Indian Institute of Technology, Bombay

Summer of Science '21

Report

Abstract Algebra

Siddhant Midha

Mentored by
Manav Batavia

July 2021

Contents

1 Preliminaries

A **Set** is a collection of distinct objects. Two sets are equal if and only if they have precisely the same elements. Further, a set a denoted by the notation $\{\dots\}$, with the elements listed inside the curly braces. For example, the set of Natural Numbers is denoted as $\mathbb{N} = \{1, 2, 3 \dots\}$.

Let A and B be two sets. We now define some more notation:

- If an element a is in the set A, we denote it as $a \in A$. Else, we write $a \notin A$.
- The number of elements in the set A is known as the *Cardinality* of A, denoted as $|A|$.
- The *Cartesian Product* of sets A and B is defined as
$$A \times B = \{(a, b) \mid a \in A \text{ and } b \in B\}$$
- A *Relation* from A to B is a subset R of $A \times B$. If $(a, b) \in R$, then we say, a is related to b, which is denoted as $a \sim b$ (or in some cases, as $a \approx b$).
- The *Union* of the two sets, is defined as
$$A \cup B = \{p \mid p \in A \textit{ or } p \in B\}$$
- The *Intersection* of the two sets, is defined as
$$A \cup B = \{p \mid p \in A \textit{ and } p \in B\}$$
- A set A is a *subset* of another set B if all elements of set A are elements of set B. We write this as $A \subseteq B$.
- Further we say that A is a *proper subset* of B if $\exists\, b \in$ B such that $b \notin A$. This is denoted as $A \subset B$.
- The Set which has *no* elements is denoted as $\emptyset$.
- An *Equivalence Relation* on A is a subset of $A \times A$ which is:
    1. *transitive*: If $a \sim b$ and $b \sim c$ then $a \sim c$.
    2. *symmetric*: If $a \sim b$ then $b \sim a$.
    3. *reflexive*: $a \sim a \,\forall\, a \in A$.
- Some common sets:
    - □ The set of all natural numbers, denoted as $\mathbb{N}$.
    - □ The set of all integers, denoted as $\mathbb{Z}$
    - □ The set of all rational numbers, denoted as $\mathbb{Q}$
    - □ The set of all Real numbers, denoted as $\mathbb{R}$
    - □ The set of all Complex Numbers, denoted as $\mathbb{C}$

A **Law of Composition** on a set S is any way to combine two elements of S, say p and q, and result in another element of the set, say r. Formally, a Law of Composition is a map, from the Cartesian product of a set with itself to itself, that is

$$S \times S \to S$$

The combination of p and $q \in S$ is denoted by $p.q$ in the multiplicative notation, or $p + q$ in the additive notation. For convenience, the '.' is usually dropped, and a combination of p and q in the multiplicative notation is simply written as pq.

A Law of Composition on the Set S is

Associative If $(a.b).c = a.(b.c)\ \forall\ a, b, c\ \in S$

Commutative If $a.b = b.a\ \forall\ a, b\ \in S$

Let us take an example. Let S be the set $\{a, b\}$. We can define four maps from $S \times S$ to S, namely,

- The *Identity* map, defined as $i(a) = a$ and $i(b) = b$.
- The *Transposition* map, defined as $\tau(a) = b$ and $\tau(b) = a$.
- The constant map, defined as $\alpha(a) = a$ and $\alpha(b) = a$.
- The constant map, defined as $\beta(a) = b$ and $\beta(b) = b$.

The laws of composition on this set can be shown in a Multiplication Table as follows.

Map	i	τ	α	β
i	i	τ	α	β
τ	τ	i	β	α
α	α	α	α	α
β	β	β	β	β

Where, each entry in the 4×4 table is a map formed by the map on the far left composed with the map on the far up, directions with reference to the aforementioned entry.

An *Identity* for a law of composition is an element $e \in S$ such that $ea = ae = e$, $\forall\ a\ \in S$. There can be at most one identity (why?). The identity element is often denoted by 1.
An element $a \in S$ is *invertible* if there is another element b such that, $ab = ba = 1$, and if so, then b is called the inverse of a, usually denoted by a^{-1}. Some properties of inverses:

- If an element a has both a left inverse l and a right inverse r, then $l = r$, a and r are invertible, and $r = a^{-1}$.
- If a is invertible, then its inverse is unique.
- If a and b are invertible, then so is the product ab, and $(ab)^{-1} = b^{-1}a{-}1$.
- An element may have a left inverse or a right inverse, thought it is not invertible.

Now, with some preliminaries out of the way, we start with groups.

2 Group Theory

2.1 Why?

Ever held a Rubik's cube in your hand?

Think about how many possible orientations, which we will call "states", of the said cube can exist? If I talk about legal moves, ergo, moves which do not mess with the pieces of the cube, this would be about $43,252,003,274,489,856,000$ possible states.

As it turns out, it has been *proven* that any one of these messy states of the cube can be reduced to the solved one, by at most 20 moves.

Well how? Let us first talk about these m. Let us index each move by $i \in \{1, 2, 3 \ldots\}$ Now, this defines a set S consisting of all these actions. Further we denote the notion of applying one move after the other with a '.', that is, $i.j$ denotes application of the move j followed by application of the move i. Now, as it turns out, the set S satisfies certain curious properties, namely,

- Two moves one after the other is another move, that is,

$$i, j \in S \Rightarrow i.j \in S \; (\mathit{Closure}) \tag{1}$$

- The sequence of moves $(i.j).k$ applied to the initial state, results in a state exactly same as the sequence of the moves $i.(j.k)$ applied to the same initial state. $(\mathit{Associativity})$
- The action of doing nothing belongs to the set, usually denoted by 1.(*Existence of Identity*)
- For every move applied to the initial state, there exists an 'inverse' which when applied to the new state reverts it back to the original state, that is, the composition of the moves results in the action of doing nothing.(*Existence of Inverse*)

Now this special set, forms something known as a *Group*.

In the discussion above, one may notice, that the words "actions" and "moves" have been used somewhat interchangeably. We shall see a precise formulation on this is section 3, and for now, develop the requisite theory for the same.

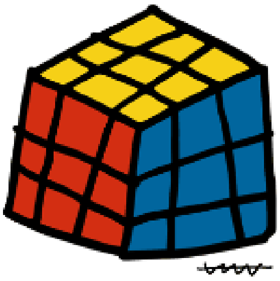

Image Source

2.2 Groups and Subgroups

A *Group* $(G, .)$ is a set G together with a law of composition, that has the following properties:

- The law of composition is associative: $(ab)c = a(bc) \ \forall \ a, b, c \ \in G$.
- G contains an identity element - denoted by 1, such that $1a = a$ and $a1 = a \ \forall \ a \ \in G$
- Every element a of G has an inverse, an element $b \in G$ such that $ab = 1$ and $ba = 1$.

An *Abelian Group* is a group whose law of composition is commutative.

The *order* of a group G is the number of elements that it contains, and is denoted by $|G|$.

The *order* of an *element* x of the group, is the least positive integer n such that $x^n = 1$ (power denoting repeated composition).

Some examples:

- The group of all invertible $n \times n$ matrices is called the *General Linear Group*, denoted by GL_n, where the law of composition is matrix multiplication.(Verify that this is a group!)
- The group of permutations of the set of indices $\{\boldsymbol{1}, \boldsymbol{2} \ldots \boldsymbol{n}\}$ is called the *Symmetric Group* and is denoted by S_n.
- Some common Abelian Groups:
  - □ The additive group of integers - $\mathbb{Z}^+$: The set of integers, with addition as its law of composition.
  - □ The additive group of Real numbers - $\mathbb{R}^+$: The set of real numbers with addition as its law of composition.
  - □ The multiplicative real group - $\mathbb{R}^\times$: The set of non zero real numbers with multiplication as the law of composition.
  - □ Analogous groups over complex numbers - $\mathbb{C}^+$ and $\mathbb{C}^x$.

Proposition 2.2.1 (Cancellation Law)**.** *Let a, b, c be elements of a group G. If $ab = ac$ or if $ba = ca$, then $b = c$.*

Proof. Follows from the invertibility axiom.

A subset H of a group G is a *subgroup* if it has the following properties:

- *Closure:* If a and $b \in H$, then $ab \in H$.
- *Existence of Identity*: $1 \in H$.
- *Existence of Inverse*: If $a \in H$, then $a^{-1} \in H$

(Why is associativity not part of these points?)

An example: Let a be an integer different from 0. We denote the subset of $\mathbb{Z}^+$ that consists of all multiples of a by $\mathbb{Z}a$:

$$\mathbb{Z}a = \{n \in \mathbb{Z} \mid n = ka, k \in \mathbb{Z}\} \tag{2}$$

This is a subgroup of $\mathbb{Z}^+$ (verify!).

