Abstract Algebra by Dummit and Foote

Henry Yan

November 2023

Notes

Any injective or bijective map (either or suffices) from a set of n elements to another set of n elements is necessarily bijective.

All cyclic groups are Abelian, but an Abelian group is not necessarily cyclic.

For some element $a \in A$, $\overline{a}$ is the equivalence class of a.

The go-to method for proving equality of sets is inclusion in both directions.

Basics and Groups

Definition 1.4 - Image/Range: Let S and T be two sets, and let $f : S \to T$ be a map. We define the *image* (also known as *range*) of f to be:

$$\text{Im}(f) := \{y \in T | \exists x \in S \text{ such that } f(x) = y\}.$$

Definition 1.5 - Preimage: Let $f : S \to T$, and suppose $U \subseteq T$. Then we define the *preimage* of U under f to be

$$f^{-1}(U) := \{s \in S | f(s) \in U\}.$$

Definition 1.13 - Equivalence Relation: An *equivalence relation* on a set S is a subset $U \subseteq S \times S$ satisfying:

1. Reflexive: $\forall x \in S, (x, x) \in U$
2. Symmetric: $(x, y) \in U \iff (y, x) \in U$
3. Transitive: Given $x, y, z \in S$, $(x, y) \in U$ and $(y, z) \in U \implies (x, z) \in U$.

We often write $x \sim y$ to mean that x, y are equivalent.

Definition 1.14 - Equivalence Class. Let $\sim$ be an equivalence relation on the set S. Let $x \in S$. The *equivalence class* containing x is the subset

$$[x] := \{y \in S | y \sim x\} \subset S.$$

Definition 1.16 - Partition: Let S be a set. Let $\{X_i\}$ be a collection of subsets for $i \in I$, some index set. We say that $\{X_i\}$ forms a *partition* of S if each X_i is non-empty, they are pairwise disjoint and their union is S.

3. Groups

Definition - Group: A group is a set G, together with a binary operation $*$, such that the following hold:

1. (Associativity): $(a * b) * c = a * (b * c)$, $\forall a, b, c \in G$.
2. (Existence of identity): $\exists e \in G$ such that $a * e = e * a = a$, $\forall a \in G$.
3. (Existence of inverses): Given $a \in G, \exists b \in G$ such that $a * b = b * a = e$.

We define a **direct product** of groups for two groups A, B by $A \times B = \{(a, b) | a \in A, b \in B\}$, and $(a_1, b_1)(a_2, b_2) = (a_1 a_2, b_1 b_2)$. Then $A \times B$ also forms a group.

Definition - Abelian. A group $(G, *)$ is called *Abelian* if it satisfies

$$a * b = b * a, \forall a, b \in G.$$

This is also called the *commutative property*.

Definition - Order of an Element: For G a group and $x \in G$ define the order of x to be the smallest positive integer n such that $x^n = 1$, and denote this integer by $|x|$. In this case x is said to be of **order** n. If no positive power of x is the identity, the order of x is defined to be infinity and x is said to be of **infinite order**.

Definition - Homomorphism: Let $(G, *)$ and $(H, \circ)$ be two groups. A *homomorphism* f, from G to H, is a map of sets $f : G \to H$, such that $f(x * y) = f(x) \circ f(y)$, $\forall x, y \in G$. If $G = H$ and $f = Id_G$ we call f the *identity homomorphism.*

Definition - Isomorphism: A homomorphism $f : G \to H$ which is bijective is called an *isomorphism.* Two groups are said to be isomorphic if there exists an isomorphism between them.

Definition - Endomorphism/Automorphism: A homomorphism from a group to itself (i.e. $f : G \to G$) is called an *endomorphism.* An endomorphism which is also an isomorphism is called an *automorphism.*

Proposition 3.6/3.7/3.8:

3.6. Identity is unique.

3.7. Inverses are unique.

3.8. For $x, y \in G$, $(x * y)^{-1} = y^{-1} * x^{-1}$.

Proposition 3.9 - Homomorphism Facts: Let $(G, *)$ and $(H, \circ)$ be two groups with identities, e_G and e_H, respectively, and $f : G \to H$ a homomorphism.

1. $f(e_G) = e_H$,
2. $f(x^{-1}) = (f(x))^{-1}, \forall x \in G$.

Definition - Subgroup. Let $(G, *)$ be a group. A subgroup of G is a subset $H \subset G$ such that

1. $e \in H$,
2. $x, y \in H \implies x * y \in H$,
3. $x \in H \iff x^{-1} \in H$.

Proposition Let $H, K \subset G$ be subgroups, then $H \cap K \subset G$ is a also subgroup of G.

Definition: Let $(G, *)$ be a group and let $H \subset G$ be a subgroup. Let us define a relation on G using H as follows: given $x, y \in G$,

$$x \sim y \iff x^{-1} * y \in H.$$

Definition - Left Coset: The equivalence class, or *left coset*, containing x equals

$$xH := \{x * h | h \in H\} \subset G.$$

Corollary 3.15: Hence for $x, y \in G, xH = yH \iff x^{-1} * y \in H$.

An immediate consequence of Corollary 3.15 is that if $y \in xH$, then $yH = xH$. Thus left cosets can generally be written with different representations in front.

Definition 3.17 - Index. Let $(G, *)$ be a group and $H \subset G$ a subgroup. We denote by G/H the set of left cosets of H in G. If the size of this set is finite then we say that H has *finite index* in G. In this case we write

$$(G : H) = |G/H|,$$

and call it the *index* of H in G.

Lagrange's Theorem: Let $(G, *)$ be a finite group and $H \subset G$ a subgroup. Then $|H|$ divides $|G|$.

Definition - Group of Permutations: Let $\Sigma(s)$ denote the group of permutations of a set S.

Definition - Dihedral Group: Let D_{2n} represent the symmetries of an n-gon as a result of actions on the object in 3 dimensions. $|D_{2n}| = 2n$, and $D_{2n} = \langle r, s | r^n = s^2 = 1, rs = sr^{-1} \rangle$.

Definition - Generators: A subset S of elements of a group G with the property that every element of G can be written as a (finite) product of elements of S and their inverses is called a set of *generators* of G. We shall indicate this notationally by writing $G = \langle S \rangle$ and say G *is generated by* S or S *generates* G. Any equations that the generators must satisfy in G are called **relations**. A **presentation** of $G = D_{2n}$ is $D_{2n} = \langle r, s | r^n = s^2 = 1, rs = sr^{-1} \rangle$.

The **symmetric group** S_Ω is denotes the set of all bijections (permutations) from Ω to itself.

S_n defines the symmetric group of degree n, where the set of elements is $\{1, 2, \ldots, n\}$ and $|S_n| = n!$.

S_n is non-Abelian for all $n \geq 3$.

Disjoint cycles commute.

Definition - Field:

1. A *field* is set F with two binary operations $+$ and $\cdot$ on F such that $(F, +)$ is an Abelian group, with identity 0, and $(F - \{0\}, \cdot)$ is also an Abelian group, and the following *distribute* law holds:

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c), \text{ for all } a, b, c \in F.$$

2. For any field F let $F^\times = F - \{0\}$.

Let $GL_n(F)$ be the set of all $n \times n$ matrices whose entries come from F and whose determinant is non-zero. $GL_n(F)$ is called the **general linear group of degree** n.

Theorems at the end of 1.4:

1. If F is a field and $|F| < \infty$, then $|F| = p^m$ for some prime p and integer m,
2. if $|F| = q < \infty$, then $|GL_n(F)| = (q^n - 1)(q^n - q)\dots(q^n - q^{n-1})$.

Definition - Quaternion Group: The *Quaternion group*, Q_8, is defined by

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$$

with product $\cdot$ computed as follows:

1. $1 \cdot a = a \cdot 1 = a$, for all $a \in Q_8$
2. $(-1) \cdot (-1) = 1, (-1) \cdot a = a \cdot (-1) = -a$
3. $i \cdot i = j \cdot j = k \cdot k = -1$
4. $i \cdot j = k, j \cdot i = -k$
5. $j \cdot k = i, k \cdot j = -i$
6. $k \cdot i = j, i \cdot k = -j$

$Q_8 = \langle i, j | i^4 = 1, j^2 = i^2, ji = ij^{-1} \rangle$.

For an isomorphism $\varphi : G \to H$, we have the following properties:

1. $|G| = |H|$.
2. G is Abelian iff H is Abelian.
3. For all $x \in G$, $|x| = |\varphi(x)|$.
4. If we have a presentation for $G = \langle s_1, s_2, \dots, s_n \rangle$, then H is generated by $\langle r_1, r_2, \dots, r_n \rangle = \langle \varphi(s_1), \varphi(s_2), \dots, \varphi(s_n) \rangle$, and the relations among the s_i's hold similarly for the r_i's (since s_i's are elements of G).

Definition - Group Action: A *group action* of a group G on a set A is a map from $G \times A \to A$ satisfying the following properties:

1. $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$, for all $g_1, g_2 \in G, a \in A$,
2. $1 \cdot a = a$, for all $a \in A$

Alternatively, we say that G is a group acting on a set A.

Define $\sigma_g : A \to A, \sigma_g(a) = g \cdot a$, then there are 2 important facts

1. for each fixed $g \in G, \sigma_g$ is a permutation of A, and
2. the map $\varphi : G \to S_A$ defined by $\varphi(g) = \sigma_g$ is a homomorphism. φ is called the *permutation representation* associated to the given action.

In particular, this could be called a left action, as a right action could be defined similarly.

The action defined by $ga = a, \forall g \in G, a \in A$, is called the *trivial action* and G is said to *act trivially* on A.

If G acts on A and each element of G induce different permutations of A, then the action is said to be *faithful*, i.e. injective.

The *kernel* of the action G on A is defined to be $\{g \in G | ga = a, \forall a \in A\}$, namely the elements of G which fix all the elements of A. The kernel of the trivial action is all of G.

Definition - Subgroup: Let G be a group. The subset H of G is a *subgroup* of G if H is nonempty and H is closed under products and inverses (i.e., $x, y \in H$ implies $x^{-1} \in H$ and $xy \in H$). If H is a subgroup of G we shall write $H \leq G$. If $H \neq G$, then we may write $H < G$ to signify a proper subgroup.

