_8} = \hat{1}$, whereas $1_S = \hat{6}$

4. In the ring $\langle F, \oplus, \odot \rangle$ all all functions from $\mathbb{R}$ to $\mathbb{R}$ the subset of all differentiable (respectively continuous) functions forms a subring, essentially because the sum and product of differentiable (continuous) functions is differentiable (continuous).

Also, for each $a \in S$, $(-a)_R \in S$ by (ii)
Clearly, $(-a)_R$ is the elt reqd by A4 to be in S.
Finally, each of A1, A2, M2 and D holds for all elts of R.
hence, in particular, all elts of S.
(Thus we have shown that $+, \cdot$ are binary operations on S and that $\langle S, +, \cdot \rangle$ is a ring.

6.4.5 THEOREM: Let S_1, S_2 be subrings of the ring R. Then the set theoretic intersection $S_1 \cap S_2$ is also a subring of R.

PROOF: Since $0_{S_1} = 0_{S_2} = 0_R$, $S_1 \cap S_2 \neq \phi$
Now suppose $x, y \in S_1 \cap S_2$.
Then $x, y \in S_1$, and $x+y$, $x \cdot y$ and $-x$ all lie in S_1
Similarly, $x+y$, $x \cdot y$ and $-x$ all lie in S_2.
So they lie in $S_1 \cap S_2 \Rightarrow$ subring of R.

There are important analogues of 6.4.1, 6.4.2 and 6.4.5 for fields, these being:

6.4.1.F DEFN: A subfield of a field F is any non-empty subset T of F such that:
(i) T is closed with respect to the binary operations $+, \cdot$ defined on F
(ii) $\langle T, +, \cdot \rangle$ is a field.

6.4.2.F THEOREM: Let T be a non-empty subset of a field F.
Then T is a subfield iff:
(i) if $a, b \in T$ then $a+b \in T$ and $a \cdot b \in T$
(ii) If $a \in T$ then $-a \in T$ and if $a \neq 0$ then $a^{-1} \in T$.

6.4.5.F THEOREM: Let $\{T_\alpha : \alpha \in A\}$ be a set of subfields of the field F.
Then $\bigcap_{\alpha \in A} T_\alpha$ is also a subfield of F

In particular, the intersection P of the sets of all subfields of F is a subfield (clearly the unique, smallest one in F) called the prime subfield of F.

6.4.6 DEFN: Let I be a non-empty subset of a ring R. Then I is called an ideal of R iff
(i) if $a, b \in I$ then $a + b \in I$
(ii) if $a \in I$ then $-a \in I$
(iii) if $a \in I$ and $r \in R$ then ra and $ar \in I$

(43) Clearly, each ideal is a subring (in (iii) r can be any elt of I)
Note that $a.r$ and $r.a$ may well be unequal – we demand that both belong to I.

6.10 ISOMORPHISMS, FIELDS OF FRACTIONS & PRIME SUBFIELDS.

6.10.1 DEFN: Let $\langle R, +, \cdot \rangle$ and $\langle S, \oplus, \odot \rangle$ be rings. We say that R and S are isomorphic iff there is a one-one map $\psi : R \to S$ such that, for all $r_1, r_2 \in R$:
(i) $(r_1 + r_2)\psi = r_1\psi \oplus r_2\psi$
(ii) $(r_1 . r_2)\psi = r_1\psi \odot r_2\psi$
We write this $R \cong S$; ψ is called an isomorphism.

6.10.3 THEOREM: Let D be an integral domain. Then there exists a field F_D containing a subring D^* isomorphic to D and such that every elt of F_D is of the form uv^{-1} where $u, v \in D^*$ (and $v \neq 0$). (Proof omitted - pg 128/9)

6.10.4 NOTES If $D = \mathbb{Z}$ then $F_D = \mathbb{Q}$. In fact, the proof of 6.10.3 is modelled on our understanding of how $\mathbb{Q}$ is obtained from $\mathbb{Z}$. Intuitively, elts of $\mathbb{Q}$ are of the form

Examples.

① Let $s \in \mathbb{Z}$. Then $\{sz : z \in \mathbb{Z}\}$ is an ideal of $\mathbb{Z}$.
In fact every ideal – indeed every subring – of $\mathbb{Z}$ has this form, for suitable s.

② Let $f \in \mathbb{Q}[x]$. Then $\{fm : m \in \mathbb{Q}[x]\}$ is an ideal of $\mathbb{Q}[x]$.
In fact every ideal, but not every subring of $\mathbb{Q}[x]$ has this form.

③ In any ring R the subsets $\{0_R\}$ and R are ideals. If F is a field then $\{0\}$ and F are its only ideals.

④ Let R be any ring and let $a_1, a_2, \ldots, a_n \in R$. Then the set of all elts of the form $z_1a_1 + \ldots + z_na_n + s_1a_1 + \ldots + s_na_n + a_1t_1 + \ldots + a_nt_n + u_1a_1$

$\frac{r}{s}$ where $r, s \in \mathbb{Z}$ and $s \neq 0$. Of course, $\frac{r_1}{s_1} = \frac{r_2}{s_2}$ is possible even though $r_1 \neq r_2$ and $s_1 \neq s_2$. But then $r_1 s_2 = s_1 r_2$. Thus a rational number $\frac{r}{s}$ is really a representative of all those $\frac{r_1}{s_1}$ for which $r s_1 = s r_1$.

In fact, we set F_D = set of all equivalence classes on $D \times D$ where the equivalence relation $\sim$ is defined by $(a,b) \sim (c,d) \Leftrightarrow ad = bc$ in D.

and define: $\{a,b\} \oplus \{c,d\} = \{a.d + b.c,\ b.d\}$

$\{a,b\} \odot \{c,d\} = \{a.c,\ b.d\}$

We must show $\oplus$ and $\odot$ are well-defined, and that $\langle F_D, \oplus, \odot \rangle$ is a field.

Then $D^* = \{\{d,1\} : d \in D\}$ can be shown to be a subring of F_D and the map $\theta : D \to D^*$ is an isomorphism, thus $D \cong D^*$

Finally, given $\{a,b\} \in F_D$ we have $\{a,b\} = \{a,1\} \odot \{1,b\}$

$= \{a,1\} \odot \{b,1\}^{-1}$

with both $\{a,1\}$ and $\{b,1\} \in D^*$ as required.

F_D is called the <u>field of fractions</u>, or <u>quotient field</u> of the integral domain D. Note that isomorphic integral domains have isomorphic quotient fields. Note that there are non-commutative domains which cannot be embedded in division rings, so D must be commutative.