Let us now state a theorem, which has an unexpected application.

Theorem 2.2.2. Let S be a subgroup of $\mathbb{Z}^+$. Either S is the trivial subgroup 0 or else it has the form $\mathbb{Z}a$, where a is the smallest positive integer in S.

Proof. If S is the trivial subgroup $\{0\}$, we are done. Let us now assume that S is not trivial. Hence, S contains an element other than zero, let this be q. If $q \in S$ then by associativity $0 - q$ is in S. Hence S has atleast one positive integer. Then let a be the smallest positive integer in S. Since S is a group, then by associativity, S contains all integers of the form na for any integer n. Hence, $a\mathbb{Z} \subset S$. Now we shall prove that $S \subset a\mathbb{Z}$.
Let $b = ka + r \in S$ where k is some integer and $r \in \{1, 2 \dots a\}$. Since S is a group, again by associativity, $ka \in S$, and further, $b - ka \in S$, that is $r \in S$. But since a is the smallest positive integer in S, r has to be zero. Thus, $S \subset a\mathbb{Z}$. Hence, we conclude, $S = \mathbb{Z}a$.

Hence, we conclude, $S = \mathbb{Z}a$.

Now let us look at an application of this theorem. Let S be a subgroup of $\mathbb{Z}^+$ defined as:

$$S = \mathbb{Z}a + \mathbb{Z}b = \{n \in \mathbb{Z} \mid n = ra + sb \, \text{for some integers } r, s\} \tag{3}$$

Let us assume a and b aren't both zero. Theorem 2.2.2 tells us that this subgroup has the form $\mathbb{Z}d$ for some positive integer d, which is nothing but the *greatest common divisor*(the *GCD*) a and b.

Proposition 2.2.3. Let a and b be integers, not both zero, and let d be their GCD, the positive integer that generates the subgroup $S = \mathbb{Z}a + \mathbb{Z}b$, that is $\mathbb{Z}d = \mathbb{Z}a + \mathbb{Z}b$, then:

- d divides a and b.
- If an integer e divides both a and b, it also divides d.
- There are integers r and s such that $d = ra + sb$.

Proof: Since $d \in S$, hence the third part is true. Since a and $b \in \mathbb{Z}d$, so d divides a and b. Further, if an integer e divides both a and b, then e divides the integer combination $ra + sb = d$.

Corollary 2.2.4. A pair a, b of integers is relatively prime if and only if there are integers r, s such that $ra + sb = 1$.

Corollary 2.2.5. Let p be a prime integer. If p divides a product ab of integers, then p divides a or p divides b.

Proof: Suppose that p divides ab but does not divide a. The only positive divisors of p are 1 and p. Hence, $\gcd(a, p) = 1$. Thus by Corollary 2.2.4, there exist integers r and s such that $ra + sp = 1$. Multiplying by b, $rab + spb = b$. Since p divides the LHS, it divides the RHS. Hence p divides b.

Let us now talk about another subgroup of $\mathbb{Z}^+$, defined as

$$S = \mathbb{Z}a \cap \mathbb{Z}b = \{n \in \mathbb{Z} \mid n = ak_2 \text{ and } n = bk_2; k_1, k_2 \in \mathbb{Z}\} \tag{4}$$

By Theorem 2.2.2 this subgroup is of the form $\mathbb{Z}m$ for some integer m, which is none other than the *least common multiple* (the *LCM*) of a and b.

Proposition 2.2.6. *Let a and b be integers different from zero, and let m be their least common multiple - the positive integer that generates the subgroup $\mathbb{Z}a \cap \mathbb{Z}b$, that is $\mathbb{Z}m = \mathbb{Z}a \cap \mathbb{Z}b$. Then,*

- *m is divisible by both a and b.*
- *If an integer n is divisible by a and by b, then it is divisible by m.*

Proof: Both statements follow from the fact that an integer is divisible by a and by b if and only if it is contained in $\mathbb{X}a \cap \mathbb{Z}b$.

Corollary 2.2.7. *Let $d = \gcd(a, b)$ and $m = \operatorname{lcm}(a, b)$. Then, $ab = dm$.*

Proof: Since b/d is an integer, a divides ab/d and similarly b divides ab/d. Hence, by Proposition 2.2.6, m divides ab/d, that is, dm divides ab.
Further, by Proposition 2.2.3, we know, there exist integers r, s such that $d = ar + bs$. Multiplying by m gives, $dm = amr + bms$. Since ab divides the RHS, it divides the LHS, that is ab divides dm. Since ab and dm are positive integers which divide one another, they are equal.

2.3 Cyclic Groups

A *Cyclic Group* is a group all of whose elements are the ”powers” (repeated composition) of some element belonging to the group. The cyclic group G generated by the element x is denoted as $G = \langle x \rangle$. For example, $\{1, -1\}$ is a cyclic group, in fact a cyclic subgroup of $\mathbb{R}^{\times}$.

Proposition 2.3.1. *Let $\langle x \rangle$ be the cyclic subgroup of a group G generated by the element x, and let S denote the set of integers k such that $x^k = 1$.*

- *The set S is a subgroup of $\mathbb{Z}^+$.*
- *$x^r = x^s$ if and only if $x^{r-s} = 1$, that is, if and only if $r - s \in S$.*
- *Suppose that S is not the trivial subgroup. Then by Theorem 2.2.1, $S = \mathbb{Z}n$ for some positive integer n.*

Proof: The first part follows from the group axioms on $\langle x \rangle$ and the definition of S. Second follows from the Cancellation Law. For the third part - If S is not trivial, by Theorem 2.2.1 $S = \mathbb{Z}n$ for some $n \in \mathbb{Z}$. Let x^a be an arbitrary power of x. We divide a by n and write $a = kn + r$, for some $k \in \mathbb{Z}$ and $r \in \{0, 1 \dots n-1\}$. Thus $x^a = x^{kn}x^r = x^r$. Thus, $x^a \in \{1, x, x^2 \dots x^{n-1}\}$. These powers are distinct, because x^n is the smallest power of x equal to 1.

Now we can give another definition of the order of x: An element x of a group has order n if the cyclic subgroup $\langle x \rangle$ generated by x has order n. When x has infinite order, the group $\langle x \rangle$ is said to be *infinite cyclic*.

Proposition 2.3.2. Let x be an element of finite order n in a group, and let k be an integer that is written as $k = nq + r$, where q and $r \in \mathbb{Z}$ and r is in the range $0 \leq r < n$.

- $x^k = x^r$.
- $x^k = 1$ if and only if $r = 0$.
- Let d be $gcd(k, n)$. The order of x^k is equal to $\frac{n}{d}$.

Proof: The proof is clear from the properties of group elements and the definition of order.

We can also talk about a subgroup of a group G which is generated by a subset U of G. That is, this is the smallest subgroup of G such that it contains U and consists of elements which can be expressed as products of a string of elements of U and their inverses. Let us take the example of the *Pauli Group* (on one *qubit*) from physics. Let us define some matrices first,

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{5}$$

Let G be the group, defined as,

$$G = \{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\} \tag{6}$$

We can see that this is the group *generated* by X, Y, Z. That is, $G = \langle X, Y, Z\rangle$.

2.4 Homomorphims

Let G and P be two groups, written with multiplicative notation. A *Homomorphism* $\varphi : G \to G'$ is a map from G to G' such that, $\forall a$ and $b \in G$

$$\varphi(a, b) = \varphi(a)\varphi(b) \tag{7}$$

Some examples:

1. The exponential map $e^{(\ )} : \mathbb{R}^+ \to \mathbb{R}^x$ defined by $x \rightsquigarrow e^x$,
2. The absolute value map $|\ | : \mathbb{C}^\times \to \mathbb{R}^\times$,
3. The determinant function det( ):$GL_n(\mathbb{R}) \to \mathbb{R}^\times$.

Proposition 2.4.1. Let $\varphi : G \to G'$ be a group homomorphism:

1. IF $a_1.a_2 \dots a_n \in G$, then $\varphi(a_1 a_2 \dots a_n = \varphi(a_1)\varphi(a_2) \dots \varphi(a_n)$.
2. φ maps identity to identity.
3. φ maps inverses to inverses $\varphi(a^{-1}) = \varphi(a)^{-1}$.

Proof: All the three statements can be easily proved using the group axioms and the definition of φ.