The *trivial subgroup* refers to a subgroup which contains only the identity element.

If $C \leq B$, and $B \leq A$, then we have that $C \leq A$, or C is a subgroup of A. This property is called *transitivity*.

Proposition 2.1 (Subgroup Criterion): A subset H of a group G is a subgroup if and only if

1. $H \neq \emptyset$, and
2. for all $x, y \in H, xy^{-1} \in H$.

Definition - Centralizers: Define $C_G(A) = \{g \in G | gag^{-1} = a, \forall a \in A\}$. This subset of G is called the *centralizer* of A in G. Since $gag^{-1} = a$ iff $ga = ag, C_G(A)$ is the set of elements of G which commute with every element of A.

The center of any group G is a subset of the centralizer of any subset A in G.

Definition - Center: Define $Z(G) = \{g \in G | gx = xg, \forall x \in G\}$ as the set of elements commuting with all elements of G. This subset of G is called the *center* of G.

Definition - Normalizer: Define the *normalizer* of A in G to be $N_G(A) = \{g \in G | gAg^{-1} = A\}$.

By definition, $C_G(A) \leq N_G(A)$.

Each of centralizers, center, and normalizer form subgroups of G.

Definition - Stabilizer: If a group G is acting on a set S, for a fixed element $s \in S$, we define the *stabilizer* of s in G as

$$G_s = \{g \in G | g \cdot s = s\}.$$

The stabilizer also forms a subgroup of G.

Definition - Kernel of a Group Action: The *kernel* of an action G on S is defined as $\ker(G) = \{g \in G | g \cdot s = s, \forall s \in S\}$.

Definition - Cyclic: A group H is cyclic if H can be generated by a single element, i.e., $H = \{x^n | n \in \mathbb{Z}\}$, where the usual operation is shorted-handed as multiplication (powers of x).

In additive notation we may write that $H = \{nx | n \in \mathbb{Z}\}$. In either case we write that $H = \langle x \rangle$ and say that H is generated by x, or x is a generator of H.

Proposition 2.2: If $H = \langle x \rangle$, then $|H| = |x|$ (where if one side of the equality is infinite then so is the other). More specifically,

1. if $|H| = n < \infty$, then $x^n = 1$ and $1, x, \ldots, x^{n-1}$ are all distinct elements of H, and
2. if $|H| = \infty$, then $x^n = 1 \iff n = 0$ and $x^a \neq x^b$ for all $a \neq b$ in $\mathbb{Z}$.

Theorem 2.4: Any two cyclic groups of the same order are isomorphic. More specifically,

1. if $n \in \mathbb{Z}^+$ and $\langle x \rangle$ and $\langle y \rangle$ are both cyclic groups of order n, then the map
$$\begin{aligned} \varphi : \langle x \rangle &\to \langle y \rangle \\ x^k &\mapsto y^k \end{aligned}$$
is well defined and is an isomorphism.
2. if $\langle x \rangle$ is an infinite cyclic group, the map
$$\begin{aligned} \varphi : \mathbb{Z} &\to \langle x \rangle \\ k &\mapsto x^k \end{aligned}$$
is well defined and is an isomorphism.

For each $n \in \mathbb{Z}^+$, let Z_n denote the cyclic group of order n, written multiplicatively. Note that up to isomorphism, $Z_n \cong \mathbb{Z}/n\mathbb{Z}$ is the unique cyclic group of order n. Similarly, $\mathbb{Z}$ (additively) will be used to denote the infinite cyclic group.

Proposition 2.5: Let G be a group, $x \in G$, and let $a \in \mathbb{Z} - \{0\}$.

1. If $|x| = \infty$, then $|x^a| = \infty$.
2. If $|x| = n < \infty$, then $|x^a| = \dfrac{n}{(n,a)}$, where (n, a) is the GCD of n and a.
3. In particular, if $|x| = n < \infty$ and a is a positive integer dividing n, then $|x^a| = \dfrac{n}{a}$.

Proposition 2.6: Let $H = \langle x \rangle$.

1. Assume $|x| = \infty$, then $H = \langle x^a \rangle$ iff $a = \pm 1$.
2. Assume $|x| = n < \infty$, then $H = \langle x^a \rangle$ iff $(a, n) = 1$. In particular, the number of generators of H is $\varphi(n)$, where φ is Euler's Totient function.

Theorem 2.7: Let $H = \langle x \rangle$ be a cyclic group.

1. Every subgroup of H is cyclic. More precisely, if $K \leq H$, then $K = \{1\}$ or $K = \langle x^d \rangle$.
2. If $|H| = \infty$, then for any distinct nonnegative integers a and b, $\langle x^a \rangle \neq \langle x^b \rangle$. Furthermore, for every integer m, $\langle x^m \rangle = \langle x^{|m|} \rangle$.
3. If $|H| = n$, then for each positive integer a dividing n there is a unique subgroup of H of order a. This is the subgroup $\langle x^d \rangle$, where $d = n/a$. Furthermore, for every integer m, $\langle x^m \rangle = \langle x^{(n,m)} \rangle$ so that the subgroups of H correspond bijectively with the positive divisors of n.

For any subgroup $H \leq G$ which contains the element x, $\langle x \rangle$ is contained within H. As the inclusion of $\langle x \rangle$ simply ensures that the axioms of closure and inverse exist within H, for the given element x.

Definition - Subgroup Generated by a Subset: If A is any subset of the group G, define

$$\langle A \rangle = \bigcap_{\substack{A \subseteq H \\ H \leq G}} H$$

to be the *subgroup of G generated by A*.

For multiple subsets $A, B \subseteq G$, we write $\langle A, B \rangle = \langle A \cup B \rangle$.

Definition - Words: Let

$$\overline{A} = \{a_1^{\epsilon_1} a_2^{\epsilon_2} \ldots a_n^{\epsilon_n} | n \in \mathbb{Z}, n \geq 0 \text{ and } a_i \in A, \epsilon_i = \pm 1 \text{ for each } i\},$$

where $\overline{A} = \{1\}$ if $A = \emptyset$. This is called the *words*, or the set of all finite products of A and inverses of elements of A. Note that each of the a_i's in the definition are not necessarily distinct.

Proposition 2.9: $\overline{A} = \langle A \rangle$.

Another way of writing

$$\langle A \rangle = \{a_1^{\alpha_1} a_2^{\alpha_2} \ldots a_n^{\alpha_n} | \text{ for each } i, a_i \in A, \alpha_i = \mathbb{Z}, a_i \neq a_{i+1} \text{ and } n \in \mathbb{Z}^+\}.$$

If G is Abelian, then

$$\langle A \rangle = \{a_1^{\alpha_1} a_2^{\alpha_2} \ldots a_n^{\alpha_n} | \alpha_i \in \mathbb{Z} \text{ for each } i\}.$$

Definition - Lattice: A lattice of a group G is essentially a graph with G at the top, and 1 at the bottom, with subgroups of increasing order as you go up. Any two subgroups A, B of G are connected via a line upwards if $B \leq A$.

Definition - Join: Given subgroups $H, K \leq G$, we define the join of H and K $\langle H, K \rangle$ as the "smallest" subgroup containing both H and K.

A similar concept for the largest subgroup contained within two subgroups A, B is $A \cap B$, which is necessarily a subgroup by proposition 2.8.

Definition - Fiber: For a homomorphism $\varphi : G \to H$, the *fibers* of φ are the sets of elements of G projecting to single elements of H. This can be viewed as the inverse of a homomorphism, i.e. the fiber of some element $h \in H$ is $\{g \in G | \varphi(g) = h\}$. We would call this the fiber above h.

For fibers X_a, X_b, we define $X_{ab} = X_a X_b$.

The set of fibers forms a group.

Quotient Groups and Homomorphisms

Definition - Kernel: For a homomorphism $\varphi : G \to H$, the kernel of φ is

$$\ker \varphi = \{g \in G | \varphi(g) = 1_H\}.$$

Proposition 3.1: For a homomorphism $\varphi : G \to H$,

1. $\varphi(1_G) = 1_H$.
2. $\varphi(g^{-1}) = \varphi(g)^{-1}$
3. $\varphi(g^n) = \varphi(g)^n$, for all $n \in \mathbb{Z}$.
4. $\ker \varphi$ is a subgroup of G.
5. $\operatorname{Im} \varphi$ forms a subgroup of H.

Definition - Quotient Group: Let $\varphi : G \to H$ be a homomorphism with kernel K. The *quotient group*, or factor group, $G/K = \overline{G}$ (read G *modulo* K or G *mod* k), is the group whose elements are the fiber of φ with group operation defined above: namely if X is the fiber above a and Y is the fiber above b then the product of X and Y is defined to be the fiber of above the product ab.

Proposition 3.2: Let $\varphi : G \to H$ be a homomorphism with kernel K. Let $X \in G/K$ be the fiber above a, i.e., $X = \varphi^{-1}(a)$. Then

1. for any $u \in X$, $X = \{uk | k \in K\}$, and similarly
2. for any $u \in X$, $X = \{ku | k \in K\}$.

Then this proposition is basically stating that a fiber over some element can basically be defined as a "shifting" of a **representative**[1] of that fiber by the kernel set. An easy example of this would be some homomorphism $\varphi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, which would have $1, 1 \pm n, 1 \pm 2n, \ldots$ as the fiber for the element $1 \in \mathbb{Z}/n\mathbb{Z}$, or that the fiber of 1 is just any preimage of 1 under φ shifted by some $kn, k \in \mathbb{Z}$, as $kn \equiv 0 \pmod{n}$, where 0 is the identity representative in the additive group.

Definition - Left and Right Cosets: For any $N \leq G$ and any $g \in G$, the left and right cosets of N in G are defined as

$$gN = \{gn | n \in N\} \text{ and } Ng = \{ng | n \in N\},$$

respectively. An element of a coset is called a *representative* for the coset.

For additive groups we may instead write $g + N$ or $N + g$.

Theorem 3.3: Let G be a group and let K be the kernel of some homomorphism from G to another group. Then the set whose elements are the left cosets of K in G with operation defined by

$$uK \circ vK = (uv)K$$

forms a group G/K. This statement also holds for right coset.

In simpler terms, theorem 3 is essentially stating that modding out by the kernel is equivalent to reducing the group to left (or right) cosets of it's kernel with the operation defined above.