6.10.7 <u>NOTATION</u>: Given fields $F \subseteq E$, and elts $\alpha, \beta, \gamma, \ldots \in E$ it is customary to denote the smallest subfield of E which contains $F, \alpha, \beta, \gamma, \ldots$ by $F(\alpha, \beta, \gamma, \ldots)$. In this notation the fields of fraction of $\mathbb{Q}[x]$, $\mathbb{Q}[x,y]$, $\mathbb{Z}[\sqrt{2}]$ $\mathbb{Z}[\sqrt[3]{2}]$ are $\mathbb{Q}(x)$, $\mathbb{Q}(x,y)$, $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt[3]{2})$ while the smallest subfield of $\mathbb{C}$ containing, for example $\mathbb{Q}$, $\sqrt{2}$ and i is denoted by $\mathbb{Q}(\sqrt{2}, i)$

Examples.

① Let $N_2(\mathbb{R})$ be the ring of all matrices of the form $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ where $a, b \in \mathbb{R}$. Then $\psi : \mathbb{C} \to N_2(\mathbb{R})$ given by:
$(x+iy)\psi = \begin{pmatrix} x & y \\ -y & x \end{pmatrix}$ is an isomorphism between $\mathbb{C}$ and $N_2(\mathbb{R})$. In particular, $N_2(\mathbb{R})$ is a field.

② The map θ from the ring $\mathbb{Z}_6$ to the direct sum $\mathbb{Z}_2 \oplus \mathbb{Z}_3$ given by $\hat{m}_6\theta = (\hat{m}_2, \hat{m}_3)$ is isomorphic

* ③ The group of all isomorphisms of a system with itself (ie automorphisms) exhibits an internal symmetry of the system.

For any ring R the identity map is an automorphism.
The fields $\mathbb{Q}$ and $\mathbb{R}$ possess no other automorphisms, while $\mathbb{C}$ has at least one other $(a+ib)\xi = a - ib$.
The map of $\mathbb{Q}[x_1, x_2, x_3, x_4, \ldots]$ to itself in which each occurrence of x_1, x_2, x_3, x_4 is replaced by, say, x_2, x_4, x_1, x_3 respectively, is an automorphism.

* ④ If T is a subring of ring S and if $\theta : R \to T$ is an isomorphism we say that θ is an embedding of R in S.
R need not be contained in S, but T is and $R \cong T$.

⑤ The fields of fractions of $\mathbb{Q}[x]$, $\mathbb{Q}[x,y]$ and $\mathbb{Z}[\sqrt{2}]$ are: $\left\{ \frac{u}{v} : u, v \in \mathbb{Q}[x], v \neq 0 \right\}$

$\left\{ \frac{u}{v} : u, v \in \mathbb{Q}[x,y], v \neq 0 \right\}$

and $\left\{ \frac{u}{v} : u, v \in \mathbb{Z}[\sqrt{2}], v \neq 0 \right\}$ respectively

6.10.9 **THEOREM**: Let F be any field and $p(F)$ the intersection of all subfields of F. Then $p(F)$, the prime subfield of F, is isomorphic to $\mathbb{Q}$ or to one of the finite fields $\mathbb{Z}_p$.

7. Factor Rings & Fields.

7.2.3 **Defn:** Let $\langle R, +, \cdot\rangle$ and $\langle S, \oplus, \odot\rangle$ be rings and $\theta : R \to S$ a map. θ is called a homomorphism from the ring $\langle R, +, \cdot\rangle$ (in)to the ring $\langle S, \oplus, \odot\rangle$ iff, for all $a, b \in R$

(i) $(a+b)\theta = a\theta \oplus b\theta$

(ii) $(a \cdot b)\theta = a\theta \odot b\theta$

Remarks:
- An isomorphism is thus a special case of a homomorphism, one in which the map is 1-1. However, we cannot say "R and S are homomorphic" as homomorphisms, unlike isomorphisms, are not 'symmetric'.
- The subset $R\theta = \{r\theta : r \in R\}$ of S is called the (homomorphic) image of R under θ. $R\theta$ is easily shown to be a subring of S.

7.2.6 **Theorem:** Let $\theta : \langle R, +, \cdot\rangle \to \langle S, \oplus, \odot\rangle$ be a ring hom. Then (i) $O_R\theta = O_S$ (ii) for each $a \in R$, $(-a)\theta = \ominus(a\theta)$

Proof (i) $O_R = O_R + O_R \Rightarrow O_R\theta = (O_R + O_R)\theta = O_R\theta \oplus O_R\theta$ in S

$\Rightarrow O_R = O_S$

(ii) $O_S = O_R\theta = (a + (-a))\theta = a\theta \oplus (-a)\theta$ in S.

$\Rightarrow (-a)\theta = \ominus(a\theta)$

7.2.7 **Theorem:** Let $\theta : \langle R, +, \cdot\rangle \to \langle S, \oplus, \odot\rangle$ be a ring hom. Then the subset $K = \{k \in R : k\theta = O_S\}$ is an ideal of R, called the kernel of θ, written $\ker\theta$

Proof: Let $k_1, k_2 \in K$. Then $(k_1 - k_2)\theta = k_1\theta \ominus k_2\theta = O_S \ominus O_S = O_S$

Thus $k_1 - k_2 \in K$. Let $k \in K$, $r \in R$. Then $(k \cdot r)\theta = k\theta \odot r\theta = O_S \odot r\theta = O_S$

Thus $k \cdot r \in K$. In a similar manner, $r \cdot k \in K$, $\Rightarrow K$ is an ideal.

Examples

① The map $\theta : \mathbb{Z} \to \mathbb{Z}_n$ given by $n\theta = \hat{n}$ defines a homo. from $\langle \mathbb{Z}, +, \cdot \rangle$ onto $\langle \mathbb{Z}_n, \oplus, \odot \rangle$. The only homomorph from $\langle \mathbb{Z}_n, \oplus, \odot \rangle$ to $\langle \mathbb{Z}, +, \cdot \rangle$ is the <u>trivial homomorphism</u>, that is, the map $\psi : \mathbb{Z}_n \to \mathbb{Z}$ given by $\hat{z}\psi = 0$.

② The map $\theta : \mathbb{Z}_8 \to \mathbb{Z}_3$ given by $\hat{m}_{,8}\theta = \hat{m}_3$ defines a homomorphism from $\langle \mathbb{Z}_{18}, \oplus, \odot \rangle$ onto $\langle \mathbb{Z}_3, \oplus, \odot \rangle$.

③ $\theta : \mathbb{Z} \to \mathbb{Z}$, $z\theta = 2z$ is no a ring homomorph from $\langle \mathbb{Z}, +, \cdot \rangle$

④ The maps $\theta, \psi : \mathbb{Q}[x] \to \mathbb{Q}$ defined by $(a_0 + a_1 x + \dots + a_n x^n)\theta = a_0$ and $(a_0 + \dots + a_n x^n)\psi = a_0 + a_1 + \dots + a_n$ are homomorphisms.