Let us now talk about some terms associated with the group homomorphism $\varphi : G \to G'$:

- The *Image* of φ is denoted by $im(\varphi)$ or $\varphi(G)$ and is defined as -

$$im(\varphi) = \{x \in G' \mid x = \varphi(a) \text{for some} a \in G\} \tag{8}$$

- The *Kernel* of φ, denoted by $ker(\varphi)$ is the set of elements in G which map to the identity in G', or more precisely,

$$ker(\varphi) = \{a \in G \mid \varphi(a) = 1_{G'}\} \tag{9}$$

  The Kernel is a subgroup of G (Check!).

Though we shall discuss this later, we would need the notion of a *Coset* of a subgroup for now.

If H is a subgroup of a group G, then the notation aH is used to define a *left coset* of H in G:

$$aH = \{g \in G \mid g = ah \text{ for some } h \in H\} \tag{10}$$

Proposition 2.4.2. Let $\varphi : G \to G'$ be a homomorphism of groups, and let a and b be in G. Let K be the kernel of φ, The following conditions are equivalent:

- $\varphi(a) = \varphi(b)$,
- $a^{-1}b \in K$,
- $b \in$ the coset aK,
- The cosets aK and bK are equal.

Proof: Use the properties that homomorphisms carry inverses to inverses and the definition of a coset of a subgroup.

Corollary 2.4.3. A homomorphism is injective if and only if its kernel is trivial, that is $K(\varphi) = \{1\}$.

Definition 2.4.4. A subgroup N of a group G is a *Normal Subgroup* if for every $a \in N$ and every $g \in G$, the conjugate gag^{-1} is in N.

Proposition 2.4.5. The kernel of a group homomorphism is a normal subgroup.

Now, we shall consider some special homomorphisms.
An *Isomorphism* $\varphi : G \to G'$ from a group G to a group G' is a homomorphism which is bijective. An example would be the exponential map talked about earlier, with its codomain being restricted to the multiplicative group of positive real numbers. Now some related terms:

1. Two groups G and G' are said to be isomorphic (denoted as $G \approx G'$) if there exists and isomorphism φ from G to G'.
2. The groups isomorphic to a given group G form what is called the isomorphism class of G.
3. An Isomorphism from G to itself is called an *Automorphism.* Some examples would be the identity map defined by $g \rightsquigarrow g \forall\ f\ inG$ and the *conjugation* by g_1 defined by $g \rightsquigarrow g_1 g g_1^{-1}$.

2.5 Equivalence Relations and Partitions

A *Partition* Π of a set S is a subdivision of S into non-overlapping, non-empty subsets whose union as expected, is S. The concept of a partition of S and an equivalence relation on S are logically equivalent, as highlighted by the following proposition.

Proposition 2.5.1. An equivalence relation on a set S determines a partition of S, and vice versa.

Proof: Given a partition Π of S, we can define a relation on S by the rule $a \sim b$ if a and b lie in the same subset of Π. Conversely, given an equivalence relation, one can define a partition as: The subset that contains $a \in S$ is the set of all elements b such that $a \sim b$. This subset is called the *equivalence class* of a.

Lemma 2.5.2. Given an equivalence relation on a set S, the subsets of S that are equivalence classes partition S.

Any map of sets $f : S \to T$ gives us an equivalence relation on the domain S, defined by $a \sim b$ if $f(a) = f(b)$. The *inverse image* (also called *fibres* of the map f) of an element $t \in T$ is the subset of S consisting of all elements s such that $f(s) = t$, denoted by

$$f^{-1}(t) = \{s \in S \mid f(s) = t\} \tag{11}$$

Proposition 2.5.3. Let K be the kernel of the homomorphism $\varphi : G \to G'$. The fibre of φ that contains an element a of G is the coset aK of k. These cosets partition the group G, and they correspond to the elements of the image of φ.

2.6 Cosets

If H is a subgroup of a group G and if $g \in G$, the subset

$$gH = \{gh \mid h \in H\} \tag{12}$$

is called a *left coset*. The subgroup itself is a left coset ($H = 1H$).

Proposition 2.6.1. The left cosets of a subgroup H of a group G partition the group G.

Proof: We can easily prove that the left cosets are the equivalence classes for the equivalence relation defined by $a \sim b$ if $b = ah$ for some h in H. Then by Lemma 2.5.2, we are done!.

The number of left cosets of a subgroup H is called the *index* of H in G, which is denoted by -

$$[G : H]$$

Lemma 2.6.2. All left cosets aH of a subgroup H of a group G have the same order.

Proof: Multiplication by a defines a map $H \to aH$ which sends $h \rightsquigarrow ah \forall h \in H$. This map is bijective because its inverse is multiplication by a^{-1}.

Theorem 2.6.3 (Lagrange's Theorem)**.** Let H be a subgroup of a finite group G. The order of H divides the order of G.

Proof: We have seen that the left cosets aH form equivalence classes for a certain equivalence relation and thus partition the group G. Further, the map $H \to aH$ is a bijection, and hence, the order of every left coset of H is the same as order of H. Thus we are done.

The result of Lagrange's Theorem is often expressed as what is called the *Counting Formula*:

$$|G| = |H|[G : H] \tag{13}$$

Corollary 2.6.4. The order of an element of a finite group divides the order of a group.

Proof: The proof follows from the Counting formula and the alternate definition of the order discussed earlier.

Corollary 2.6.5. Suppose that a group G has prime order P. Let a be any element of G other than the identity. Then G is the cyclic group $\langle a \rangle$ generated by a.

When the Counting Formula is applied to group homomorphisms, we obtain the following corollary:

Corollary 2.6.6. Let $\varphi : G \to G'$ be a homomorphisms of finite groups, then:

- $|G| = |ker\varphi|.|im\varphi|$
- $|ker\varphi|$ divides $|G|$
- $|im\varphi|$ divides both $|G|$ and $|G'|$.

Just as we have defined left cosets, we can do the same for right cosets. The right cosets of a subgroup H of a group G are the sets:

$$Ha = \{ha \mid h \in H\} \tag{14}$$

We can define equivalence classes in this case exactly as we did earlier, and hence prove that the right cosets of a subgroup H of group G too partition G. We shall now state another proposition:

Proposition 2.6.7. Let H be a subgroup of a group G. The following conditions are equivalent:

1. H is a normal subgroup: $\forall\ h \in H$ and $\forall\ g \in G,\ \ ghg^{-1} \in H$,
2. $\forall\ g \in G,\ gHg^{-1} = H$,
3. $\forall\ g \in G,\ gH = Hg$,
4. Every left coset of H in G is a right coset.

Proposition 2.6.8.

1. If H is a subgroup of a group G and $g \in G$, the set ghg^{-1} is also a subgroup.
2. If a group G has just one subgroup H of order r, then that subgroup is normal.

Proof:

1. Conjugation by g is an automorphism of G, and gHg^{-1} is the image of H.
2. Follows from Proposition 2.6.7.

2.7 The Correspondence Theorem

Let $\varphi : G \to G'$ be a group homomorphism and let H be a subgroup of G. We may *restrict* φ to H, obtaining a homomorphism:

$$\varphi|_H : J \to G'$$

That is, we are simply restricting the domain to H. The restriction is a homomorphism because φ is one, and the kernel of $\varphi|_H$ is the interesection of the kernel of φ with H:

$$ker(\varphi|_H) = ker(\varphi) \cap H \tag{15}$$

The image of $\varphi|_H$ is same as the image $\varphi(H)$ of H under the map φ.

Proposition 2.7.1. Let $\varphi : G \to G'$ be a homomorphism with kernel K and let H' be a subgroup of G'. Denote its inverse image $\varphi^{-1}(H')$ by H. Then H is a subgroup of G that contains K. If H' is a normal subgroup of G' then H is a normal subgroup of G. If φ is surjective and if H is a normal subgroup of G, then H' is a normal subgroup of G'.

Proof: The proof is left as an exercise to the reader.

Theorem 2.7.2. Let $\varphi : G \to G'$ be a *surjective* homomorphism with kernel K. There exists a bijective correspondence between subgroups of G' and the subgroups of G that contain K.

The correspondence is defined as follows:

$$\text{a subgroup } H \text{ of } G \text{ that contains } K \rightsquigarrow \text{its image } \varphi(H) \text{ in } G$$
$$\text{a subgroup } H' \text{ of } G' \rightsquigarrow \text{its inverse image } \varphi^{-1}(H') \text{ in } G$$

If H and H' are corresponding subgroups, then H is normal in GH' is normal in G', and $|H| = |H'||K|$.

Proof: To prove this, we must check the following points:

- $\varphi(H)$ is a subgroup of G'.
- $\varphi^{-1}(H')$ is a subgroup of G and it contains K.
- $|\varphi^{-1}(H')| = |H'||K|$
- H' is a normal subgroup if and only if $\varphi^{-1}(H')$ is a normal subgroup of G.
- $\varphi(\varphi^{-1}(H')) = H'$ and $\varphi^{-1}(\varphi(H)) = H$.