Proposition 3.4: Let N be any subgroup of the group G. The set of left cosets of N in G form a partition of G. Furthermore, for all $u, v \in G, uN = vN$ if and only if $v^{-1}u \in N$ and in particular, $uN = vN$ if and only if u and v are representatives of the same coset.

Proposition 3.5: Let G be a group and let N be a subgroup of G.

1. The operation on the set of left cosets of N in G described by

$$uN \cdot vN = (uv)N$$

is well defined iff $gng^{-1} \in N$ for all $g \in G$ and $n \in N$.

[1] A *representative* is an element of a equivalence class used to *represent* all the elements in that equivalence class.

2. If the above operation is well defined, then it makes the set of left cosets of N in G into a group. In particular the identity of this group is the coset $1N$ and the inverse of gN is the coset $g^{-1}N$, i.e., $(gN)^{-1} = g^{-1}N$.

This proposition is essentially an extension of theorem 3 (in that G/K forms a group) to all subgroups N rather than just the kernel.

Definition - Conjugate, Normal: The element gng^{-1} is called the *conjugate of* $n \in N$ *by* g. The set $gNg^{-1} = \{gng^{-1} | n \in N\}$ is called the *conjugate of* N *by* g. The element g is said to *normalize* N if $gNg^{-1} = N$. A subgroup N of a group G is called *normal* if every element of G normalizes N, i.e., if $gNg^{-1} = N$ for all $g \in G$. If N is a normal subgroup of G we shall write $N \trianglelefteq G$. It is important to remember that normality is a embedding property, i.e. N being normal depends on the group G of which it is a subgroup.

Theorem 6: Let N be a subgroup of the group G. The following are equivalent:

1. $N \trianglelefteq G$,
2. $N_G(N) = G$ (recall $N_G(N)$ is the normalizer of N in G),
3. $gN = Ng$, for all $g \in G$,
4. the operation on left cosets of N in G described in proposition 5 makes the set of left cosets into a group,
5. $gNg^{-1} \subseteq N$ for all $g \in G$.

If a subgroup $H \leq G$ of some order is the unique subgroup of that order, then $H \trianglelefteq G$.

Proposition 3.7: A subgroup N of the group G is normal if and only if it is the kernel of some homomorphism.

For $N \trianglelefteq G$, $gN = N$ iff $g \in N$.

Definition - Natural Projection, Complete Preimage: Let $N \trianglelefteq G$. The homomorphism $\pi : G \to G/N$ defined by $\pi(g) = gN$ is called the *natural projection* (homomorphism) of G onto G/N. If $\overline{H} \leq G/N$ is a subgroup of G/N, the *complete preimage* of $\overline{H}$ in G is the preimage of $\overline{H}$ under the natural projection homomorphism.

Then given $N \trianglelefteq G$, $\ker \pi = N$.

Quotient groups of a cyclic group are cyclic.

Theorem 3.8 - Lagrange's Theorem: If G is a finite group and H is a subgroup of G, then the order of H divides the order of G and the number of left cosets of H in G is $\dfrac{|G|}{|H|}$.

Definition - Index: If G is a group and $H \leq G$, the number of left cosets of H in G is called the index of H in G and is denoted by $|G : H|$.

In the case of finite groups $|G : H| = |G|/|H|$.

Corollary 3.9: If G is a finite group and $x \in G$, then the order of x divides the order of G. In particular, $x^{|G|} = 1_G$, for all $x \in G$.

Corollary 3.10: If G is of prime order p, then G is cyclic and $G \cong Z_p$.

Theorem 3.11/Proposition 3.21 - Cauchy's Theorem: If G is a finite group and p is a prime dividing $|G|$, then G has an element of order p.

Theorem 3.12 - Sylow: If G is a finite group of order $p^\alpha m$, where p is a prime and $p \nmid m$, then G has a subgroup of order p^α.

Definition - Multiplication of Subgroups: Let H, K be subgroups of a group and define

$$HK = \{hk | h \in H, k \in K\}.$$

Proposition 3.13: If H, K are finite subgroups of a group then

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Proposition 3.14: If H, K are subgroups of a group, HK is a subgroup iff $HK = KH$.

One should be careful not to misinterpret 3.14 to mean that the subgroup HK is Abelian, rather that $hk = k'h'$.

Corollary 3.15: If H, K are subgroups of G and $H \leq N_G(K)$, then HK is a subgroup of G. In particular, if $K \trianglelefteq G$, then $HK \leq G$ (HK is a subgroup) for any $H \leq G$.

Definition - Normalizes: If A is any subset of $N_G(K)$ (or $C_G(K)$), we shall say that A *normalizes* K (or *centralizes*, respectively).

Theorem 3.16 - The First Isomorphism Theorem: If $\varphi : G \to H$ is a homomorphism of groups, then $\ker \varphi \trianglelefteq G$ and $G/\ker \varphi \cong \varphi(G)$.

Another way to interpret theorem 3.16 is that for any homomorphism $\varphi : G \to H$, there exists a injective group homomorphism $\overline{\varphi} : G/\ker \varphi \to H$.

Corollary 3.17: Let $\varphi : G \to H$ is a homomorphism of groups.

1. φ is injective iff $\ker \varphi = 1$.
2. $|G : \ker \varphi| = |\varphi(G)|$.

Theorem 3.18 - The Second/Diamond Isomorphism Theorem: Let G be a group and $A, B \leq G$ and assume $A \leq N_G(B)$. Then AB is a subgroup of G, $B \trianglelefteq AB, A \cap B \trianglelefteq A, AB/B \cong A/A \cap B$.

Theorem 3.19 - The Third Isomorphism Theorem: Let G be a group and let H, K be normal subgroups of G with $H \leq K$. Then $K/H \trianglelefteq G/H$ and

$$(G/H)/(K/H) \cong G/K.$$

Theorem 3.20 - The Fourth/Lattice Isomorphism Theorem: Let G be a group and let N be a normal subgroup of G. Then there is a bijection from the set of subgroups A of G which contain N onto the set of subgroups $\overline{A} = A/N$ of G/N. In particular, every subgroup of $\overline{G}$ is of the form A/N for some subgroup A of G containing N (namely, it's preimage in G under the projection homomorphism from G to G/N). This bijection has the following properties: for all $A, B \leq G$ with $N \leq A, B$,

1. $A \leq B$ iff $\overline{A} \leq \overline{B}$,
2. if $A \leq B$, then $|B : A| = |\overline{B} : \overline{A}|$,

3. $\overline{\langle A, B\rangle} = \langle \overline{A}, \overline{B}\rangle$,
4. $\overline{A \cap B} = \overline{A} \cap \overline{B}$,
5. $A \trianglelefteq G$ iff $\overline{A} \trianglelefteq \overline{G}$.

Definition - Simple: A (finite or infinite) group G is called *simple* if $|G| > 1$ and the only normal subgroups of G are 1 and G.

If $|G|$ is prime, then it's only subgroups are 1 and G, and is thus simple. In fact, every simple Abelian group is isomorphic to Z_p, for some prime p.

Proposition 3.21: If G is a finite abelian group and p is a prime dividing $|G|$, then G contains an element of order p.

Definition - Composition Series: In a group G a sequence of subgroups

$$1 = N_0 \leq N_1 \leq \cdots \leq N_{k-1} \leq N_k = G$$

is called a *composition series* if $N_i \trianglelefteq N_{i+1}$ and N_{i+1}/N_i is a simple group, $0 \leq i \leq k-1$. If the above sequence is a composition series, the quotient groups N_{i+1}/N_i are called *composition factors* of G.

Theorem 3.22 - Jordan-Hölder Theorem: Let G be a finite group with $G \neq 1$. Then

1. G has a composition series and
2. The composition factors in a composition series are unique, namely, if $1 = N_0 \leq N_1 \leq \cdots \leq N_r = G$ and $1 = M_0 \leq M_1 \leq \cdots \leq M_s = G$ are two composition series for G, then $r = s$ and there is some permutation π of $\{1, 2, \ldots, r\}$ such that

$$M_{\pi(i)}/M_{\pi(i)-1} \cong N_i/N_{i-1}, 1 \leq i \leq r.$$

In other words, a composition series of a finite group G is essentially a factorization of G. Unlike factorizing integers, however, the series itself need not be unique, but the number of composition factors and their isomorphism types are uniquely determined.

The Hölder Program:

1. Classify all finite simple groups.
2. Find all ways of "putting simple groups together" to form other groups (sometimes called the *Extension Problem*)

Definition - Transposition: A 2-cycle is called a *transposition*.

Every element of S_n can be written as a product of transpositions, though not uniquely.

Definition - Sign of a Permutation: Define $\Delta = \prod_{1 \leq i < j \leq n}(x_i - x_j)$ and $\sigma(\Delta) = \prod_{1 \leq i < j \leq n}(x_{\sigma(i)} - x_{\sigma(j)})$. Then it is clear that $\sigma(\Delta) = \pm\Delta$ for all $\sigma \in S_n$. Define $\epsilon(\sigma)$, the *sign* of σ, by

$$\epsilon(\sigma) = \begin{cases} +1, & \text{if } \sigma(\Delta) = \Delta \\ -1, & \text{if } \sigma(\Delta) = -\Delta \end{cases}.$$

We say that σ is an *even permutation* if $\epsilon(\sigma) = +1$ or *odd permutation* if $\epsilon(\sigma) = -1$.

Proposition 3.23: The map $\epsilon : S_n \to \{\pm 1\}$ is a homomorphism (where $\{\pm 1\}$ is a multiplicative version of the cyclic group of order 2). This proposition basically just tells you that composing two even/odd permutations results in an even permutation, and composing an even and an odd permutation results in an odd permutation.

Proposition 3.24: Transpositions are all odd permutations and ϵ is a surjective homomorphism.

Definition - Alternating Group: The *alternating group of degree* n, denoted by A_n, is the kernel of the homomorphism ϵ (i.e., the set of even permutations).

$|A_n| = \frac{n!}{2}$.

Using the fact that an m-cycle can be written as a product of $m-1$ transpositions, an m-cycle is an odd permutation iff m is even.

Proposition 3.25: The permutation σ is odd iff the number of cycles of even length in its cycle decomposition is odd.