⑤ The map $\theta : \mathbb{Q}[x] \to \mathbb{R}$ given by $(a_0 + a_1 x + \dots + a_n x^n)\theta = a_0 + a_1\sqrt{2} + \dots + a_n(\sqrt{2})^n$ is a homo. of $\langle \mathbb{Q}[x], +, \cdot \rangle$ onto $\langle \mathbb{Q}[\sqrt{2}], +, \cdot \rangle$

⑥ The map $\theta : \mathbb{Z} \to \mathbb{Q}$ given by $z\theta = \binom{z}{1}$ is a homomorph. of $\langle \mathbb{Z}, +, \cdot \rangle$ onto $\langle \mathbb{Q}, +, \cdot \rangle$ (isomorphism)

⑦ The map $\theta : \mathbb{Q}[x,y] \to \mathbb{C}$ given by $(\sum a_{jk} x^j y^k)\theta = \sum a_{jk}(1+i)^j(\sqrt{3}\sqrt{2})^k$ is a homomorphism.

Kernels

① The ideal $[n] = \{kn, k \in \mathbb{Z}\}$. The whole ring $\mathbb{Z}_n$

② The ideal $\{\hat{0}, \hat{3}, \hat{6}, \hat{9}, \hat{12}, \hat{15}\}$ in $\mathbb{Z}_{18}$

④ The ideal $[x] = \{xf : f \in \mathbb{Q}[x]\}$ in $\mathbb{Q}[x]$, and the ideal comprising all f in $\mathbb{Q}[x]$ whose coefficients have sum zero, ie $\{(x-1)f : f \in \mathbb{Q}[x]\} = [x-1]$

⑤ The ideal $[x^2 - 2]$ in $\mathbb{Q}[x]$

⑥ The subset $\{0\}$

⑦ The least ideal of $\mathbb{Q}[x,y]$ containing (ie generated by) the polynomials $x^2 - 2x + 2$ and $y^3 - 2$

7.2.11 **THEOREM**: Let $\langle R, +, \cdot \rangle$ be a ring and I an ideal of R. Then there exists a ring $\langle S, \oplus, \odot \rangle$ and a homomorph. $\Theta : R \xrightarrow{\text{onto}} S$ such that $\ker \Theta = I$ exactly.

Thus we need to: (i) construct S (ii) define Θ (iii) check $\ker \Theta = I$. We first construct S.

7.2.12 **NOTATION**: Let $\langle R, +, \cdot \rangle$ be a ring, I an ideal and r_0 an elt of R. We denote the subset $\{r_0 + i : i \in I\}$ of R by $r_0 + I$

7.2.13 **NOTES**: It is quite possible for $r_0 \neq r_1$ in R, but $r_0 + I = r_1 + I$. In fact, $r_0 + I = r_1 + I \Leftrightarrow r_1 - r_0 \in I$. As an example, let I be the ideal $\{5k ; k \in \mathbb{Z}\}$ in the ring $\langle \mathbb{Z}, +, \cdot \rangle$. Then $3 + I = \{3 + 5k : k \in \mathbb{Z}\} = \{8 + 5k : k \in \mathbb{Z}\} = 8 + I$ and $8 \neq 3$, $8 - 3 \in I$. $0 + I$, $1 + I$, ..., $4 + I$ are just new names for the elts $\hat{0}, \hat{1}, \hat{2}, \hat{3}, \hat{4}$ of $\mathbb{Z}_5$. In fact the following construction of S from R is merely a generalisation of our construction of $\mathbb{Z}_n$ from $\mathbb{Z}$ using the notation $r + I$ instead of $\hat{r}$. In particular, replacing R and I by $\mathbb{Z}$ and $\{5k\}_{k \in \mathbb{Z}}$ in 7.2.14, 7.2.16 & 7.2.19 will retrieve familiar results about $\mathbb{Z}_5$.

7.2.14 **LEMMA**: Let $r_1, r_2 \in R$. Then either $r_1 + I = r_2 + I$ or else $(r_1 + I) \cap (r_2 + I) = \Phi$,

PROOF: Suppose that $(r_1 + I) \cap (r_2 + I) \neq \Phi$. Then there is an elt t in both $r_1 + I$ and $r_2 + I$. By defn, this means $t = r_1 + i_1$ and $t = r_2 + i_2$ for suitable i_1, i_2 in I. But then $r_1 = r_2 + i_2 - i_1$ and hence, for each $i \in I$, $r_1 + i = r_2 + i_2 - i_1 + i$. Since $i_2, i_1, i \in I$ we see that $r_1 + i \in r_2 + I$. It follows that $r_1 + I \subseteq r_2 + I$, and similarly vice-versa. Thus $r_1 + I = r_2 + I$

7.2.15 NOTES: ① $r_1 + I$ is called the coset of I in R determined by r_1

② The cosets of I in R form a partition of R (since each $r \in R$ is an elt of $r+I$, and these complete cover R in a non-overlapping manner.)

③ We denote the set of all distinct cosets of I in R by R/I, the factor ring (quotient ring) of R by I

7.2.16 THEOREM: Let $\langle R, +, \cdot \rangle$ be a ring, I an ideal of R. Then R/I can be made into a ring.

PROOF: Let $a+I, b+I \in R/I$. Define:

$$(a+I) \oplus (b+I) = (a+b) + I$$
$$(a+I) \odot (b+I) = (a.b) + I$$

Then $\langle R/I, \oplus, \odot \rangle$ is a ring.

7.2.19 LEMMA: Let $\langle R, +, \cdot \rangle$, I and $\langle R/I, \oplus, \odot \rangle$ be as above. The mapping $\theta: R \to R/I$ given by $r\theta = r+I$ is a homomorphism from R onto R/I, and $\ker \theta = I$.

7.4 CONSTRUCTIONS OF $\mathbb{R}$ FROM $\mathbb{Q}$ AND $\mathbb{C}$ FROM $\mathbb{R}$.

See Allenby pp 156 - 161.

CANTOR: $\mathbb{R} = \{$equivalence classes of Cauchy convergent series$\}$

DEDEKIND: $\mathbb{R} = \{$all upper sections of $\mathbb{Q}\}$

THEOREM: Any complete ordered field is isomorphic to $\mathbb{R}$.