2.8 Product and Quotient Groups

Let G, G' be two groups. The product set $G \times G'$, that is the set of pairs of elements (a, a') with $a \in G$ and $a' \in G'$, can be made into a group, with the group operation defined by the rule

$$(a, a').(b, b') = (ab, a'b') \tag{16}$$

The reader is urged to check that the group axioms are satisfied. The group thus obtained is called the *product* of G and G' and is denoted by $G \times G'$.

Proposition 2.8.1. Let H and K be subgroups of a group G, and let $f : H \times K \to G$ be the multiplication map, defined by $f(h, k) = hk$. Its image is the set $HK = \{hk \mid h \in H, k \in K\}$,

1. f is injective if and only if $H \cap K = \{1\}$
2. f is a homomorphism from the product group $H \times K$ to G if and only if elements of K commute with the elements of H: $hk = kh$
3. If H is a normal subgroup of G, then HK is a normal subgroup of G
4. f is an isomorphism from the product group $H \times K$ to G if and only if $H \cap K = \{1\}$, $HK = G$ and H and K are normal subgroups of G.

Let G be a group and N be a normal subgroup of G. We denote the set of cosets of N as G/N, that is,

$$G/N := \{aN \mid a \in G\} \tag{17}$$

When we regard a coset C as an element of the set of cosets, the bracket notation $[C]$ may be used. If $C = aN$ we may also denote $[C]$ by $\bar{a}$, then we denote the set of cosets by $\bar{G}$, that is,

$$\bar{G} = G/N \tag{18}$$

Theorem 2.8.2. Let N be a normal subgroup of the group G, and let $\bar{G}$ denote the set of cosets of N in G. There is a law of composition on $\bar{G}$ that makes this set into a group, such that the map $\pi : G \to \bar{G}$ defined by $\pi(a) = \bar{a}$ is a surjective homomorphism whose kernel is N.

We use the following notation: if $A, B \subset G$ then AB, called the *product set* denotes the set of products ab with $a \in A, b \in B$.

Lemma 2.8.3. Let N be a normal subgroup of a group G, and let aN and bN be cosets of N, where $a, b \in G$. The product set $(aN)(bN)$ is also a coset, and is equal to the coset $(ab)N$. Further, if $aN = xN$ and $bN = yN$, where $x, y \in G$ and $x \neq a, y \neq b$, then $(aN)(bN) = (xN)(yN) = (ab)N = (xy)N$.

Proof: Use the definition of a normal subgroup to prove this.

The lemma allows to define multiplication on the set $\bar{G} = G/N$ and shows that it is well defined. Thus, we see, if $a, b \in G$ and hence $\bar{a}, \bar{b} \in \bar{G}$, then $\bar{a}\bar{b} = [aN][bN] = [abN] = \bar{ab}$. Hence we see

$$\pi(a)\pi(b) = \bar{a}\bar{b} = \bar{ab} = \pi(ab) \tag{19}$$

Lemma 2.8.4. Let G be a group, and let Y be a set with a law of composition, both laws written with multiplicative notation. Let $\varepsilon : G \to Y$ be a surjective map with the homomorphism property, that $\varepsilon(ab) = \varepsilon(a)\varepsilon(b) \forall a, b \in G$. Then Y is a group and ε is a homomorphism.

Proof: The group axioms that are true in G are carried over to Y by the surjective map ε. Use the group axioms of G and the homomorphism property of ε to prove this.

Theorem 2.8.5 (First Isomorphism Theorem)**.** Let $\varepsilon : G \to G'$ be a surjective group homomorphism with kernel N. The quotient group $\bar{G} = G/N$ is isomorphic to the image G'. More precisely, let $\pi : G \to \bar{G}$ be the canonical map. There is a unique isomorphism $\bar{\varepsilon} : \bar{G} \to G'$ such that $\varepsilon = \bar{\varepsilon} \circ \pi$.

Proof: The elements of $\bar{G}$ are the cosets of N, and also are the fibres of the map ε. The map $\bar{\varepsilon}$ referred to in this theorem is the one that sends a nonempty fibre to its image $\bar{\varepsilon}(\bar{x}) = \varepsilon(x)$. For any surjective map of sets $\varepsilon : G \to G'$ we can form the set of fibres $\bar{G}$ and establish a bijective map $\bar{\varepsilon}$ that sends a fibre to its image. When ε is a group homomorphism, $\bar{\varepsilon}$ is an isomorphism. (why?)

3 Abstract Symmetry

3.1 Generalising Symmetry

The set of automorphisms of an algebraic structure X forms a a group, with the law of composition being the composition of maps (Verify!). The words "automorphism" and "Symmetry" are synonymous, with the difference being in preservation of the algebraic and geometric structure respectively. Both of these are special cases of the more general concept of a group operation.

An operation of a group G on a set S is a rule for combining an element $g \in G$ and an element $s \in S$ to get another element of S. That is, it is a map $G \times S \to S$. We denote the action of g on s as gs, hence the aforementioned map is defined as $(g, s) \rightsquigarrow gs$.
For each $s \in S$. we define a set O_s, called the orbit of s, which consists of all the possible elements of S that s can map to, when acted on by an element of G:

$$O_s = \{\mathfrak{s} \in S \mid \mathfrak{s} = gs \text{ for some } g \in G\} \tag{20}$$

The orbits for a group are equivalence classes (define the equivalence relation!), and hence partition S. If S consists of just one orbit, the operation of G on S is called transitive.

The *stabilizer* of an element $s \in S$, denoted by G_s, is the set of group elements that leave s fixed. It is a subgroup of G (verify!):

$$G_s = \{g \in G \mid gs = s\} \tag{21}$$

Proposition 3.1.1. Let S be a set on which a group G operates, let s be an element of S, and let H be the stabilizer of s.

1. If $a, b \in G$, then $as = bs$ if and only if $a^{-1}b \in H$, which is true if and only if $b \in aH$.
2. Suppose that $as = s'$. The stabilizer H' of s' is a *conjugate subgroup*:

$$H' = aHa^{-1} = \{g \in G \mid g = aha^{-1} \text{ for some } h \in H\} \tag{22}$$

Proof:

1. $as = bs \Leftrightarrow s = a^{-1}bs$.
2. If g is in aHa^{-1}, say $g = aha^{-1}$ with h in H, then $gs' = (aha^{-1})(as) = ahs = as = s'$, so g stabilizes s'. Thus $aHa^{-1} \subset H'$. Since $s = a^{-1}s'$, we can reverse the roles of s and s', to conclude that $a^{-1}H'a \subset H \Rightarrow H' \subset aHa^{-1}$. Therefore, $H' = aHa^{-1}$.

3.2 The operation on Cosets

We shall use the same notation as that of our discussion on quotient groups.

Proposition 3.2.1. Let H be a subgroup of G.

1. The operation of G on the set G/H of cosets is transitive,
2. The stabiliser of the coset $[H]$ is the subgroup H.

Let us take an example. Let G be the symmetric group S_3, and H be the cyclic subgroup $\{1, y\}$. Its left cosets are,

$$C_1 = H = \{1, y\},\ C_2 = xH = \{x, xy\},\ C_3 = x^2H = \{x^2, x^2y\} \tag{23}$$

and G operates on the set of cosets $G/H = \{[C_1], [C_2], [C_3]\}$. The elements x and y operate in the same way as on the set of indices $\{\mathbf{1}, \mathbf{2}, \mathbf{3}\}$:

$$m_x(\mathbf{123}) \text{ and } m_y(\mathbf{12}) \tag{24}$$

The next proposition is also called the orbit stabilizer theorem.

Proposition 3.2.2. Let S be a set on which a group G operates, and let $s \in S$. Let H and O_s be the stabilizer and orbit of s, respectively. There is a bijective map $\epsilon : G/H \to O_s$ defined by $[aH] \rightsquigarrow as$. This map is compatible with the operations of the group: $\epsilon(g[C]) = g\epsilon([C])$ for every $[C] \in G/H$ and every $g \in G$.

3.3 The Counting Formula

Proposition 3.3.1. Let S be a finite set on which a group G operates, and let G_s and O_s be the stabilizer and orbit of $s \in S/$ Then,

$$|G| = |G_s||O_s| \tag{25}$$

Thus the order of the orbit is equal to the index of the stabilizer,

$$|O_s| = [G : G_s] \tag{26}$$

Another formula is one which uses the partition of the set S into orbits to count its elements. If we index the orbits arbitrarily as O_i, we have,

$$|S| = |O_1| + |O_2| + \cdots + |O_k| \tag{27}$$

3.4 Permutation Representations

A *Permutation Representation* of a group G is a homomorphism from the group to a symmetric group:

$$\varphi : G \to S_n \tag{28}$$

Proposition 3.4.1. Let G be a group, There is a bijective correspondence between operations of G on the set $S = \{1, 2 \dots n\}$ and the permutation representations $G \to S_n$.