Chapter 4 - Group Actions

Definition - Group Action: A *group action* of a group G on a set A is a map from $G \times A \to A$ satisfying the following properties:

1. *Compatibility*: $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$, for all $g_1, g_2 \in G, a \in A$,
2. *Identity*: $1 \cdot a = a$, for all $a \in A$

Definition - Permutation Representation: Define $\sigma_g : A \to A$ by $\sigma_g : a \mapsto g \cdot a$ and $\varphi : G \to S_A$ by $\varphi(g) = \sigma_g$. φ is called the *permutation representation* associated to the given action.

Definition - Stabilizer: If a group G is acting on a set A, for a fixed element $a \in A$, we define the *stabilizer* of a in G as

$$G_a = \{g \in G | g \cdot a = a\}.$$

The stabilizer of any element a forms a subgroup of G.

Definition - Kernel of a Group Action: The *kernel* of an action G on A is defined as

$$\ker(G) = \{g \in G | g \cdot a = a, \forall a \in A\} = \bigcap_{a \in A} G_a.$$

Definition - Faithful: If G acts on A and each element of G induce different permutations of A, then the action is said to be *faithful*, i.e. injective. An action is faithful if it's kernel is the identity.

An action of G on A can be equivalently viewed as a faithful action of $G/\ker\varphi$ on A.

Proposition 4.1: For any group G and any nonempty set A there is a bijection between the actions of G on A and the homomorphisms of G into S_A.

4.1 can be realized by defining an action G on A by $g \cdot a = \varphi(g)(a)$, where φ is the permutation representation of the action G.

Definition - Induce: If G is a group, a *permutation representation* of G is any homomorphism of G into the symmetric group S_A for some nonempty set A. We shall say a given action of G on A *affords* or *induces* the associated permutation representation of G.

Proposition 4.2: Let G be a group acting on the nonempty set A. The relation on A defined by

$$a \sim b \text{ iff } a = g \cdot b \text{ for some } g \in G$$

is an equivalence relation. For each $a \in A$, the number of elements in the equivalence class containing a is $|G : G_a|$, the index of the stabilizer of a.

Definition - Orbit, Transitive: Let G be a group acting on the nonempty set A.

1. The equivalence class $\{g \cdot a | g \in G\}$ is called the *orbit* of G containing a.
2. The action of G on A is called *transitive* if there is only one orbit, i.e., given any two elements $a, b \in A$ there is some $g \in G$ such that $a = g \cdot b$.

Subgroups of symmetric groups are called *permutation groups*.

Any group action of a group G acting on itself can be given a permutation representation $\sigma_g \in S_n$, for every $g \in G$, by labeling the elements of G as $\{g_1, g_2, \dots, g_n\}$, where the identity permutation corresponds to $g = 1$. The same can be done on left cosets of some subgroup $H \leq G$. This form of representing a group action is useful because $\sigma_{sr^2} = \sigma_s \sigma_r^2$.

The action of a group on itself by left multiplication is always transitive and faithful, and the stabilizer of any point is the identity subgroup.

Theorem 4.3: Let G be a group, let H be a subgroup of G and let G act by left multiplication on the set A of left cosets of H in G. Let π_H be the associated permutation representation afforded by this action. Then

1. G acts transitively on A
2. the stabilizer in G of the point $1H \in A$ is the subgroup H
3. the kernel of the action (i.e., the kernel of π_H) is $\cap_{x \in G} x H x^{-1}$, and $\ker \pi_H$ is the largest normal subgroup of G contained in H.

Corollary 4.4 - Cayley's Theorem: Every group is isomorphic to a subgroup of some symmetric group. If G is a group of order n, then G is isomorphic to a subgroup of S_n (permutation group).

Corollary 4.5: If G is a finite group of order n and p is the smallest prime dividing n, then any subgroup of index p is normal.

A group acting on itself by conjugating is a group G acting on a set G by

$$g \cdot a = gag^{-1}, \text{ for all } g \in G, a \in G$$

where gag^{-1} is computed in the group G.

Definition - Conjugate, Conjugacy Classes: Two elements $a, b \in G$ are said to be *conjugate* in G if there is some $g \in G$ such that $b = gag^{-1}$ (i.e., if and only if they are in the same orbit of G acting on itself by conjugation). The orbits of G acting on itself by conjugation are called the *conjugacy classes* of G.

G acting on $\mathcal{P}(G)$ is called G acting on it's subsets.

Definition - Conjugate In G: Two subsets S and T of G are said to be *conjugate in G* if there is some $g \in G$ such that $T = gsg^{-1}$ (i.e., if and only if they are in the same orbit of G acting on its subsets by conjugation).

$\{x\}$ is a conjugacy class of size 1 iff $x \in Z(G)$.

Proposition 4.6: The number of conjugates of a subset S in a group G is the index of the normalizer of S, $|G : N_G(S)|$. In particular, the number of conjugates of an element s of G is the index of the centralizer of s, $|G : C_G(s)|$.

Theorem 4.7 - The Class Equation: Let G be a finite group and let $g_1, g_2, \ldots, g_r$ be representatives of the distinct conjugacy classes of G not contained in the center $Z(G)$ of G. Then

$$|G| = |Z(G)| + \sum_{i=1}^{r} |G : C_G(g_i)|.$$

Theorem 4.8: If p is a prime and P is a group of prime power order p^a for some $a \geq 1$, then P has a nontrivial center: $Z(P) \neq 1$.

Corollary 4.9: If $|P| = p^2$ for some prime p, then P is Abelian. More precisely, P is isomorphic to either Z_{p^2} or $Z_P \times Z_P$.

Proposition 4.10: Let σ, τ be elements of the symmetric group S_n and suppose σ has cycle decomposition

$$(a_1 a_2 \ldots a_{k_1})(b_1 b_2 \ldots b_{k_2}) \ldots.$$

Then $\tau\sigma\tau^{-1}$ has cycle decomposition

$$(\tau(a_1)\tau(a_2) \ldots \tau(a_{k_1}))(\tau(b_1)\tau(b_2) \ldots \tau(b_{k_2})) \ldots,$$

that is, $\tau\sigma\tau^{-1}$ is obtained by replacing each entry i in the cycle decomposition for σ by the entry $\tau(i)$.

Definition - Cycle Type, Partition:

1. If $\sigma \in S_n$ is the product of disjoint cycles of lengths $n_1, n_2, ..., n_r$ with $n_1 \leq n_2 \leq \cdots \leq n_r$ (including its 1-cycles) then the integers $n_1, n_2, ..., n_r$ are called the *cycle type* of σ.
2. If $n \in \mathbb{Z}^+$, a *partition* of n is any non-decreasing sequence of positive integers whose sum is n.

Proposition 4.11: Two elements of S_n are conjugate in S_n if and only if they have the same cycle type. The number of conjugacy classes of S_n equals the number of partitions of n.

For an m-cycle $\sigma \in S_n$, $|C_{S_n}(\sigma)| = m \cdot (n-m)!$, as

$$C_{S_n}(\sigma) = \{\sigma^i \tau | 0 \leq i < m, \tau \in S_{n-m}\},$$

where S_{n-m} denotes the subgroup of S_n which fixes all the indices which appear in the m-cycle σ.

Theorem 4.12: A_5 is a simple group.

Define the right conjugation of a by g as

$$a^g = g^{-1} a g, \text{ for all } a, g \in G.$$

Definition - Corresponding Group Actions: *Corresponding group actions* are left and right group actions which do the same thing on different sides of the value they are acting on. In other words, g acts on the left the same way that g^{-1} acts on the right. Orbits are the same for left and right actions.

Definition - Automorphism: Let G be a group. An isomorphism from G onto itself is called an automorphism of G. The set of all *automorphisms* of G is denoted by $\text{Aut}(G)$.

Automorphisms map subgroups to subgroups, as a result of being a homomorphisms.

$\text{Aut}(G)$ forms a group. Note that automorphisms of G are essentially just the elements of G up to permutation, so $\text{Aut}(G) \leq S_G$.

Proposition 4.13: Let H be a normal subgroup of the group G. Then G acts by conjugation on H as automorphisms of H. More specifically, the action of G on H by conjugation is defined for each $g \in G$ by

$$\varphi_g : h \mapsto ghg^{-1}, \text{ for each } h \in H.$$

For each $g \in G$, conjugation by g is an automorphism of H. The permutation representation afforded by this action is a homomorphism of G into $\text{Aut}(H)$ with kernel $C_G(H)$. In particular, $G/C_G(H)$ is isomorphic to a subgroup of $\text{Aut}(H)$.

Note about 4.13: Then the permutation representation of these automorphisms φ_g defined for each $g \in G$ is homomorphism $\psi : G \to S_H$ defined by $\psi(g) = \varphi_g$.

Proposition 13 shows that a group acts by conjugation on a normal subgroup as structure preserving permutations, i.e., as automorphisms.

Corollary 4.14: If K is any subgroup (not necessarily normal) of the group G and $g \in G$, then $K \cong gKg^{-1}$. Conjugate elements and conjugate subgroups have the same order.

Corollary 4.15: For any subgroup H of a group G, the quotient group $N_G(H)/C_G(H)$ is isomorphic to a subgroup of $\text{Aut}(H)$. In particular, $G/Z(G)$ is isomorphic to a subgroup of $\text{Aut}(G)$.

Definition - Inner Automorphism: Let G be a group and let $g \in G$. Conjugation by g is called an *inner automorphism* of G and the subgroup of $\text{Aut}(G)$ consisting of all inner automorphisms is denoted by $\text{Inn}(G)$.

The "subgroup of $\text{Aut}(G)$" referenced in corollary 4.15 (both of them) is $\text{Inn}(G)$.

Definition - Characteristic: A subgroup H of a group G is called *characteristic in* G, denoted $H \operatorname{char} G$, if every automorphism of G maps H to itself, i.e., $\sigma(H) = H$ for all $\sigma \in \text{Aut}(G)$.

Results Concerning Characteristic Subgroups:

1. characteristic subgroups are normal,
2. if H is the unique subgroup of G of a given order, then H is characteristic in G, and
3. if $K \operatorname{char} H$ and $H \trianglelefteq G$, then $K \trianglelefteq G$ (so although "normality" is not a transitive property (i.e., a normal subgroup of a normal subgroup need not be normal, a characteristic subgroup of a normal subgroup is normal).