GAUSS/HAMILTON: $\mathbb{C} = \{(a,b) : a, b \in \mathbb{R}\}$ with defns of $=, +, \cdot$

CAUCHY: $\mathbb{C}$ is the factor ring $\dfrac{\mathbb{R}[x]}{[x^2+1]}$

(eg $2x^4 + 3x^3 + 3x^2 - x + 4 \equiv -4x + 3 \bmod x^2+1$, which Cauchy wrote as: $2i^4 + 3i^3 + 3i^2 - i + 4 = -4i + 3$)

Examples.

① If $R = \mathbb{Q}[x]$ and $I = [x^2 - 2]$ then every elt of R/I can be written in the form $a + bx + I$, where $a, b \in \mathbb{Q}$.
Further, $\langle R/I, \oplus, \odot \rangle$ is isomorphic to the field of all real numbers of the form $a + b\sqrt{2}$ where $a, b \in \mathbb{Q}$.

8 Basic Group Theory.

8.3.1 **Defn**: A group is an (ordered) pair $\langle G, \circ \rangle$ where G is a non-empty set and $\circ$ is a binary operation on G satisfying the following axioms:

A: Associativity : $\forall a,b,c \in G,\ (a \circ b) \circ c = a \circ (b \circ c)$
N: Identity $\exists e \in G : \forall a \in G,\ e \circ a = a \circ e = a$
I: Inverse $\forall a \in G,\ \exists a^{-1} \in G : a \circ a^{-1} = a^{-1} \circ a = e$.

Note: G is closed under $\circ$.

8.3.2 **Defn**: If for all x, y in G we have $x \circ y = y \circ x$ the group G is called commutative or abelian.

8.3.5 **Defn**: Let X be any non-empty set. A permutation on X is a function $f: X \to X$ which is 1-1 and onto.

Remarks (see example 6): When X is a finite set with n elts, $P(X)$ is often denoted by S_n, called the symmetric group on n symbols since S_n leaves fixed each of the n (formal) elementary symmetric polynomials on the elts of X. Clearly S_n contains exactly $n!$ elts.

8.3.6 **Notation**: Cauchy suggested the notation (for example) of $f = \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}$, $g = \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix}$. Then, $f \circ g = \begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix}$ and $f^{-1} = \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}$.

8.3.7 **Defn**: The number of elts in the group $\langle G, \circ \rangle$ is denoted $|G|$, called the order of G.
(see examples pp 190-2)

Examples.

① $\langle \mathbb{Z}, + \rangle$ is an abelian group.

② $\langle \mathbb{R}, + \rangle$ and $\langle \mathbb{R}^+, \cdot \rangle$ are abelian groups.

③ Let $\langle R, +, \cdot \rangle$ be a ring and $\langle F, +, \cdot \rangle$ be a field. Then $\langle R, + \rangle$, $\langle F, + \rangle$ and $\langle F^\times, \cdot \rangle$ are all abelian groups where $F^\times = \{ f \in F : f \neq 0 \}$.

④ $\langle \mathbb{Z}^+, - \rangle$ is not a group. Neither are:

⑤ $\langle \mathbb{Z}, - \rangle$, $\langle \mathbb{Z}^+, + \rangle$, $\langle \mathbb{Z}^+, \cdot \rangle$

⑤ Let $n \in \mathbb{Z}^+$ and let $M(n)$ denote the set of all equivalence classes mod n of integers coprime to n. Then $\langle M(n), \cdot \odot \rangle$ is an (finite) abelian group with $\phi(n)$ elts.

⑥ If $P(X)$ denotes the set of all permutations on X then $\langle P(X), \circ \rangle$ is a group, where $\circ$ represents the composition of functions which is associative. The identity function $I : X \to X$ given by $I(x) = x$ acts as the identity elt of $P(X)$ and, given $f \in P(X)$ the function f^{-1} acts as an inverse to f. (If $\#X = n$, then order $P(X)$ is $n!$)

⑦ Let C_n denote the set $\left\{ \cos \frac{2\pi k}{n} + i \sin \frac{2\pi k}{n} : k = 0, 1, \ldots, n-1 \right\}$ of the n complex n^{th} roots of 1. With respect to multiplication, C_n forms a group of order n.

8.4 Deductions from the Axioms.

8.4.1 **Theorem** (cf 6.3.1) *In any group G there is exactly one identity element. Further, to each $a \in G$ there corresponds exactly one inverse.*

Proof: • Axiom N assures us of the existence of at least one identity elt e. Let e, f be identity elts. Then $e.f = f.e = e$ and $e.f = f.e = f \Rightarrow e = f$.

• Axiom I assures us that to each $a \in G$ there corresponds at least one inverse a^{-1}. Let b be another. Then $(a^{-1}.a)b = eb = b$ and $(a^{-1})(ab) = a^{-1}$ gives $b = a^{-1}$.

8.4.2 **Theorem** (cf 6.3.2(i)): *For any group G and any $a \in G$, $(a^{-1})^{-1} = a$.*

Proof: We know $a.a^{-1} = a^{-1}.a = e$. Thus a is an inverse (unique) of a^{-1}, i.e. $a = (a^{-1})^{-1}$.

8.4.3 **Theorem**: *If $a, b, c \in G$ satisfy $ab = ac$, then $b = c$*

Proof: From $ab = bc$ we deduce $a^{-1}(ab) = a^{-1}(ac)$ thus $eb = ec \Rightarrow b = c$.

8.4.4 **Theorem**: *Let $a, b \in G$. Then $(ab)^{-1} = b^{-1}a^{-1}$.*

Proof: $(ab).(b^{-1}.a^{-1}) = (a(b.b^{-1}))a^{-1} = a.a^{-1} = e$
Similarly $(b^{-1}.a^{-1})(a.b) = b^{-1}(a.a^{-1})b = b^{-1}b = e$.

Examples

① Let $A = \begin{pmatrix} 3 & 2 \\ 1 & \frac{1}{2} \end{pmatrix}$ $B = \begin{pmatrix} -2 & 1 \\ 3 & -5 \end{pmatrix}$ then $A, B \in GL_2(\mathbb{Q})$

$$A^{-1} = \begin{pmatrix} -1 & 4 \\ 2 & -6 \end{pmatrix} \quad B^{-1} = \begin{pmatrix} -\frac{5}{7} & -\frac{1}{7} \\ -\frac{3}{7} & -\frac{2}{7} \end{pmatrix}$$

$$(AB)^{-1} = \begin{pmatrix} 0 & -7 \\ -\frac{1}{2} & -\frac{3}{2} \end{pmatrix}^{-1} = \begin{pmatrix} \frac{3}{7} & -2 \\ -\frac{1}{7} & 0 \end{pmatrix} = B^{-1} \cdot A^{-1}$$

whereas $A^{-1} \cdot B^{-1} = \begin{pmatrix} -1 & -1 \\ \frac{8}{7} & \frac{10}{7} \end{pmatrix}$

8.5 Symmetric & Alternating Groups.

8.5.1 **Defn:** Let f be a permutation on the set $X = \{1, 2, \ldots, n\}$ and let $x_1, x_2, \ldots, x_r$ $(1 \leq r \leq n)$ be distinct elements of X. If for $1 \leq i < r$ we have $x_i f = x_{i+1}$, if $x_r f = x_1$ and if $yf = y$ for every other elt of X, then f is called a <u>cyclic permutation</u> or <u>cycle</u> and is denoted briefly by $(x_1, x_2, \ldots, x_r)$. r is called the <u>length</u> of the cycle.