Proof: If we are given an operation of G on S, we define a permutation representation φ by setting $\varphi(g) = m_g$, that is, multiplication by g. The associative property $g(hi) = (gh)i$ shows that

$$m_g(m_h i) = g(hi) = (gh)i = m_{gh} i$$

Hence φ is a homomorphism. Conversely, if φ is a permutation representation, the same formula defines an operation of G on S.

Corollary 3.4.2. Let $\mathrm{Perm}(S)$ denote the group of permutations of a set S and let G be a group. There is a bijective correspondence between operations of G on S, and permutation representations $\varphi : G \to \mathrm{Perm}(S)$.

A permutation representation $G \to \mathrm{Perm}(S)$ need not be injective, and if it is, we say that the corresponding operation is *faithful*. More precisely, an operation is faithful if it possesses this property:

The only element g of G such that $gs = s \ \forall s \ \in S$ is the identity

4 Fields

This section provides a brief introduction to fields and some properties associated with fields.

We shall develop the concept of a field by discussing the *subfields* of the *field* $\mathbb{C}$ of complex numbers. A subfield F of $\mathbb{C}$ is a subset that is closed under the four operations of addition, subtraction, multiplication, and division, and which contains 1. With these conditions, can we deduce whether $0 \in F$?. Some examples of subfields of $\mathbb{C}$:

1. the field $\mathbb{R}$ of real numbers,
2. the field $\mathbb{Q}$ of rational numbers.

Now we shall proceed to the concept of an abstract field.

Definition 4.0.1. A *field* F is a set together with two laws of composition

$$F \times F \xrightarrow{\times} F \text{ and } F \times F \xrightarrow{+} F$$

called addition $a, b \rightsquigarrow a + b$ and multiplication $a, b \rightsquigarrow ab$, which satisfy the following axioms:

1. Addition makes F into an abelian group F^+; its identity element is denoted by 0.
2. Multiplication is commutative, and it makes the set of nonzero elements of F into an abelian group $F^\times$; its identity element being denoted as 1.
3. *distributive law:* For all a, b and $c \in F$, $a(b + c) = ab + ac$.

The next lemma describes how the zero element multiplies,

Lemma 4.0.2. Let F be a field.

1. For all $a \in F$, $a0 = 0a = 0$.
2. The elements 0 and 1 of F are distinct.
3. Multiplication in F is associative. and 1 is the corresponding identity element.

Proof: To prove the first statement we see that, since 0 is the identity for addition, $0 + 0 = 0$, thus, $a0 + a0 = a0$, and since F^+ is a group, we can cancel $a0$ and get $a0 = 0$. Similarly, $0a = 0$. To prove that $0 \neq 1$ in F, we note that F is an abelian group under multiplication with the identity element 1, and hence $a1 = 1a = a, \forall a \in F$. Let us assume that $0 = 1$. We immediately face a contradiction, as per the first statement for any nonzero a. The third statement can be simply proved by using the first statement and the fact that $F - \{0\}$ is an abelian group under multiplication.

Now let us discuss what are called prime fields. We know that the set $\mathbb{Z}/n\mathbb{Z}$ of congruence classes modulo an integer n has laws of addition and multiplication derived from addition and multiplication of integers. All of the axioms for a field except the existence of multiplicative inverses hold here. And we noted that these axioms carry over to the addition and multiplication of congruence classes (where did we see this?). As it happens when n is prime ($n = p$, say), all non zero congruence classes modulo p have inverses, and therefore the set $\mathbb{Z}/p\mathbb{Z}$ is a field, called a *prime field*, and denoted by $\mathbb{F}_p$. Using bar notation,

$$\mathbb{F}_p = \{\bar{1}, \bar{2}, \ldots p \bar{-} 1\} = \mathbb{Z}p/\mathbb{Z} \tag{29}$$

Theorem 4.0.3. Let p be a prime integer. Every nonzero congruence class modulo p has a multiplicative inverse, and therefore $\mathbb{F}_p$ is a field of order p.

To prove this theorem, we will need the following proposition:

Proposition 4.0.4. Let p be a prime integer and let $\bar{a}, \bar{b}$ and $\bar{c} \in \mathbb{F}_p$:

- If $\bar{a}\bar{b} = 0$ then $\bar{a} = 0$ or $\bar{b} = 0$.
- If $\bar{a} \neq \bar{0}$, and if $\bar{a}\bar{b} = \bar{a}\bar{c}$, then $\bar{b} = \bar{c}$.

Proof: To do this, we represent the classes $\bar{a}$ and $\bar{b}$ by integers a and b, and then we have to prove the following - If p divides ab then p divides a or p divides b. And then second statement follows naturally.

Proof of Theorem 4.0.3: Let $\bar{a}$ be a nonzero element of $\mathbb{F}_p$. Consider the powers $\bar{a}, \bar{a}^2, \bar{a}^3 \ldots$. Since there are infinitely many exponents and only finitely many elements in $\mathbb{F}_p$, there must be two powers that are equal, say $\bar{a}^m = \bar{a}^n$ with $m < n$. We cancel $\bar{a}^m$ from both sides: $\bar{1} = \bar{a}^{n-m}$. Then we can see that $\bar{a}^{m-n-1}$ is the inverse of $\bar{a}$.

We shall state another theorem concerning prime fields, whose proof will be left for later.

Theorem 4.0.5 (Structure of the Multiplicative Group)**.** Let p be a prime integer. The multiplicative group $\mathbb{F}_p^\times$ of the prime field is a cyclic group of order $p-1$.
A generator for the cyclic group $\mathbb{F}_p^\times$ is called a *primitive root* modulo p. Thus, if we drop the bar notation (keeping in mind that an integer in this context represents a congruence class), and let ϵ be a primitive root, there are two ways to list the elements of $\mathbb{F}_p^\times$:

$$\mathbb{F}_p^\times = \{1, 2, 3 \ldots p-1\} = \{1, \epsilon, \epsilon^2 \ldots \epsilon^{p-2}\} \tag{30}$$

5 Rings

5.1 Definition

Let us begin by the definition of a Ring:

Definition 5.1.1. A *ring* R is a set with two laws of composition $+$ and $\times$ - called addition and multiplication, that satisfy these axioms:

1. With the law of composition $+$, R is an abelian group that we denote by R^+; it has the identity denoted by 0.
2. Multiplication is commutative and associative, and has the identity denoted by 1,
3. *distributive law:* For all a, b and c in R, $(a+b)c = ac + bc$.

A *Subring* of a ring is a subset that is closed under the operations of addition, subtraction, and multiplication and that contains the element 1. For example, the *Gauss integers*, the complex numbers of the form $a + bi$ is a subring of the ring of the complex numbers $\mathbb{C}$ which we denote by $\mathbb{Z}[i]$:

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$$

Geometrically, we can see that the elements of $\mathbb{Z}[i]$ form a square lattice in the complex plane. We can, in fact form a subring $\mathbb{Z}[\alpha]$ for any $\alpha \in \mathbb{C}$. (Will its elements too form a lattice in the complex plane?). Since a subring is closed under addition and multiplication and contains 1, and $\mathbb{Z}[\alpha]$ contains α, we can see that, $\mathbb{Z}[\alpha]$ is the set of all complex numbers β such that:

$$\beta = a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 \text{ where, all } a_i \in \mathbb{Z}$$

A complex number α is *algebraic* if it is a root of a nonzero polynomial with integer coefficients. Think of some examples!. If there is no such polynomial, then α is *transcedental.* Again, examples! - the numbers e and π are transcedental. When a complex number α is transcedental, then the elements of the ring $\mathbb{Z}[\alpha]$ correspond bijectively to polynomials with integer coefficients, with the correspondence defined by $p(\alpha) \rightsquigarrow p(x)$.

Proposition 5.1.2. A ring R in which elements 1 and 0 are equal is the zero ring.

Proof: We note that $0a = 0 \; \forall \; a \in R$. Let us assume that $1 = 0$. Let a be any element in R. Then $a = 1a = 0a = 0$. Thus the only element in R is 0!

Though all the elements of a ring are not required to have multiplicative inverses, some might, and if so, then the inverse is unique. A *unit* of a ring is an element that has a multiplicative inverse. The units in $\mathbb{Z}[i]$ are ± 1 and $\pm i$. The identity element of a ring is always a unit, and any ill-defined mention of a unit of a ring is more often than not directed at the identity element.