Then characteristic is a stronger condition than normal.

Proposition 4.16: The automorphism group of the cyclic group of order n is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$, an abelian group of order $\varphi(n)$ (where φ is Euler's function).

Proposition 4.17 (Inc. Elementary Abelian Definition):

1. If p is an odd prime and $n \in \mathbb{Z}^+$, then the automorphism group of the cyclic group of order p is cyclic of order $p-1$. More generally, the automorphism group of the cyclic group of order p^n is cyclic of order $p^{n-1}(p-1)$.
2. For all $n \geq 3$ the automorphism group of the cyclic group of order 2^n is isomorphic to $Z_2 \times Z_{2^{n-2}}$, and in particular is not cyclic but has a cyclic subgroup of index 2.
3. Let p be a prime and let V be an abelian group (written additively) with the property that $pv = 0$ for all $v \in V$. If $|V| = p^n$, then V is an n-dimensional vector space over the field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ called the *elementary abelian group of order* p^n. The automorphisms of V are precisely the non-singular linear transformations from V to itself, that is

$$\operatorname{Aut}(V) \cong GL(V) \cong GL_n(\mathbb{F}_p),$$

where $GL(V)$ is the group of all invertible (non-singular) linear transformations from V to itself.
4. For all $n \neq 6$ we have $\operatorname{Aut}(S_n) = \operatorname{Inn}(S_n) \cong S_n$. For $n = 6$ we have $|\operatorname{Aut}(S_6) : \operatorname{Inn}(S_6)| = 2$.
5. $\operatorname{Aut}(D_8) \cong D_8$ and $\operatorname{Aut}(Q_8) \cong S_4$

The Klein 4-group V_4 is called the elementary abelian group of order 4.

For any prime p, the elementary abelian group of order p^2 is $Z_p \times Z_p$.

Definition - p-Groups, Sylow p-Subgroup: Let G be a group and let p be a prime.

1. A group of order p^a for some $a \geq 1$ is called a *p-group*. Subgroups of G which are p-groups are called *p-subgroups*.
2. If G is a group of order $p^a m$, where $p \nmid m$, then a subgroup of order p^a is called a *Sylow p-subgroup of G*.
3. The set of Sylow p-subgroups of G will be denoted by $\operatorname{Syl}_p(G)$ and the number of Sylow p-subgroups of G will be denoted by $n_p(G)$ (or just n_p when G is clear from the context).

Theorem 4.18 - Sylow's Theorem: Let G be a group of order $p^a m$, where p is a prime not dividing m.

1. Sylow p-subgroups of G exist, i.e., $\operatorname{Syl}_p(G) \neq 0$.
2. If P is a Sylow p-subgroup of G and Q is any p-subgroup of G, then there exists $g \in G$ such that $Q \leq gPg^{-1}$, i.e., Q is contained in some conjugate of P. In particular, any two Sylow p-subgroups of G are conjugate in G.
3. The number of Sylow p-subgroups of G is of the form $1 + kp$, i.e.,

$$n_p \equiv 1 \pmod{p}.$$

Further, n_p is the index of the normalizer $N_G(P)$ in G for any Sylow p-subgroup P, hence n_p divides m.

Lemma 4.19: Let $P \in \operatorname{Syl}_p(G)$. If Q is any p-subgroup of G, then $Q \cap N_G(P) = Q \cap P$.

Corollary 4.20: Let P be a Sylow p-subgroup of G. Then the following are equivalent:

1. P is the unique Sylow p-subgroup of G, i.e., $n_p = 1$
2. P is normal in G

3. P is characteristic in G
4. All subgroups generated by elements of p-power order are p-groups, i.e., if X is any subset of G such that $|x|$ is a power of p for all $x \in X$, then $\langle X \rangle$ is a p-group.

If a subgroup $H \leq G$ has index 2, then H is normal.

Proposition 4.21: If $|G| = 60$ and G has more than one Sylow 5-subgroup, then G is simple.

Proposition 4.23: If G is a simple group of order 60, then $G \cong A_5$.

5. Direct and Semi-direct Products and Abelian Group

Definition - Direct Product:

1. The *direct product* $G_1 \times G_2 \times \cdots \times G_n$ of the groups $G_1, G_2, \dots, G_n$ with operations $\star_1, \star_2, \dots, \star_n$ respectively, is the set of n-tuples $(g_1, g_2, \dots, g_n)$ where $g_i \in G_i$ with operation defined component-wise:
$$(g_1, g_2, \dots, g_n) \star (h_1, h_2, \dots, h_n) = (g_1 \star_1 h_1, g_2 \star_2 h_2, \dots, g_n \star_n h_n).$$
2. Similarly, the *direct product* $G_1 \times G_2 \times \dots$ of the groups $G_1, G_2, \dots$ with operations $\star_1, \star_2, \dots$ respectively, is the set of sequences $(g_1, g_2, \dots)$ where $g_i \in G_i$ with operation defined component-wise:
$$(g_1, g_2, \dots) \star (h_1, h_2, \dots) = (g_1 \star_1 h_1, g_2 \star_2 h_2, \dots).$$

Proposition 5.1: If $G_1, G_2 \dots, G_n$ are groups, their direct product is a group of order $|G_1||G_2| \dots |G_n|$ (if any G_1 is infinite, so is the direct product).

Proposition 5.2: Let $G_1, G_2 \dots, G_n$ be groups and $G = G_1 \times \cdots \times G_n$ be their direct product.

1. For each fixed i the set of elements of G which have the identity of G_j in the jth position for all $j \neq i$ and arbitrary elements of G_1 in position i is a subgroup of G isomorphic to G_i:
$$G_i \cong \{(1, \dots, 1, g_i, 1, \dots, 1) | g_i \in G_i\},$$
(here g_i appears in the ith position and the subgroup on the right is often called the ith component or ith factor of G). If we identify G_i with this subgroup, then $G_i \trianglelefteq G$ and
$$G/G_i \cong G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n$$
2. For each fixed i define $\pi_i : G \to G_i$ by
$$\pi_i(g_1, \dots, g_n) = g_i.$$
Then π_i is a surjective homomorphism with
$$\begin{aligned} \ker \pi_i &= \{(g_1, \dots, g_{i-1}, 1, g_{i+1}, \dots, g_n) | g_j \in G_j \text{ for all } j \neq i\} \\ &\cong G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n \end{aligned}$$
3. Under the identifications in part (1), if $x \in G_i$ and $y \in G_j$ for some $i \neq j$, then $xy = yx$ (this idea is similar to commutativity of disjoint cycles).

$E_{p^n} = Z_p \times Z_p \times \cdots \times Z_p$ is the *elementary abelian group* of order p^n.

Definition - Finitely Generated, Free Abelian Group of Rank r:

1. A group G is *finitely generated* if there is a finite subset A of G such that $G = \langle A \rangle$.

2. For each $r \in \mathbb{Z}$ with $r \geq 0$, let $\mathbb{Z}^r = \mathbb{Z} \times \cdots \times \mathbb{Z}$ be the direct product of r copies of the group $\mathbb{Z}$, where $\mathbb{Z}^0 = 1$. The group $\mathbb{Z}^r$ is called the *free abelian group of rank* r.

Theorem 5.3 - Fundamental Theorem of Finitely Generated Abelian Groups: Let G be a finitely generated abelian group. Then

1. $$G \cong \mathbb{Z}^r \times Z_{n_1} \times \cdots \times Z_{n_s},$$
   for some integers $r, n_1, \ldots, n_s$ satisfying the following conditions:
   (a) $r \geq 0$ and $n_j \geq 2$ for all j, and
   (b) $n_{i+1} | n_i$ for $1 \leq i \leq s-1$

2. the expression in (1) is unique: if $G \cong \mathbb{Z}^t \times Z_{m_1} \times \cdots \times Z_{m_u}$, where t and $m_1, \ldots, m_u$ satisfy (a) and (b) (i.e., $t \geq 0, m_j \geq 2$ for all j, and $m_{i+1} | m_i$ for $1 \leq i \leq u-1$), then $t = r, u = s$ and $m_i = n_i$ for all i.

Definition - Free Rank/Betti Number, Invariant Factor (Decomposition), Type: The integer r in Theorem 3 is called the *free rank* or *Betti number* of G and the integers $n_1, n_2, \ldots, n_s$ are called the *invariant factors* of G. The description of G in Theorem 3(1) is called the *invariant factor decomposition* of G. If G is a finite abelian group, satisfying (b) above, then G is said to be of *type* $(n_1, n_2, \ldots, n_s)$.

Thus a finitely generated abelian group is a finite group if and only if its free rank is zero.

Some Observations:

1. $n_1 \geq n_2 \geq \cdots \geq n_s$ as a result of the divisibility condition.

2. Every prime divisor of n must divide the first invariant factor n_1.

3. One immediate consequence is that if n is a product of distinct primes (square-free), then $n | n_1$, and thus $n = n_1$ and there is only one possible list of invariant factors for an abelian group of order n, namely just the length 1 list $n = n_1$ itself.

Corollary 5.4: If n is the product of distinct primes, then up to isomorphism the only abelian group of order n is the cyclic group of order n, Z_n. This is an immediate consequence of part 3 from the above observations.

Theorem 5.5: Let G be an abelian group of order $n > 1$ and let the unique factorization of n into distinct prime powers be
$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}.$$
Then

1. $G \cong A_1 \times A_2 \times \cdots \times A_k$, where $|A_i| = p_i^{\alpha_i}$, or A_i is the Sylow p_i-subgroup of G.

2. For each $A \in \{A_1, A_2, \ldots, A_k\}$ with $|A| = p^\alpha$,
   $$A \cong Z_{p^{\beta_1}} \times Z_{p^{\beta_2}} \times \cdots \times Z_{p^{\beta_t}}$$
   with $\beta_1 \geq \beta_2 \geq \cdots \geq \beta_t \geq 1$ and $\beta_1 + \beta_2 + \cdots + \beta_t = \alpha$. In other words, the β_j's form a partition of α.

3. the decomposition in (1) and (2) is unique, i.e., if $G \cong B_1 \times B_2 \times \cdots \times B_m$, with $|B_i| = p_i^{\alpha_i}$ for all i, then $B_i \cong A_i$ and B_i and A_i have the same invariant factors.