Next, let f be any permutation on X and let $\alpha \in X$ be arbitrary. Writing f^k for the composition of f with itself k times $(k > 0)$ in $\langle S_n, \circ \rangle$, (where S_n is the set of all permutations of a finite set with n elts), consider the subset: $A = \{\alpha, \alpha f, \alpha f^2, \ldots, \alpha f^n\}$ of X. As there are only n elts in X, not all of the $n+1$ elts of A can be distinct - suppose αf^j is the first elt to be repeated (ie $\min_j$). Thus $\exists i \in \mathbb{Z} : 0 \leq i < j$ and $\alpha f^i = \alpha f^j$. Applying the permutation f^{-i} to this we find $(\alpha f^i) f^{-i} = \alpha (f^j) f^{-i}$, ie $\alpha = \alpha f^{j-i}$. By the minimality of j we see that $i = 0$. Thus A consists of the set of distinct elts $\alpha, \alpha f, \ldots, \alpha f^{j-1}$

8.5.2 **Defn:** The set A described above is called the <u>orbit</u> of f on X determined by α.

Now suppose $A \subset X$. Then $\exists \beta \in X : \beta \notin A$. So we can find the orbit of f on X determined by β, say B. Then $A \cap B = \phi$. Continuing to obtain orbits in this fashion until X is exhausted, we can put this in a theorem if we first make:

8.53 **Defn:** To each orbit A define the function f_A by:

$$x f_A = xf \text{ if } x \in A$$
$$x f_A = x \text{ if } x \notin A$$

8.5.4 THEOREM Let f be a permutation on the finite set X and let $A, B, \ldots, T$ be the finitely many pairwise disjoint orbits of f on X. Then each of $f_A, f_B, \ldots, f_T$ is a cyclic permutation and f is equal to their product, taken in any order, ie f is expressible as a product of disjoint cycles. (see example ①)

8.5.6 NOTATION: It is usual to omit cyclic permutations involving only one element. Commas too are often omitted. Thus f from ex ① could be written $f = (1\ 7\ 3\ 13)(2\ 10\ 9)(6\ 12)(8\ 15)$

8.5.7 DEFN: If the permutation f on the set X is a cycle which interchanges just two elts of X leaving all the others fixed then f is a transposition.

8.5.8 THEOREM: Every cyclic permutation (and hence every permutation) can be expressed as a product of transpositions.

PROOF: One only has to see that $(x_1 x_2).(x_1 x_3)\ldots(x_1 x_n) = (x_1, x_2, \ldots, x_n)$ (see ex ②)

8.5.9 THEOREM: Let the permutation f on the set $X = \{1, 2, \ldots, n\}$ be expressible in some way as an even (respectively odd) number of transpositions. Then every way of expressing f as a product of transpositions requires an even (odd) number of transpositions.

PROOF: Consider, in $\mathbb{Z}[x_1, \ldots, x_n]$ the polynomial $P = \prod_{1 \le i < j \le n} (x_i - x_j)$

$$P = \prod_{1 \le i < j \le n} (x_i - x_j) = (x_1 - x_2)(x_1 - x_3)\ldots(x_1 - x_n)$$
$$(x_2 - x_3)\ldots(x_2 - x_n)$$
$$\vdots$$
$$(x_{n-1} - x_n)$$

Examples

① $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 7 & 10 & 13 & 4 & 5 & 12 & 3 & 15 & 2 & 9 & 11 & 6 & 1 & 14 & 8 \end{pmatrix}$

has orbits $\{1,7,3,13\}$ $\{2,10,9\}$ $\{4\}$ $\{5\}$ $\{6,12\}$ $\{8,15\}$ $\{11\}$ $\{14\}$

and we can write (omitting $\circ$):

$$f = (1,7,3,13)(2,10,9)(4)(5)(6,12)(8,15)(11)(14)$$

Apart from the order of the $(\,)$ groups, and the shifting of order within these (eg $(2,10,9) = (10,9,2)$), f is clearly unique.

② $(1,2,3,4,5) = \underset{f_\alpha}{(1,2)}\underset{f_\beta}{(1,3)}\underset{f_\Omega}{(1,4)}\underset{f_\delta}{(1,5)}$, because:

$f_\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$ $f_\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 4 & 5 \end{pmatrix}$ $f_\Omega = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 3 & 1 & 5 \end{pmatrix}$

$f_\delta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 3 & 4 & 1 \end{pmatrix}$

So $f_\alpha \cdot f_\beta \cdot f_\Omega \cdot f_\delta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \\ 2 & 3 & 4 & 1 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}_{\alpha\ \beta\ \Omega\ \delta} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} = (1,2,3,4,5)$

Note that this is not unique, as for eg $(1\,2\,3\,4\,5) = (2\,4)(4\,5)(3\,5)(1\,2)(1\,4)(4\,5)$

Check

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \\ 1 & 5 & 3 & 2 & 4 \\ 1 & 3 & 5 & 2 & 4 \\ 2 & 3 & 5 & 1 & 4 \\ 2 & 3 & 5 & 4 & 1 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} \begin{matrix} \\ 2 \leftrightarrow 4 \\ 4 \leftrightarrow 5 \\ 3 \leftrightarrow 5 \\ 1 \leftrightarrow 2 \\ 1 \leftrightarrow 4 \\ 4 \leftrightarrow 5 \end{matrix}$$

Now each transposition (i,j), say, in $P(X)$ gives rise to a mapping (indeed, an automorphism) of $\mathbb{Z}[x_1, x_2, \ldots, x_n]$ onto itself, namely that determined by interchanging x_i and x_j and leaving the remaining x's fixed. Such a mapping changes P to $-P$. Likewise, each permutation f of $P(X)$ gives rise to a mapping of $\mathbb{Z}[x_1, x_2, \ldots, x_n]$ onto itself and similarly maps P either to P or $-P$. Clearly if f can be expressed as the product of an even number of transpositions, f maps P to P, and not to $-P$, so f cannot be expressed as the product of an odd number of transpositions (and vice-versa).