5.2 Polynomial Rings

A *Formal Polynomial* with coefficients in a ring R is a finite linear combination of powers of the variable:

$$f(x) = a_nx^n + a_{n-1}x^{n-1} + \ldots a_1x + a_0$$

where the coefficients a_i are elements of R. Every formal polynomial with real coefficients determines a polynomial function on the real numbers. From now on, we shall use *polynomial* for a formal polynomial.

- The set of polynomials with coefficients in a ring R will be denoted by $R[x]$. Two polynomials in $R[x]$ are equal if and only if all their coefficients are equal,
- The *degree* of a nonzero polynomial, denoted by deg f is the largest n such that the coefficient a_n of x^n is not zero,
- A polynomial of degree 0 is called a constant polynomial,
- The nonzero highest coefficient of a polynomial is called the *leading coefficient*, and a polynomial with a leading coefficient one is called a *monic polynomial.*

Proposition 5.2.1. There is a unique commutative ring structure on the set of polynomials $R[x]$ having these properties:

- Addition of polynomials is defined by

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots = \sum_k (a_k + b_k)x^k$$

- Multiplication of polynomials is defined by

$$f(x)g(x) = p_0 + p_1 x + p_2 x^2 \ldots$$

  with

$$p_k = \sum_{i+j=k} a_i b_j$$

- The ring R becomes a subring of $R[x]$ when the elements of R are identified with the constant polynomials.

We shall now state another proposition and its corollaries without proof, as they are elementary.

Proposition 5.2.2. Let R be a ring, let f be a monic polynomial and let g be any polynomial, both with coefficients in R. There are uniquely determined polynomials q and r in $R[x]$ such that

$$g(x) = q(x)f(x) + r(x)$$

and such that, the remainder r, if not zero, has degree less than that of f. Moreover, f divides g in $R[x]$ if and only if the remainder r is zero.

Corollary 5.2.3. Division with remainder can be done whenever the leading coefficient of f is a unit. In particular, it can be done whenever the coefficient ring is a field and $f \neq 0$.

Corollary 5.2.4. Let $g(x)$ be a polynomial in $R[x]$ and let α be an element of R. The remainder of division of $g(x)$ by $(x - \alpha)$ is $g(\alpha)$. Thus $x - \alpha$ divides g in $R[x]$ if and only if $g(\alpha) = 0$

A *monomial* is a formal product of some variables $x_1, x_2 \ldots x_n$ which in multi index notation is written symbolically as:

$$x^i = x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}$$

where $i = (i_1, i_2 \ldots i_n)$ denotes a multi index in the vector form.
A *polynomial* in the variables x_j with coefficients in R is a linear combination of finitely many monomials with coefficients in R, and in multi index notation is written uniquely as

$$f(x) = \sum_i a_i x^i$$

where i runs through all the multi index tuples.

5.3 Homomorphisms and Ideals

A *ring homomorphism* $\varphi : R \to R'$ is a map from one ring to another which is compatible with the laws of composition and which carries the unit 1 of R to the unit 1 of R', that is,

$$\varphi(a+b) = \varphi(a) + \varphi(b), \varphi(ab) = \varphi(a)\varphi(b) \text{ ,and } \varphi(1) = 1.$$

Question for the reader - Why did we state $\varphi(1) = 1$ separately? Does it not follow from the compatibility with multiplication?
A very important example of a ring homomorphism can be obtained by evaluation of polynomials, such as - evaluation of real polynomials at a real number a defines a homomorphism

$$\mathbb{R}[x] \to \mathbb{R} \text{ that sends } p(x) \rightsquigarrow p(a)$$

Proposition 5.3.1. Let $\varphi : R \to R'$ be a ring homomorphism, and let $R[x]$ be the ring of polynomials with coefficients in R.

1. Let α be an element of R'. There is a unique homomorphism $\Phi : R[x] \to R'$ that agrees with the map φ on constant polynomials and sends $x \rightsquigarrow \alpha$.
2. More generally, given elements $\alpha_1, \alpha_2 \dots \alpha_n$ of R' there is a unique homomorphism $\Phi : R[x_1, x_2 \dots x_n] \to R'$ from the polynomial ring in n variables to R', that agrees with φ on constant polynomials and that sends $x_i \to \alpha_i$ for $i \in \{1, 2, 3 \dots n\}$.

Proof: 1. Can be easily proved by defining Φ as

$$\Phi(\sum a_i x^i) = \sum \varphi(a_i)\alpha^i$$

With this we can verify the conditions on Φ to be a homomorphism, and its uniqueness. Further 2. can be proved similarly with multi index notation. Now, given two rings R and S and a ring homomorphism $\varphi : R \to S$, we can, by composing φ with the inclusion of S as a subring of $S[x]$, and applying the substitution principle, we obtain a homomorphism $\Phi : R[x] \to S[x]$ that sends $x \rightsquigarrow x$. The use of this is highlighted in the next proposition.

Proposition 5.3.2. Let $x = (x_1, x_2 \dots x_n)$ and $y = (y_1, y_2 \dots y_n)$ denotes sets of variables, and R be a ring. There is a unique isomorphism $R[x, y] \to R[x][y]$ which is the identity on R and which sends the variables to themselves.

Let R and R' be rings and $\varphi : R \to R'$ be a ring homomorphism. The *kernel* of φ is defined as:

$$ker(\varphi) = \{s \in R \mid \varphi(s) = 0\}$$

Compare this with kernel of the group homomorphism of additive groups $R^+ \to R'^+$. What do you observe? We see that the two are the same, and hence the properties of the kernel of a group homomorphism apply.

Definition 5.3.3. An *ideal* $I$of a ring R is a non empty subset of R with these properties:

- I is closed under addition, and
- If $s \in I$ and $r \in R \Rightarrow rs \in I$

It is easy to see that, the kernel of a ring homomorphism is an ideal.
In any ring R, the multiples of a particular element a form an ideal called the *principal ideal* generated by a, denoted as:

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

The ring itself is the principal ideal (1), called the unit ideal and the set consisting of zero alone is the principal ideal (0), called the zero ideal. An ideal is *proper* if it is neither the zero ideal nor the unit ideal. Can a proper ideal have 1 as an element?

An example: Let $\varphi : \mathbb{R}[x] \to \mathbb{R}$ be defined by substituting the real number 5 for x. Its kernel is the set of polynomials divisible by $x - 5$. This is a principal ideal, and can be denoted by $(x - 5)$.
Every ideal satisfies the requirements for a subring, except that the unit element 1 of R will not be in I unless I is the whole ring. Hence, by definition, an ideal is not a subring unless it is the whole ring.

Proposition 5.3.4. The ideals in the rings of integers are the subgroups of $\mathbb{Z}^+$, and they are principal ideals.

Proof: An ideal of the ring of integers will be a subgroup of $\mathbb{Z}^+$ (why?). And we have already proved that every such subgroup has a form $\mathbb{Z}n$ for some $n \in \mathbb{Z}$.

5.4 Quotient and Product Rings

Let I be an ideal of a ring R. The cosets of the additive subgroup I^+ of R^+ are the subsets $a + I$. It follows from what has been proved for groups that the set of cosets $\bar{R} = R/I$ is a group under addition. It is also a ring:

Theorem 5.4.1. Let I be an ideal of a ring R. There is a unique ring structure on the set $\bar{R}$ of additive cosets of I such that the map $\pi : R \to \bar{R}$ that sends $a \rightsquigarrow \bar{a} = [a + I]$ is a ring homomorphism. The kernel of π is the ideal I.
$\bar{R}$ is called the quotient ring, and the map π is called the canonical map.

Proof: We want to put a ring structure on $\bar{R}$ and if we forget about multiplication and consider only the addition law, I becomes a normal subgroup of R^+, for which the proof has already been done. What is left, is to define multiplication, to verify the ring axioms, and to prove that π is a homomorphism. Let $\bar{a} = [a + I]$ and $\bar{b} = [b + I]$ be elements of $\bar{R}$. We would like to define the product by setting $\bar{a}\bar{b} = [ab + I]$. The rest of the proof follows from the pattern followed in quotient groups.

Theorem 5.4.2 (Mapping Property of Quotient Rings)**.** Let $f : R \to R'$ be a ring homomorphism with kernel K and let I be another ideal. Let $\pi : R \to \bar{R}$ be the canonical map from R to $\bar{R} = R/I$.

1. If $I \subset K$, there is a unique homomorphism $\bar{f} : \bar{R} \to R'$ such that $\bar{f}\pi = f$:
2. *First Isomorphism Theorem:* If f is surjective and $I = K$, $\bar{f}$ is an isomorphism.