Note that since G is assumed to be abelian above, each Sylow p_i-subgroup A_i is normal, and thus unique, in G.

Definition - Elementary Divisor (Decomposition): The integers p^{β_j} described in the preceding theorem are called the *elementary divisors* of G. The description of G in Theorem 5(1) and 5(2) is called the *elementary divisor decomposition* of G.

The elementary divisors of G are not invariant factors of G, rather they are invariant factors of subgroups $(p_i^{\alpha_i})$ of G.

Proposition 5.6: Let $m, n \in \mathbb{Z}^+$.

1. $Z_m \times Z_n \cong Z_{mn}$ iff the GCD $(m, n) = 1$.
2. If $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, then $Z_n \cong Z_{p_1^{\alpha_1}} \times Z_{p_2^{\alpha_2}} \times \cdots \times Z_{p_k^{\alpha_k}}$.

Definition - Rank, Exponent:

1. If G is a finite abelian group of type $(n_1, n_2, \dots, n_t)$, the integer t is called the *rank* of G (the free rank of G is 0 so there will be no confusion).
2. If G is any group, the *exponent* of G is the smallest positive integer n such that $x^n = 1$ for all $x \in G$ ((if no such integer exists the exponent of G is ∞).

Definition - Commutator, Commutator Subgroup: Let G be a group, let $x, y \in G$ and let A, B be nonempty subsets of G.

1. Define $[x, y] = x^{-1}y^{-1}xy$ to be the *commutator* of x and y.
2. Define $[A, B] = \langle [a, b] | a \in A, b \in B \rangle$, the group generated by commutators of elements of A and B.
3. Define $G' = \langle [x, y] | x, y \in G \rangle$, the subgroup of G generated by commutators of elements from G, called the *commutator subgroup of* G.

Thus $x, y \in G$ commute iff $[x, y] = 1$.

Proposition 5.7: Let G be a group, let $x, y \in G$ and let $H \leq G$. Then

1. $xy = yx[x, y]$ (in particular, $xy = yx$ iff $[x, y] = 1$).
2. $H \trianglelefteq G$ iff $[H, G] \leq H$.
3. $\sigma[x, y] = [\sigma(x), \sigma(y)]$ for any automorphism σ of G, $G' \operatorname{char} G$ and G/G' is abelian.
4. G/G' is the largest abelian quotient of G in the sense that if $H \trianglelefteq G$ and G/H is abelian, then $G' \leq H$. Conversely, if $G' \leq H$, then $H \trianglelefteq G$ and G/H is abelian.
5. If $\varphi : G \to A$ is any homomorphism of G into an abelian group A, then φ factors through G' i.e., $G' \leq \ker \varphi$ and the following diagram commutes:

$$\begin{tikzcd} G \arrow[r] \arrow[dr, "\varphi"'] & G/G' \arrow[d] \\ & A \end{tikzcd}$$

Proposition 5.8: Let H and K be subgroups of the group G. The number of distinct ways of writing each element of the set HK in the form hk, for some $h \in H$ and $k \in K$ is $|H \cap K|$. In particular, if $H \cap K = 1$, then each element of HK can be written uniquely as a product hk, for some $h \in H$ and $k \in K$.

Theorem 5.9: Suppose G is a group with subgroups H and K such that

1. H and K are normal in G, and
2. $H \cap K = 1$.

Then $HK \cong H \times K$.

Definition - Internal/External Direct Product: If G is a group and H and K are normal subgroups of G with $H \cap K = 1$, we call HK the *internal direct product* of H and K. We shall (when emphasis is called for) call HxK the *external direct product* of H and K.

Theorem 5.10: Let H and K be groups and let φ be a homomorphism from K into $\mathrm{Aut}(H)$. Let $\cdot$ denote the (left) action of K on H determined by $\varphi\cdot$ Let G be the set of ordered pairs (h, k) with $h \in H$ and $k \in K$ and define the following multiplication on G:

$$(h_1, k_1)(h_2, k_2) = (h_1 k_1 \cdot h_2, k_1 k_2).$$

1. This multiplication makes G into a group of order $|G| = |H||K|$.
2. The sets $\{(h, 1)|h \in H\}$ and $\{(1, k)|k \in K\}$ are subgroups of G and the maps $h \mapsto (h, 1)$ for $h \in H$ and $k \mapsto (1, k)$ for $k \in K$ are isomorphisms of these subgroups with the groups H and K respectively:
$$H \cong \{(h, 1)|h \in H\} \text{ and } K \cong \{(1, k)|k \in K\}.$$

Identifying H and K with their isomorphic copies in G described in (2) we have

3. $H \trianglelefteq G$,
4. $H \cap K = 1$,
5. for all $h \in H$ and $k \in K$, $khk^{-1} = k \cdot h = \varphi(k)(h)$.

Definition - Semidirect Product: Let H and K be groups and let φ be a homomorphism from K into $\mathrm{Aut}(H)$. The group described in Theorem 10 is called the *semidirect product* of H and K with respect to φ and will be denoted by $H \rtimes_\varphi K$ (when there is no danger of confusion we shall simply write $H \rtimes K$).

Proposition 5.11: Let H and K be groups and let $\varphi : K \to \mathrm{Aut}(H)$ be a homomorphism. Then the following are equivalent:

1. the identity (set) map between $H \rtimes K$ and $H \times K$ is a group homomorphism (hence an isomorphism).
2. φ is the trivial homomorphism from K into $\mathrm{Aut}(H)$.
3. $K \trianglelefteq H \rtimes K$.

Theorem 5.12: Suppose G is a group with subgroups H and K such that

1. $H \trianglelefteq G$, and
2. $H \cap K = 1$.

Let $\varphi : K \to \mathrm{Aut}(H)$ be the homomorphism defined by mapping $k \in K$ to the automorphism of left conjugation by k on H. Then $HK \cong H \rtimes K$. In particular, if $G = HK$ with H and K satisfying (1) and (2), then G is the semidirect product of H and K.

Definition - Complement: Let H be a subgroup of the group G. A subgroup K of G is called a *complement* for H in G if $G = HK$ and $H \cap K = 1$.

7. Introduction to Rings

Definition - Ring:

1. A ring R is a set together with two binary operations $+$ and $\times$ (called addition and multiplication) satisfying the following axioms:

   (i). $(R, +)$ is an abelian group,

   (ii). $\times$ is associative: $(a \times b) \times c = a \times (b \times c)$ for all $a, b, c \in R$

   (iii). the distributive laws hold in R: for all $a, b, c \in R$

   $$(a + b) \times c = (a \times c) + (b \times c) \text{ and } a \times (b + c) = (a \times b) + (a \times c)$$

2. The ring R is *commutative* if multiplication is commutative.

3. The ring R is said to have an *identity* (or contain a 1) if there is an element $1 \in R$ with $1 \times a = a \times 1 = a$ for all $a \in R$.

The additive identity in a ring will always be denoted by 0.

Definition - Field, Division Ring/Skew Field: A ring R with identity 1, where $1 \neq 0$, is called a *division ring* (or *skew field*) if every nonzero element $a \in R$ has a multiplicative inverse, i.e., there exists $b \in R$ such that $ab = ba = 1$. A commutative division ring is called a *field*.

Trivial rings are obtained by taking R to be any abelian group under addition and defining the multiplication of any two elements in R to be 0. If $R = \{0\}$ is the trivial group, then the resulting ring R is called the *zero ring*, denoted $R = 0$. Note that the zero ring is the only ring where $1 = 0$, so we immediately exclude this ring by imposing the standard condition that $1 \neq 0$.

Definition - The (real) Hamilton Quaternions: Let $\mathbb{H}$ be the collection of elements of the form $a + bi + cj + dk$ where $a, b, c, d \in \mathbb{R}$ are real numbers (loosely, "polynomials in $1, i, j, k$ with real coefficients") where addition is defined "componentwis" by

$$(a + bi + cj + dk) + (a' + b'i + c'j + d'k) = (a + a') + (b + b')i + (c + c')j + (d + d')k$$

and multiplication is defined using the distributive law and simplifying using the relations

$$i^2 = j^2 = k^2 = -1, ij = -ji = k, jk = -kj = i, ki = -ik = j$$

where the real coefficients commute with i, j, k.
The real Hamiltonian Quaternions (similarly is true for rational coefficients) form a non-commutative division ring with identity $1 = 1 + 0(i + j + k)$. Inverses are given by $(a + bi + cj + dk)^{-1} = \dfrac{a - bi - cj - dk}{a^2 + b^2 + c^2 + d^2}$.

Proposition 7.1: Let R be a ring. Then

1. $0a = a0 = 0$ for all $a \in R$.

2. $(-a)b = a(-b) = -(ab)$ for all $a, b \in R$ (recall $-a$ is the additive inverse of a).

3. $(-a)(-b) = ab$ for all $a, b \in R$.

4. if R has an identity 1, then the identity is unique and $-a = (-1)a$.

Definition - Zero Divisor, Unit: Let R be a ring.

1. A nonzero element $a \in R$ is called a *zero divisor* if there is a nonzero element $b \in R$ such that either $ab = 0$ or $ba = 0$.

2. Assume R has an identity $1 \neq 0$. An element u of R is called a *unit* in R if there is some v in R such that $uv = vu = 1$. The set of units in R is denoted $R^\times$.

Consequences of the Above Definitions:

1. Note that $R^\times$ forms a group under multiplication and will be referred to as the *group of units of R*.
2. In this terminology a field is just a commutative ring F with identity $1 \neq 0$ in which every nonzero element is a unit, i.e., $F^\times = F - \{0\}$.
3. Note that a zero divisor can never be a unit.
4. (2) and (3) imply that a field has no zero divisors.
5. $\mathbb{Z}/n\mathbb{Z}$ is a field iff n is prime.
6. $\mathbb{Q}(\sqrt{D})$ is called a *quadratic field* for D is a square-free integer.

Definition - Integral Domain: A commutative ring with identity $1 \neq 0$ is called an *integral domain* if it has no zero divisors.

Proposition 7.2: Assume a, b, c are elements of any ring with a not a zero divisor. If $ab = ac$, then either $a = 0$ or $b = c$ (i.e., if $a \neq 0$ we can cancel the a's). In particular, if a, b, c are any elements in an integral domain and $ab = ac$, then either $a = 0$ or $b = c$.