8.5.10 DEFINITION: Let f be a permutation on the finite set X. f is an even (odd) permutation iff f can be expressed as an even (odd) number of transpositions.

Since the product of two even permutations is clearly even, since the identity permutation is even, and since the inverse of an even permutation is even, we have:

8.5.11 THEOREM: Let $X = \{1, 2, \ldots, n\}$. The set of all even permutations on X forms a group under composition of functions. This group, called the alternating group on n symbols, is denoted by A_X or A_n and has $\frac{n!}{2}$ elts.

PROOF: All we have left to prove is $|A_X| = \frac{n!}{2}$. Every permutation on X is either even or odd. Let $p_1, p_2, \ldots, p_r$ be the set of even perms, $q_1, q_2, \ldots, q_s$ the odd perms. The permutations $(1,2)p_i$ are all odd and pairwise unequal, and there are r of them, so $r \leq s$. Similarly the perms $(1,2)q_i$ are all even etc, and there are s of them, so $s \leq r$. Thus $s = r$, and we have the result from $s + r = n!$

8.6 SUBGROUPS & THE ORDER OF AN ELEMENT.

8.6.1 DEFN: A non-empty subset S of the group $\langle G, \circ \rangle$ is a subgroup of G iff (a) the restriction $\bar{\circ}$ of $\circ$ to $S \times S$ is a binary operation on S, and (b) $\langle S, \bar{\circ} \rangle$ is a group.

If S is a subgroup of G we write $S \leq G$ (or $S \neq G$, $S < G$)
We can write $\circ$ for $\bar{\circ}$ and just say (a) S is closed under $\circ$.
See examples.
In example (4) we may have $x^r = x^s$ for some $r, s \in \mathbb{Z}$, $r > s$.
In this case $x^{r-s} = x^r \cdot x^{-s} = x^s \cdot x^{-s} = e$. This leads to:

8.6.3 DEFN: Let G be a group and let $a \in G$. If there exists a positive integer m such that $a^m = e$ then the smallest such positive integer is the order of a. If no such m exists a is said to be of infinite order.

8.6.5 THEOREM: Let $\langle G, \circ \rangle$ be a group and S a non-empty subset of G. Then $S \leq G$ iff for all $a, b \in S$ we have both:
(i) $a \circ b \in S$ (ii) $a^{-1} \in S$

PROOF: If S is a subgroup of G, then $a \circ b \in S$ since S closed under $\circ$. Since S is a group it has identity elt $\bar{e}$ satisfying $\bar{e} \circ \bar{e} = \bar{e}$. It follows that $\bar{e} = e$, the identity elt of $\langle G, \circ \rangle$
a^{-1} is the unique inverse of a with respect to e in G.
Since S is a group, it follows that a has a unique inverse $\bar{a}$ with respect to $\bar{e}$ $(= e)$ in S. It follows that $a^{-1} = \bar{a} \in S$.

Conversely, let S be a non-empty subset of G such that (i) & (ii) hold. From (i) S is closed under $\circ$.
If $a, b, c \in S$ then $a, b, c \in G$ and so $a \circ (b \circ c) = (a \circ b) \circ c$ follows.
Given $a \in S$ we know $a^{-1} \in S$ (by (ii)) and then $e = a \cdot a^{-1} \in S$ by (i).

Examples

① $S_4 = \{$ permutations on $X = \{1,2,3,4\}\}$ Thus S_4 comprises the $4! = 24$ elts $\begin{pmatrix} 1 & 2 & 3 & 4 \\ a & b & c & d \end{pmatrix}$. The subset $V = \{I, (12), (34), (12)(34)\} < S_4$ with respect to composition of permutations.
The subsets $U = \{s : s \in S_4 \wedge d = 4\}$ of order $3!$ and $W = \{s : s \in S_4 \wedge \{b,c\} = \{2,3\}\}$ of order $2!$ are subgroups of S_4.
A_4 is a subgroup of S_4 of order $\frac{4!}{2} = 12$.

② In the group $M = GL_n(\mathbb{C})$ (invertible (non-singular) $n \times n$ matrices of $\mathbb{C}$) the subset S of all those $n \times n$ matrices with determinant ± 1 and the subset T of all matrices with determinant 1 are subgroups, and T is a subgroup of S. (In fact a subgroup of a subgroup of G is a subgroup of G (any group G))

③ Let $\langle G, \circ \rangle$ be a group. The subsets G and $\{e\}$ are two (extreme) subgroups of G. $\{e\}$ is called the trivial subgroup, any subgroup $S \neq \{e\}$ is a non-trivial subgroup of G, and any subgroup S other than G is called a proper subgroup of G.

④ Let $\langle G, \circ \rangle$ be a group, $x \in G$. Let $C = \{x^k : k \in \mathbb{Z}\}$. Then $C < G$, called the cyclic subgroup of G generated by x.

⑤ In $\langle \mathbb{C}^*, \cdot \rangle$ ($\{$non-zero elts of $\mathbb{C}\}$), -1 has order 2, i has order 4, and de Moivre's Theorem (rg 51 ex ⊕) tells us that $\cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$ has order n. 2 has infinite order.

⑥ In $GL_2(\mathbb{Z})$, $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $\begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ have orders $4, 6$ & ∞ respectively

⑦ 5 has ∞ order in $\langle \mathbb{Z}, + \rangle$; $\hat{5}$ has order 2 in $\langle \mathbb{Z}_{10}, \oplus \rangle$ and order 11 in $\langle \mathbb{Z}_{11}, \oplus \rangle$

⑧ In a finite group every elt has finite order.

⑨ The order of $(1\ 3\ 2\ 6\ 7)(4,5)$ in S_7 is 10.

Then, trivially, $e \circ s = s \circ e = s$ for all $s \in S$, so $e \in S$ and acts as identity elt.

Finally, given $a \in S$ there exists (by (iii)) an elt (namely a^{-1}) in S which is such that $a \circ a^{-1} = a^{-1} \circ a = e$.

Thus $\langle S, \circ \rangle$ is a group, and $S \leq G$.

8.6.8 DEFN: (i) Let $a, b \in G$ be such that $ab = ba$. We say a and b commute

(ii) Let $Z(G) = \{x \in G : xg = gx \ \forall g \in G\}$. $Z(G)$ is called the centre of G.

8.6.9 THEOREM: $Z(G)$ is an abelian subgroup of G.

PROOF: Clearly $e \in Z(G)$ so $Z(G)$ is not empty. Let $a, b \in Z(G)$ and let $g \in G$. It follows that $(ab)g = a(bg) = a(gb) = (ag)b = (ga)b = g(ab)$, so $ab \in Z(G)$. Also $a^{-1}(ag)a^{-1} = a^{-1}(ga)a^{-1}$, that is, $ga^{-1} = a^{-1}g$, thus $a^{-1} \in Z(G)$. So $Z(G)$ is a subgroup of G. Finally $Z(G)$ is abelian. For, let a, b be any two elements of $Z(G)$. Then $ag = ga$ for all $g \in G$; in particular when $g = b$.