Theorem 5.4.3 (Correspondence Theorem)**.** Let $\varphi : R \to \mathcal{R}$ be a *surjective* ring homomorphism with kernel K. There is a bijective correspondence between the set of all ideals of $\mathcal{R}$ and the set of ideals of R that contain K. The correspondence is defined as follows:

- If I is an ideal of R and if $K \subset I$, the corresponding ideal of $\mathcal{R}$ is $\varphi(I)$.
- If $\mathcal{I}$ is an ideal of $\mathcal{R}$, the corresponding ideal of R is $\varphi^{-1}(\mathcal{I})$

If the ideal I of R corresponds to the ideal $\mathcal{I}$ of $\mathcal{R}$, the quotient rings R/I and $\mathcal{R}/\mathcal{I}$ are isomorphic.

Proof: Let $\mathcal{I}$ be an ideal of $\mathcal{R}$ and let $I \supset K$ be an ideal of R. The reader is encouraged to prove this by checking the following points:

1. $\varphi(I)$ is an ideal of $\mathcal{R}$,
2. $\varphi^{-1}(\mathcal{I})$ is an ideal of R and $K \in \varphi^{-1}(\mathcal{I}$,
3. $\varphi(\varphi^{-1}(\mathcal{I}) = \mathcal{I}$ and $\varphi^{-1}(\varphi(I) = I$
4. If $\varphi(I) = \mathcal{I}$, then $R/I \sim \mathcal{R}/\mathcal{I}$

The next proposition describes the notion of product rings.

Proposition 5.4.4. Let R and R' be rings,

1. The product set $R \times R'$ is called the product rings, with addition and multiplication defined component wise -
$$(x, x') + (y, y') = (x + x', y + y') \ (x, x')(y, y') = (xx', yy')$$
2. The additive and multiplicative identities are $(0, 0)$ and $(1, 1)$ respectively.
3. The projections $\pi : R \times R' \to R$ and $\pi' : R \times R' \to R'$ defined by $\pi(x, x') = x$ and $\pi'(x, x') = x'$ are ring homomorphisms. The kernels of π and π' are the ideals $\{0\} \times R'$ and $R \times \{0\}$ respectively of $R \times R'$,
4. The kernel $R \times \{0\}$ of π' is a ring, with multiplicative identity $e = (1, 0)$. It is not a subring of $R \times R'$ unless R' is the zero ring. Similarly, $\{0\} \times R'$ is the ring with identity $(0, 1)$ and is not a subring of $R \times R'$ unless R is the zero ring.

5.5 Fractions

Let us denote the ring of integers by R, and review some of the familiar properties of fractions:

- A *fraction* is a symbol a/b or $\frac{a}{b}$, where a and b are elements of R and $b \neq 0$.
- Elements of R are viewed as fractions by the rule $a = \frac{a}{1}$.
- Two fractions $\frac{a_1}{b_1}$ and $\frac{a_2}{b_2}$ are equivalent, $\frac{a_1}{b_1} \sim \frac{a_2}{b_2}$, if $a_1 b_2 = a_2 b_1$.
- Sums and products of fractions are given by $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$, and $\frac{a}{b}\frac{c}{d} = \frac{ac}{bd}$.

When we try to apply these ideas to a general ring R, the problem that awaits us lies in the fourth point - while $b \neq 0$ and $c \neq 0$, bd very well be zero. Take the example of $R = \mathbb{Z}/(6)$ with $b = [2]$ and $c = [3]$.

Definition 5.5.1. An *Integral Domain* R, or just a *domain* for short, is a ring with this property: R is not the zero ring, and if a and b are elements of R whose product ab is zero, then $a ==$ or $b = 0$.

Any subring of a field is a domain (is the reverse implication true?), and if R is a domain, the polynomial ring $R[x]$ is also a domain. An integral domain R satisfies the *cancellation law*:

$$\text{If } ab = ac \text{ and } a \neq 0, \Rightarrow b = c. \tag{31}$$

An element a of a ring is called a *zero divisor* if it is nonzero, and if there is another nonzero element b such that $ab = 0$. An integral domain is a nonzero ring which contains no zero divisors.

Theorem 5.5.2. Ler F be the set of equivalence classes of fractions of elemetns of an integral domain R,

1. With the laws defined as above, F is a field, called the *fraction field* of R.
2. R embeds as a subring of F by the rule $a \rightsquigarrow a/1$.
3. *Mapping Property:* If R is embedded as a subring of another field $\mathcal{F}$, the rule $\frac{a}{b} = ab^{-1}$ embeds F into $\mathcal{F}$ too.

To elaborate on the "Mapping property", we can imagine that the embedding of R into $\mathcal{F}$ is given by an injective ring homomorphism $\varepsilon : R \to \mathcal{F}$. The assertion then is that the rule $\epsilon\frac{a}{b} = \varepsilon(a)\varepsilon(b)^{-1}$ extends ε to an injective homomorphism $\epsilon : F \to \mathcal{F}$.

Proof: We lay the basis of the proof by firstly showing that the equivalence of fraction is indeed an equivalence relation.

- Symmetricity: Let $\frac{a}{b} \sim \frac{c}{d} \Rightarrow ad = bc \Rightarrow bc = ad \Rightarrow \frac{c}{d} \sim \frac{a}{b}$
- Transitivity: Let us take the non trivial case when numerators are non zero too, and let $\frac{a}{b} \sim \frac{c}{d}$ and $\frac{e}{f} \sim \frac{c}{d}$. Then we have, $ad = bc$ and $ed = fc \Rightarrow fc = ed$. Multiplying the two equations, we have $afdc = bedc$. Now, since R is an integral domain, and $c \neq 0, d \neq 0$, we have $af = be \Rightarrow \frac{a}{b} \sim \frac{e}{f}$.
- Reflexivity: Trivial.

Now we show that addition and multiplication are well defined on the equivalence classes. We again take the nontrivial case with nonzero numerators. Let $\frac{a_1}{b_1} \sim \frac{a_2}{b_2} \Rightarrow a_1b_2 = a_2b_1$. We have $\frac{a_1}{b_1} + \frac{c}{d} = \frac{a_1d+b_1c}{b_1d}$. Now since $a_1 = \frac{a_2b_1}{b_2}$ we have, $\frac{a_1d+b_1c}{b_1d} \sim \frac{a_2d+b_2c}{b_2d}$. Thus, $\frac{a_1}{b_1} + \frac{c}{d} \sim \frac{a_2}{b_2} + \frac{c}{d}$. And similarly, $\frac{a_1}{b_1}\frac{c}{d} \sim \frac{a_2}{b_2}\frac{c}{d}$. Now to complete the proof, some straightforward verifications are needed.

Now, a fraction of polynomials is callled a *rational function*, and the fraction field of the polynomial ring $K[x]$, where K is a field, is called the *field of rational functions* in x, with coefficients in K, usually denoted by $K(x)$:

$$\begin{gathered} K(x) = \text{equivalence classes of fractions } \tfrac{f}{g}, \text{ where, } f, g \text{ are polynomials, and} \\ g \text{ is not the zero polynomial.} \end{gathered} \tag{32}$$

6 Vector Spaces and Modules

6.1 Vector Spaces

In this report, rather than building up from the idea of column vectors, we will rather delve into the abstract definition of a vector space.

Definition 6.1.1. A *vector space* V over a field F is a set together with two laws of composition:

1. *addition:* $V \times V \to V$, written $v, w \rightsquigarrow v + w$, for v and w in V.
2. *scalar multiplication* by the elements of the field: $F \times V \to V$, written $c, v \rightsquigarrow cv$ for $c \in F$ and $v \in V$.

These laws are required to satisfy the following axioms:

- Addition makes V into a commutative group V^+, with identity denoted by 0.
- $1v = v \forall v \in V$.
- *associative law:* $(ab)v = a(bv)$ for all $a, b \in F$ and all $v \in V$.
- *distributive laws:* $(a + b)v = av + bv$ and $a(v + w) = av + aw$, for all $a, b \in F$ and $v, w \in V$.

Note that the first axioms inherits all the axioms of a commutative group.