Corollary 7.3 - Wedderburn's little theorem: Any finite integral domain is a field.

Definition - Subring: A *subring* of the ring R is a subgroup of R that is closed under multiplication.

The conditions for checking if a subset $S \subseteq R$ is a subring are that it is nonempty and closed under subtraction (addition and inverses under addition) and under multiplication.

The *Gaussian Integers* are all numbers of the form $a + bi$, for integers a, b.

Definition - Ring of Integers in the Quadratic Field $\mathbb{Q}(\sqrt{D})$: Define

$$\mathcal{O} = \mathcal{O}_{\mathbb{Q}(\sqrt{D})} = \mathbb{Z}[\omega] = \{a + b\omega | a, b \in \mathbb{Z}\},$$

where $\omega = \begin{cases} \sqrt{D}, & \text{if } D \equiv 2, 3 \pmod 4 \\ \dfrac{1+\sqrt{D}}{2}, & \text{if } D \equiv 1 \pmod 4. \end{cases}$

Definition - Field Norm: Define the *field norm* $N : \mathbb{Q}(\sqrt{D}) \to \mathbb{Q}$ by

$$N(a + b\sqrt{D}) = (a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - Db^2 \in \mathbb{Q}.$$

If the quadratic field $\mathbb{Q}(\sqrt{D})$ is in some $w = \frac{1+\sqrt{D}}{2}$, then the norm is defined to be the conjugate of

Definition - Polynomial, Degree, Monic, $R[x]$: Given a ring R, the formal sum

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

with $n \geq 0$ and each $a_i \in R$ is called a *polynomial* in x with coefficients $a_i \in R$. If the *leading coefficient* $a_n \neq 0$, then this polynomial is said to be of *degree n*. $a_n x^n$ is called the *leading term*. This polynomial is said to be monic if $a_n = 1$. The set of all such polynomials is called the *ring of polynomials in the variable* *x with coefficients in R* and will be denoted $R[x]$.

The ring R appears in $R[x]$ as the *constant polynomials*, i.e. $R \subset R[x]$. Note that by definition of the multiplication, $R[x]$ is a commutative ring with identity (the identity 1 from R).

Proposition 7.4: Let R be an integral domain and let $p(x), q(x)$ be nonzero elements of $R[x]$. Then

1. $\deg(p(x)q(x)) = \deg p(x) + \deg q(x)$,
2. the units of $R[x]$ are just the units of R,
3. $R[x]$ is an integral domain.

Given a ring R we define $M_n(R)$ to be the set of all $n \times n$ matrices with entries from R. The element (a_{ij}) of $M_n(R)$ is an $n \times n$ square array of elements of R whose entry in row i and column j is $a_{ij} \in R$. $M_n(R)$ forms a ring. The units in $M_n(R)$ are $GL_n(R)$, the group of invertible $n \times n$ matrices with entries in R.

An element (a_{ij}) of $M_n(R)$ is called a *scalar matrix* if for some $a \in R, a_{ii} = a$ for all $i \in \{1, \ldots, n\}$ and $a_{ij} = 0$ for all $i \neq j$ (i.e., all diagonal entries equal a and all off-diagonal entries are 0).

If S is a subring of R then $M_n(S)$ is a subring of $M_n(R)$.

Definition - Group Ring: For a finite group $G = \{g_1, g_2, \ldots, g_n\}$, define the **group ring**, RG, of G with coefficients in R to be the set of all formal sums

$$a_1 g_1 + a_2 g_2 + \cdots + a_n g_n, \text{ for } a_i \in R, 1 \leq i \leq n.$$

Addition is defined component-wise and multiplication is defined using the distributive law and the group relations.

$\mathbb{Z}G$ (called the *integral group ring of* G) is a subring of $\mathbb{Q}G$ (the *rational group ring of* G). Furthermore, if H is a subgroup of G then $\mathbb{R}H$ is a subring of $\mathbb{R}G$.

Definition - Ring Homomorphism, Kernel. Let R and S be rings.

1. A *ring homomorphism* is a map $\varphi : R \to S$ satisfying
   (i). $\varphi(a + b) = \varphi(a) + \varphi(b)$ for all $a, b \in R$ (so φ is a group homomorphism on the additive groups) and
   (ii). $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in R$.
2. The *kernel* of the ring homomorphism φ, denoted $\ker \varphi$, is the set of elements of R that map to 0 in S (i.e., the kernel of φ viewed as a homomorphism of additive groups).
3. A bijective ring homomorphism is called an *isomorphism.*

We use $\cong$ to denote an isomorphism of rings, similarly to groups.

Proposition 7.5: Let R and S be rings and let $\varphi : R \to S$ be a homomorphism.

1. The image of φ is a subring of S.
2. The kernel of φ is a subring of R. Furthermore, if $\alpha \in \ker \varphi$ then $r\alpha$ and $\alpha r \in \ker \varphi$ for every $r \in R$, i.e., $\ker \varphi$ is closed under multiplication by elements from R.

Definition - Quotient Ring: This ring of cosets is called the *quotient ring* of R by $I = \ker\varphi$ and is denoted R/I.

Definition - (Left/Right) Ideal: Let R be a ring, let I be a subset of R and let $r \in R$.

1. $rI = \{ra | a \in I\}$ and $Ir = \{ar | a \in I\}$.
2. A subset I of R is a *left ideal* of R if
   (i). I is a subring of R, and
   (ii). I is closed under left multiplication by elements from R, i.e., $rI \subseteq I$ for all $r \in R$.

   Similarly I is a *right ideal* if (i) holds and in place of (ii) one has
   (ii)'. I is closed under right multiplication by elements from R, i.e., $Ir \subseteq I$ for all $r \in R$.
3. A subset I that is both a left ideal and a right ideal is called an *ideal* (or, for added emphasis, a *two-sided ideal*) of R.

Proposition 7.6: Let R be a ring and let I be an ideal of R. Then the (additive) quotient group R/I is a ring under the binary operations:

$$(r + I) + (s + I) = (r + s) + I \text{ and } (r + I)x(s + I) = (rs) + I$$

for all $r, s \in R$. Conversely, if I is any subgroup such that the above operations are well defined, then I is an ideal of R.

Definition - Quotient Ring: When I is an ideal of R the ring R/I with the operations in the previous proposition is called the *quotient ring* of R by I.

Theorem 7.7:

1. (*The First Isomorphism Theorem for Rings*) If $\varphi : R \to S$ is a homomorphism of rings, then the kernel of φ is an ideal of R, the image of φ is a subring of S and $R/\ker\varphi$ is isomorphic as a ring to $\varphi(R)$.
2. If I is any ideal of R, then the map

$$R \to R/I \qquad \text{defined by} \qquad r \mapsto r + I$$

   is the surjective ring homomorphism with kernel I (this homomorphism is called the natural projection of R onto R/I). Thus every ideal is the kernel of a ring homomorphism and vice versa.

Similarly to groups, we may write $\overline{r} = r + I$ for some ideal I and $\overline{r} + \overline{s} = \overline{r + s}$ and $\overline{r}\ \overline{s} = \overline{rs}$.

Theorem 7.8: Let R be a ring.

1. (*The Second Isomorphism Theorem for Rings*) Let A be a subring and let B be an ideal of R. Then $A + B = \{a + b | a \in A, b \in B\}$ is a subring of R, $A \cap B$ is an ideal of A and $(A + B)/B \cong A/(A \cap B)$.
2. (*The Third Isomorphism Theorem for Rings*) Let I and J be ideals of R with $I \subseteq J$. Then J/I is an ideal of R/I and $(R/I)/(J/I) \cong R/J$.
3. (*The Fourth or Lattice Isomorphism Theorem for Rings*) Let I be an ideal of R. The correspondence $A \leftrightarrow A/I$ is an inclusion preserving bijection between the set of subrings A of R that contain I and the set of subrings of R/I. Furthermore, A (a subring containing I) is an ideal of R if and only if A/I is an ideal of R/I.

Definition - Sum and Product of Ideals: Let I and J be ideals of R.

1. Define the *sum* of I and J by $I + J = \{a + b | a \in I, b \in J\}$.
2. Define the *product* of I and J, denoted by IJ, to be the set of all finite sums of elements of the form ab with $a \in I$ and $b \in J$.
3. For any $n \geq 1$, define the nth power of I, denoted by I^n, to be the set consisting of all finite sums of elements of the form $a_1 a_2 \dots a_n$ with $a_i \in I$ for all i. Equivalently, I^n is defined inductively by defining $I^1 = I$, and $I^n = II^{n-1}$ for $n = 2, 3, \dots$.

Definition - (A), Principle Ideal, Finitely Generated Ideal: Let A be any subset of the ring R with identity $1 \neq 0$.

1. Let (A) denote the smallest ideal of R containing A, called the *ideal generated by* A.
2. Let RA denote the set of all finite sums of elements of the form ra with $r \in R$ and $a \in A$ i.e., $RA = \{r_1 a_1 + r_2 a_2 + \cdots + r_n a_n | r_i \in R, a_i \in A, n \in \mathbb{Z}^+\}$ (where the convention is $RA = 0$ if $A = \emptyset$). Similarly, $AR = \{a_1 r_1 + a_2 r_2 + \cdots + a_n r_n | r_i \in R, a_i \in A, n \in \mathbb{Z}^+\}$ and $RAR = \{r_1 a_1 r_1 + r_2 a_2 r_2 + \cdots + r_n a_n r_n | r_i \in R, a_i \in A, n \in \mathbb{Z}^+\}$.
3. An ideal generated by a single element is called a *principal ideal.*
4. An ideal generated by a finite set is called a *finitely generated ideal.*

The (two-sided) ideal $I = (A)$ generated by some subset $A \subseteq R$ must be closed under multiplication of elements of R, so I contains all elements of the form $ar, \forall a \in A, r \in R$. Thus, for any ring R, the ideal generated by 1 is R, as $1r = r \in I, \forall r \in R$.

When $A = \{a\}, \{a_1, a_2, \dots, a_n\}$, or $\{a_1, a_2, \dots\}$, we can write $(a), (a_1, a_2, \dots, a_n), (a_1, a_2, \dots)$ to mean (A), respectively.

$$(A) = \bigcap_{\substack{I \text{ an ideal} \\ A \subseteq I}} I,$$

in other words, the ideal (A) generated by some set A is the intersection of all ideals of R containing the set A.