Any group whose centre is no bigger than the trivial subgroup is called a group with trivial centre or even a group with no centre.

8.6.11 DEFN: Let G be a group and let $U = \{a, b, c, \ldots\}$ be a non-empty (possibly ∞) set of elts of G. We denote by $\langle U \rangle$ or $\langle a, b, c \ldots \rangle$ the set (actually subgroup) of all elts g of G which can be expressed as a product $g = x_{i_1}^{\varepsilon_1} x_{i_2}^{\varepsilon_2} \ldots x_{i_r}^{\varepsilon_r}$ where $r \in \mathbb{Z}^+$, where each $x_i \in U$ and each $\varepsilon_i \in \{-1, 1\}$. We call $\langle U \rangle$ the subgroup of G generated by $a, b, c, \ldots$ (or by U) and $\{a, b, c \ldots\}$ a set of generators for $\langle U \rangle$. If $\langle U \rangle = G$ then $\{a, b, c \ldots\}$ is a

Examples.

① If A is an abelian group then $A = Z(A)$.

② $Z(S_3) = \{e\}$. The inequality $(12)(123) \neq (123)(12)$ shows that neither (12) nor (123) is central in S_3. Other elts can be dealt with similarly.

set of generators for G. If U is finite and $G = \langle U \rangle$ then G is called a finitely generated group.

Every subgroup S of G (including G) has a set of generators. In general G will have many different sets of generators.

8.6.12 THEOREM: $\langle U \rangle$ is a subgroup of G.

PROOF: Since U is non-empty certainly $\langle U \rangle$ is not empty.
Suppose $u_1 = x_{i_1}^{\varepsilon_1} \dots x_{i_r}^{\varepsilon_r}$ and $u_2 = y_{j_1}^{n_1} \dots y_{j_s}^{n_s} \in \langle U \rangle$. Then,
$u_1 u_2 = x_{i_1}^{\varepsilon_1} \dots x_{i_r}^{\varepsilon_r} y_{j_1}^{n_1} \dots y_{j_s}^{n_s} \in U$ and $u_1^{-1} = x_{i_r}^{-\varepsilon_r} \dots x_{i_1}^{-\varepsilon_1} \in U$.

8.6.13 THEOREM: Let $\{S_\lambda : \lambda \in \Lambda\}$ be the set of all subgroups of G which contain the subset U. Then $\langle U \rangle = \bigcap_{\lambda \in \Lambda} S_\lambda$

PROOF: By 8.6.6 (Omitted), $\bigcap_{\lambda \in \Lambda} S_\lambda$ is a subgroup of G.
Rest of proof left as exercise.

Note: We see that 'the cyclic subgroup generated by x' of pg 56 ex ⑥ has, according to 8.6.11, a generating set comprising just $\{x\}$. Thus 8.6.11 generalises the notion of generator for a cyclic (sub) group.

Examples

① $\langle \mathbb{Z}, + \rangle$ has, amongst infinitely many others, the generating sets $\{1\}$, $\{-1\}$, $\{2, 3\}$, $\{1, 2, 3, 4\}$. The first two are the only one-generator subsets; the third has two elts, neither of which is redundant.

② $\langle \mathbb{Q}^+, \cdot \rangle$ has as one of its generating sets, the set of all (positive) primes. $\langle \mathbb{Q}^+, \cdot \rangle$ has no finite generating sets.

8.7 Cosets of Subgroups & Lagrange's Theorem.

8.7.1 **Defn:** Let $H \leq G$ and let g be a fixed elt of G. We denote by gH the subset $\{gh : h \in H\}$ of G and call this the left coset of H in G determined by g. Similarly we can define the right coset.

8.7.3 **Lemma:** Let $H \leq G$ and let $g \in G$. The mapping τ from H to gH defined by $h\tau = gh$ is a 1-1 map of H onto gH.

Proof: Clearly τ is a mapping. Next, if $h_1\tau = h_2\tau$ then $gh_1 = gh_2$ so $h_1 = h_2$. Thus τ is 1-1.
Let $x \in gH$. Then $x \in gh^*$, some $h^* \in H$. Then $h^*\tau = gh^*$ so τ is onto.

8.7.4 **Lemma:** Let $H \leq G$ and let $g_1, g_2 \in G$. Then either $g_1H = g_2H$ or $g_1H \cap g_2H = \phi$.

Proof: Suppose $g_1H \cap g_2H$ is not empty and contains an elt c. Then $c \in g_1H$ so $c = g_1h^*$ some $h^* \in H$. Then $cH = \{ch : h \in H\} = \{g_1h^*h : h \in H\} = \{g_1\bar{h} : \bar{h} \in H\} = g_1H$. Similarly, since $c \in g_2H$ we deduce $cH = g_2H$. Thus $g_1H = cH = g_2H$.

Note: as $g = ge \in gH$, every elt of G lies in some left coset of H in G, so G is the union of a number of left cosets of H. From 8.7.3, 8.7.4 we see that distinct cosets are mutually disjoint and contain the same number $|H|$ of elts. Thus if G is a finite group and if G is the union of r distinct left cosets of H in G we see that $|G| = r|H|$. An identical argument for right cosets shows that if G is the union of s distinct right cosets of H in G then $|G| = s|H|$. It follows that $r = s$. This leads to:

Examples

① The group S_3 contains the subset $H = \{I, (12)\}$ as a subgroup. There are three distinct left cosets of H in S_3, namely $H = IH = (12)H$;

$$(23)H = (123)H$$
$$(13)H = (132)H$$

and three distinct right cosets:

$$H = HI = H(12)$$
$$H(23) = H(132)$$
$$H(13) = H(123)$$

② In our construction of factor rings we had occasion to consider subsets of the form $a + I = \{a + i : i \in I\}$ where I is an ideal in a ring R and a is a fixed elt of R. Note that in this case $a + I = I + a$ since the group $\langle R, + \rangle$ is abelian.