The space F^n of column vectors with entries in the field F forms a vector space over F. Here we would have the operations:

$$\textit{addition: } \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix} + \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix} = \begin{bmatrix} a_1 + b_1 \\ a_2 + b_2 \\ \vdots \\ a_n + b_n \end{bmatrix} \tag{33}$$

$$\textit{scalar multiplication: } c \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix} = \begin{bmatrix} ca_1 \\ ca_2 \\ \vdots \\ ca_n \end{bmatrix} \tag{34}$$

for all $a_1 \dots a_n, b_1 \dots b_n, c \in F$.
Some more examples include,

1. The solutions of the linear ordinary differential equation $y''' + y'' - 2y = 0$ form a vector space over $\mathbb{R}$, with addition being defined as the addition of functions and scalar multiplication being defined in the usual sense of multiplying a function by a scalar.
2. The set of real polynomials in the variable x, $p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots a_0$ is a vector space over $\mathbb{R}$, with addition and scalar multiplication being defined in the usual sense for polynomials.
3. The set of $m \times n$ $(m, n \in \mathbb{N})$ matrices with entries in $\mathbb{C}$ form a vector space over $\mathbb{C}$.

Now, as with groups and subgroups, rings and subrings, we have subspaces of a vector space. A subspace W of a vector space V over a field F is a non empty subset closed under the operations of addition and scalar multiplication. A subspace is said to be proper if it is neither the trivial subspace $\{0\}$ or the vector space V itself. There is another way to state the condition for a subspace:

$$\text{A non empty subset } W \text{ of the vector space, and if } a_1, a_2 \ldots a_n \in W \text{ and}$$
$$c_1, c_2 \ldots c_n \in F \Rightarrow c_1a_1 + c_2a_2 + \ldots c_na_n \in W$$

6.2 Modules

Modules have some deal of similarity with vector spaces, as will be evident by the definition:

Definition 6.2.1. Let R be a ring. A *left R module* or a *left module over R* is a set M together with

1. An operation $+$ on M which makes M into an abelian group
2. A map $R \times M \to M$ defined by $r, m \rightsquigarrow rm$ for all $r \in R$ and for all$m \in M$ which satisfies the following axioms,
   - $(r+s)m = rm + rs$, for all $r, s \in R$ and $m \in M$,
   - $(rs)m = r(sm)$m for all $r, s \in R$ and $m \in M$,
   - $r(m+n) = rm + rn$ for all $r \in R$ and $m, n \in M$,
   - $1m = m \; \forall \; m \in M$.

Note, in the last axiom the '1' denotes the element 1 in R. We have only dealt with rings containing the multiplicative identity, but it is to be noted that the last axiom is not to be imposed if the ring in consideration does not have a multiplicative identity.

The descriptor "left" in the definition describes that the ring elements appear only on the left. Right R modules are defined analogously. Further if R is commutative (like the rings that we mostly have dealt with) and M is a left R module, then we can make M into a right R module by defining $mr = rm$.

Now to comment on the similarity between vector spaces and modules - when R is a field F the axioms for a R-module are precisely the same as thse for a vector space over F, and thus,

modules over a field F and vector spaces over F are exactly the same

Now, analogous to vector spaces and subspaces, we proceed to talk about submodules, in the context of a left ring module.

Let R be a ring and M be an R-module. An R submodule of M is a subgroup N of M which is closed under the action of rind elements, that is, $rn \in N \forall r \in R$ and $n \in N$.
Again, if R is a field, the submodules are exactly the same as subspaces.

7 More on Fields

7.1 Field Extensions and Examples

A *Field Extension* has to do with a pair of fields $F \subset K$, one contained in the other. Given such a pair, K is called a field extension of F, and F is called a *subfield* of K. The notation K/F will indicate that $K$is a field extension of F. The most common example being, that the complex numbers are a field extension of the real numbers.

A *Finite Field* is a field that contains finitely many elements. A finite field contains one of the prime fields $\mathbb{F}_p$ and therefore is an extension of that field.

Extensions of the field $\mathbb{F} = \mathbb{C}(t)$ of rational functions are called function fields. These can be defined by an implicit equation $f(t, x) = 0$. And we may also define x implicitly as a function $x(t)$ of t. Let us take an example, $x^2 - t = 0$, here we have the explicit form $x(t) = \sqrt{t}$, and the corresponding function field consists of the combinations $p + q\sqrt{t}$, where p and q are rational functions in t.

7.2 Algebraic and Transcedental Elements

Let K be an extension of a field F, and let α be an element of K. The element α is algebraic *over* F if it is a root of a monic polynomial with coefficients in F, say,

$$f(x) = x^n + a_{n-1}x^{n-1} + \ldots a_0, \text{ with } a_i \in F \tag{35}$$

and $f(\alpha) = 0$. An element is transcedental over F if no such polynomial exists.

Proposition 7.2.1. Let α be an element of an extension field K of a field f that is algebraic over F. The following conditions on a monic polynomial f with coefficients in F are equivalent. The unique monic polynomial that satisfies these confitions is called the *irreducible polynomial for α over F.*

- f is the monic polynomial of lowest degree in $F[x]$ that has α as a root.
- f is an irreducible element of $F[x]$ and α is a root of f.
- f has coefficients in F, α is a root of f, and the principal ideal of $F[x]$ that is generated by f is a maximal ideal.
- α is a root of f and if g is any polynomial in $F[x]$ that has α as a root, then f divides g.

The degree of the irreducible polynomial for α over F is called the *degree of α over F.*

Note that, calling a polynomial irreducible is only sensible when the associated field or ring of coefficients is specified. And when it is, we say that the polynomial f is *irreducible over F*.

Let F be a sub field of the field K. Let $\alpha \in K$. We define $F(\alpha)$ as:

$$F(\alpha) \text{ is the smallest subfield of } K \text{ that contains } F \text{ and } \alpha \tag{36}$$

Similarly if $\alpha_1, \alpha_2 \ldots \alpha_n$ are elements of the extension field K, the notation $F(\alpha_1, \alpha_2 \ldots \alpha_n)$ stands for the smallest subfield of K that contains F and these elements. We denote the ring generated by α over F by $F[\alpha]$. It is the image of the substitution homomorphism $\varphi : F[x] \to K$ defined by $x \rightsquigarrow \alpha$, which consists of the elements β of K that can be expressed as polynomials in α with coefficients in F:

$$\beta = b_n\alpha^n + b_{n-1}\alpha^{n-1} + \ldots b_1\alpha + b_0, \text{with } b_i \in F \tag{37}$$

Again, if $\alpha_1, \alpha_2 \ldots \alpha_n$ are elements of K, the smallest subring of K that contains F, and these elements is denoted by $F[\alpha_1, \alpha_2 \ldots \alpha_n]$. It contains of elements of K that can be expressed as polynomials in the α_i with coefficients in F. The field $F(\alpha_1, \alpha_2 \ldots \alpha_n)$ is the field of fractions of the ring $F[\alpha_1, \alpha_2 \ldots \alpha_n]$. The field $F(\alpha)$ is isomorphic to the field of fractions of $F[\alpha]$.

We see that if $\alpha \in K$ is transcedental over F if φ defined above is injective (why?), and algebraic over F if φ is not injective. Further we see that if α is transcedental over F, the map $F[x] \to F[\alpha]$ is an isomorphism.

Proposition 7.2.2. Let α be an element of an extension field K/F which is algebraic over F, and let f be the irreducible polynomial for α over F.

1. The canonical map $F[x]/(f) \to F[\alpha]$ is an isomorphism, and $F[\alpha]$ is a field. Thus, $F[\alpha] = F(\alpha)$
2. More generally, let $\alpha_1, \alpha_2 \ldots \alpha_n$ be the elements of an extension field K/F which are algebraic over F. The ring $F[\alpha_1, \alpha_2 \ldots \alpha_n]$ is equal to the field $F(\alpha_1, \alpha_2 \ldots \alpha_n)$

Proof:

1. Let $\varphi : F[x] \to K$ be the substitution map we referred to earlier. Since the ideal (f) is maximal, $f(x)$ generates the kernel, and $F[x]/(f)$ is isomorphic to the image of φ, which is $F[\alpha]$. Moreover, $F[x]/(f)$ is a field, and thus $F[\alpha]$ is a field. Since $F(\alpha)$ is the fraction field of $F[\alpha]$, it is equal to $F[\alpha]$.
2. This can be proved by induction on the number of α_i's. The case for $i = 1$ is clear. We assume the proposition to hold true for $\alpha_1, \alpha_2 \ldots \alpha_{k-1}$. Thus, $F[\alpha_1, \alpha_2 \ldots \alpha_{k-1}] = F(\alpha_1, \alpha_2 \ldots \alpha_{k-1})$. Now, $F[\alpha_1, \alpha_2 \ldots \alpha_k] = F[\alpha_1, \alpha_2 \ldots \alpha_{k-1}][F_k] = F(\alpha_1, \alpha_2 \ldots \alpha_{k-1})[\alpha_k] = F(\alpha_1, \alpha_2 \ldots \alpha_k)$

References

[1] Algebra (Second Edition) - Michael Artin

[2] Abstract Algebra - Dummit and Foote