③ Let $\mathbb{R}^3$ denote the set of all triples (x, y, z) of real numbers. Then $\mathbb{R}^3$ forms a group under $\oplus$ if $\oplus$ is defined by $(x_1, y_1, z_1) \oplus (x_2, y_2, z_2) = (x_1 + x_2, y_1 + y_2, z_1 + z_2)$. If we consider the subset $H = \{(x, y, z) : 2\pi x + 7y - \frac{5}{3}z = 0\}$ one soon sees that H is a subgroup of G. In geometrical terms H is a plane through the origin in 3-dimensional space. The coset $\left(3, 5e, \frac{1}{4\sqrt{2}}\right) \oplus H$ is, in geometrical terms, the plane K passing through the point $\left(3, 5e, \frac{1}{4\sqrt{2}}\right)$ and parallel to H in $\mathbb{R}^3$.

8.7.5 DEFN: Let $H \leq G$ with $|G|$ finite. The number of right (left) cosets of H in G is called the index of H in G, denoted $|G:H|$

LAGRANGE'S THEOREM: Let $H \leq G$, G a finite group. Then $|G| = |G:H| \cdot |H|$. (i.e. the order of a subgroup divides the order of a group)

8.8 Cyclic Groups.

Since every group contains, along with each of its elts x, the whole of the cyclic subgroup generated by x, we see that:

(i) every group is built up from (⋃ of) its cyclic subgroups

(ii) the simplest possible types of groups are those which comprise the distinct powers of some one elt (the cyclic groups)

The prototype amongst cyclic groups of order n is the multiplicative group of the n complex n^{th} roots of 1. In the case of infinite cyclic groups, the prototype is $\langle \mathbb{Z}, + \rangle$.

We know that for each $n \in \mathbb{Z}^+$ there exists at least one cyclic group of order n (the prototype). We illustrate the power of Lagrange's Theorem by showing that, if n is a prime, then all groups of order n are cyclic.

8.8.1 Theorem: Any group of prime order is cyclic

Proof: Let G be a finite group of prime order, and select x $(x \neq e)$ in G. Now x generates a cyclic subgroup H, say. By Lagrange's Theorem $|H| \,||\, |G| = p \Rightarrow |H| = 1$ or $|H| = p$. The former is impossible since H contains e and x. Thus $|H| = p$, and hence $H = G$, so G is cyclic.

8.8.2 Theorem: (i) Each subgroup S of a finite cyclic group G is a (finite) cyclic group whose index in G divides $|G|$. Further, given any $j \in \mathbb{Z}^+$ such that $j \mid |G|$ there exists exactly one subgroup of G with index j

(ii) Each subgroup $S \neq \{e\}$ of an infinite cyclic group G is an infinite cyclic group of finite index in G. Further, given any $j \in \mathbb{Z}^+$ there exists exactly one subgroup of G with index j

8.9 Isomorphisms & Group Tables, Cayley's Theorem

8.9.1 **Defn** (i) Let $\langle G, \circ\rangle$ and $\langle H, *\rangle$ be groups. A 1-1 mapping $\psi: G \to H$ from the set G onto the set H is an *isomorphism* iff, for all $a, b \in G$ we have

$$(a \circ b)\psi = (a)\psi * (b)\psi.$$

(ii) If $\langle G, \circ\rangle$, $\langle H, *\rangle$ are groups such that at least one isomorphism can be found between them, then G and H are *isomorphic*, $G \cong H$

8.9.6 **Theorem (Cayley's)**: Let $\langle G, *\rangle$ be any group. Then $\langle G, *\rangle$ is isomorphic to a group of permutations on the set G.

Proof: To each elt $a \in G$, define a map $\rho_a: G \to G$ by $g\rho_a = g * a$ for all $g \in G$. Clearly ρ_a is a map from G to G. Further, ρ_a is a permutation on the set G (given any $h \in G$, note $(h * a^{-1})\rho_a = h$ so ρ_a is clearly onto G; further, from $g_1\rho_a = g_2\rho_a \Rightarrow g_1 * a = g_2 * a \Rightarrow g_1 = g_2$ so ρ_a is 1-1).

The subset $S = \{\rho_a : a \in G\}$ is a subgroup of the group of all permutations on the set G. For, given $\rho_a, \rho_b \in S$, for all $g \in G$, $g(\rho_a \circ \rho_b) = (g\rho_a)\rho_b = (g * a)\rho_b = (g * a) * b = g * (a * b)$. Thus $\rho_a \circ \rho_b = \rho_{a*b}$. Similarly we find that $(\rho_a)^{-1} = \rho_{a^{-1}} \in S$. Thus $\langle S, \circ\rangle$ is a group.

Finally we claim that the mapping $\theta: G \to S$ given by $a\theta = \rho_a$ establishes the isomorphism of G and S. Briefly:

(i) θ is clearly onto

(ii) θ is 1-1 (for if $a\theta = b\theta$ then $\rho_a = \rho_b$, and $e\rho_a = e\rho_b$ i.e. $a = b$)

(iii) Given $a, b \in G$, $(a * b)\theta = \rho_{a*b} = \rho_a \circ \rho_b = (a\theta) \circ (b\theta)$.

Examples

① $\theta : \langle \mathbb{Z}, + \rangle \to \langle 2\mathbb{Z}, + \rangle$ where $z\theta = 2z$ is an isomorphism.

② In the groups S_n of all permutations of $[n]$ the subgroup comprising all permutations fixing '1' is a subgroup isomorphic to S_{n-1}

③ The group of 8 symmetries of a square is isomorphic to the subgroup of S_4 generated by $(12)(34)$ and (1234) but not to the subgroup of S_6 generated by (12), (34) and $(5,6)$, the latter being abelian.

④ The group of matrices generated by $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ w.r.t. multiplication is a group of order 8, not isomorphic to the group of symmetries of a square in ③. This is the group of quaternions.

⑤ $\langle \mathbb{Q}^+, \cdot \rangle \cong \langle \mathbb{Z}[x], + \rangle$. For $r = 2^{\alpha_0} 3^{\alpha_1} 5^{\alpha_2} \dots p_{s+1}^{\alpha_s} \in \mathbb{Q}$ define $r\theta = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \dots + \alpha_s x^s$. θ is an isomorphism.

⑥ $\langle \mathbb{Z}, + \rangle \not\cong \langle \mathbb{Q}, + \rangle$ since the equation $nx = a$ $(n \in \mathbb{Z})$ is always soluble in $\mathbb{Q}$ but not always in $\mathbb{Z}$.
$\langle \mathbb{Q}, + \rangle \not\cong \langle \mathbb{R}, + \rangle$ since there is no 1-1 map between $\mathbb{Q}$ & $\mathbb{R}$.

⑦ $\langle \mathbb{Z}_6, \oplus \rangle \cong \langle M(7), \odot \rangle$ (see ⑤ pg 51). The maps $\hat{n}\theta = \hat{3}^n$ and $\hat{n}\psi = \hat{4}^n$ both establish this. The map $\hat{n}\sigma = \hat{2}^n$ does not (why not?)