Similarly, the *left ideal generated by* A is the intersection of all left ideals of R that contain A.

Then RA is the left ideal generated by A, AR is the right ideal generated by A and RAR is the (two-sided) ideal generated by A. If R is commutative then $RA = AR = RAR = (A)$.

Proposition 7.9: Let I be an ideal of R with identity $1 \neq 0$.

1. $I = R$ if and only if I contains a unit.
2. Assume R is commutative. Then R is a field if and only if its only ideals are 0 and R.

Corollary 7.10: If R is a field then any nonzero ring homomorphism from R into another ring is an injection.

Definition - Maximal Ideal: An ideal M in an arbitrary ring S is called a *maximal ideal* if $M \neq S$ and the only ideals containing M are M and S.

Proposition 7.11: In a ring with identity every proper ideal is contained in a maximal ideal.

Proposition 7.12: Assume R is a commutative ring with identity $1 \neq 0$. The ideal M is a maximal ideal if and only if the quotient ring R/M is a field.

Definition - Prime Ideal: Assume R is a commutative ring with identity $1 \neq 0$. An ideal P is called a *prime ideal* if $P \neq R$ and whenever the product ab of two elements $a, b \in R$ is an element of P, then at least one of a and b is an element of P.

Proposition 7.13: Assume R is a commutative ring with identity $1 \neq 0$.. Then the ideal P is a prime ideal in R if and only if the quotient ring R/P is an integral domain.

Corollary 7.14: Assume R is commutative. Every maximal ideal of R is a prime ideal.

Theorem 7.15: Let R be a commutative ring. Let D be any nonempty subset of R that does not contain 0, does not contain any zero divisors and is closed under multiplication (i.e., $ab \in D$ for all $a, b \in D$). Then there is a commutative ring Q with 1 such that Q contains R as a subring and every element of D is a unit in Q. The ring Q has the following additional properties.

1. every element of Q is of the form $rd^{-1} = d^{-1}r$ for some $r \in R$ and $d \in D$. In particular, if $D = R - \{0\}$ then Q is a field.
2. (uniqueness of Q) The ring Q is the "smallest" ring containing R in which all elements of D become units, in the following sense. Let S be any commutative ring with identity and let $\varphi : R \to S$ be any injective ring homomorphism such that $\varphi(d)$ is a unit in S for every $d \in D$. Then there is an injective homomorphism $\phi : Q \to S$ such that $\phi|_R = \varphi$. In other words, any ring containing an isomorphic copy of R in which all the elements of D become units must also contain an isomorphic copy of Q.

Definition - Ring (Field) of Fractions, Quotient Field: Let R, D and Q be as in Theorem 15.

1. The ring Q is called the *ring of fractions of D with respect to R* and is denoted $D^{-1}R$.
2. If R is an integral domain and $D = R - \{0\}$, Q is called the *field of fractions* or *quotient field* of R.

Corollary 7.16: Let R be an integral domain (which means R is commutative) and let Q be the field of fractions of R. If a field F contains a subring R' isomorphic to R then the subfield of F generated by R' is isomorphic to Q.

Definition - Ring Direct Product: We define a direct product of rings $R_1 \times R_2 \times \cdots \times R_n$ (or for infinitely many R_i) as the set of ordered pairs $(r_1, r_2, \ldots, r_n), r_i \in R_i$, where addition and multiplication are defined component-wise, i.e.,

$$(r_1, r_2) + (s_1, s_2) = (r_1 + s_1, r_2 + s_2) \text{ and } (r_1, r_2)(s_1, s_2) = (r_1 s_1, r_2 s_2).$$

Then a map from a ring R into a direct product of rings is a homomorphism iff the induced maps into each component of the direct product are homomorphisms.

Definition - Comaximal. The ideals A and B of the commutative ring R with identity $1 \neq 0$ are said to be *comaximal* if $A + B = R$.

Theorem 7.17 - Chinese Remainder Theorem: Let $A_1, A_2, \ldots, A_k$ be ideals in commutative ring R with identity $1 \neq 0$. The map

$$R \to R/A_1 \times R/A_2 \times \cdots \times R/A_k \text{ defined by } r \mapsto (r + A_1, r + A_2, \ldots, r + A_k)$$

is a ring homomorphism with kernel $A_1 \cap A_2 \cap \cdots \cap A_k$. If for each $i, j \in \{1, 2, \ldots, k\}$ with $i \neq j$ the ideals A_i and A_j are comaximal, then this map is surjective and $A_1 \cap A_2 \cap \cdots \cap A_k = A_1 A_2 \ldots A_k$, so

$$R/(A_1 A_2 \ldots A_k) = R/(A_1 \cap A_2 \cap \cdots \cap A_k) \cong R/A_1 \times R/A_2 \times \cdots \times R/A_k.$$

Corollary 7.18: Let n be a positive integer and let $P_1^{\alpha_1} P_2^{\alpha_2} \ldots P_k^{\alpha_k}$ be its factorization into powers of distinct primes. Then

$$\mathbb{Z}/n\mathbb{Z} \cong (\mathbb{Z}/P_1^{\alpha_1}\mathbb{Z}) \times (\mathbb{Z}/P_2^{\alpha_2}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/P_k^{\alpha_k}\mathbb{Z}),$$

as rings, so in particular we have the following isomorphism of multiplicative groups:

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/P_1^{\alpha_1}\mathbb{Z})^\times \times (\mathbb{Z}/P_2^{\alpha_2}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/P_k^{\alpha_k}\mathbb{Z})^\times.$$

8. Euclidean Domains, Principal Ideal Domains, and Unique Factorization Domains

Definition - (Positive) Norm: Any function $N : R \to \mathbb{Z}^+ \cup \{0\}$ with $N(0) = 0$ is called a *norm* on the integral domain R. If $N(a) > 0$ for a $a \neq 0$ define N to be a *positive norm*.

Definition - Euclidean Domain/Division Algorithm, Quotient, Remainder: The integral domain R is said to be a *Euclidean Domain* (or possess a *Division Algorithm*) if there is a norm N on R such that for any two elements a and b of R with $b \neq 0$ there exist elements q and r in R with

$$a = bq + r, \text{ with } r = 0 \text{ or } N(r) < N(b).$$

The element q is called the *quotient* and the element r the *remainder* of the division.

Definition - Euclidean Algorithm: We care about the existence of a division algorithm on an integral domain R because it allows for a *Euclidean algorithm* for two elements $a, b \in R$,

$$\begin{aligned}
a &= q_0 b + r_0 && (1)\\
b &= q_1 r_0 + r_1 && (2)\\
r_0 &= q_2 r_1 + r_2 && (3)\\
&\vdots && (4)\\
r_{n-2} &= q_n r_{n-1} + r_n && (5)\\
r_{n-1} &= q_{n+1} r_n && (6)
\end{aligned}$$

The sequence of (r_i) necessarily terminates at some $i = n$ as $N(b) > N(r_0) > \cdots > N(r_n)$ is a decreasing sequence of integers bounded below at 0.

Proposition 8.1: Every ideal in a Euclidean Domain is principal. More precisely, if I is any nonzero ideal in the Euclidean Domain R then $I = (d)$, where d is any nonzero element of I of minimum norm.

Definition - Greatest Common Divisor: Let R be a commutative ring and let $a, b \in R$ with $b \neq 0$.

1. a is said to be a *multiple* of b if there exists an element $x \in R$ with $a = bx$. In this case b is said to *divide* a or be a *divisor* of a, written $b|a$.
2. A *greatest common divisor* of a and b is a nonzero element d such that
   (i). $d|a$ and $d|b$, and
   (ii). if $d'|a$ and $d'|b$ then $d'|d$.

   A greatest common divisor of a and b will be denoted by $GCD(a, b)$, or (abusing the notation) simply (a, b).

$b|a$ iff $a \in (b)$ iff $(a) \subseteq (b)$.

If I is the ideal of R generated by a and b, then d is a greatest common divisor of a and b if

(i). I is contained in the principal ideal (d), and

(ii). if (d') is any principal ideal containing I then $(d) \subseteq (d')$.

This is essentially saying that (d) is the unique smallest ideal containing $I = (a, b)$.

Proposition 8.2: If a and b are nonzero elements in the commutative ring R such that the ideal generated by a and b is a principal ideal (d), then d is a greatest common divisor of a and b.

Definition - Bezout Domain: An integral domain in which every ideal (a, b) generated by two elements is principal is called a *Bezout Domain*.

Proposition 8.3: Let R be an integral domain. If two elements d and d' of R generate the same principal ideal, i.e., $(d) = (d')$, then $d' = ud$ for some unit u in R. In particular, if d and d' are both greatest common divisors of a and b, then $d' = ud$ for some unit u.

Theorem 8.4: Let R be a Euclidean Domain and let a and b be nonzero elements of R. Let $d = r_n$ be the last nonzero remainder in the Euclidean Algorithm for a and b described at the beginning of this chapter. Then

1. d is a greatest common divisor of a and b, and
2. the principal ideal (d) is the ideal generated by a and b. In particular, d can be written as an R-linear combination of a and b, i.e., there are elements x and y in R such that

$$d = ax + by.$$

Definition - Universal Side Divisor: Let $\tilde{R} = R^{\times} \cup \{0\}$ denote the collection of units of commutative ring R together with 0. An element $u \in R - \tilde{R}$ is called a *universal side divisor* if for every $x \in R$ there is some $z \in \tilde{R}$ such that u divides $x - z$ in R, i.e. $x = qu + z$, where z is either a unit or 0.

Proposition 8.5: Let R be an integral domain that is not a field. If R is a Euclidean Domain then there are universal side divisors in R.

Definition - Principal Ideal Domain (P.I.D.): A *Principal Ideal Domain (P.I.D.)* is an integral domain in which every ideal is principal.

Proposition 8.1 showed that every Euclidean domain is a principle ideal domain, so a Euclidean domain is a stronger condition than a P.I.D.

Proposition 8.6: Let R be a Principal Ideal Domain and let a and b be nonzero elements of R. Let d be a generator for the principal ideal generated by a and b. Then

1. d is a greatest common divisor of a and b,
2. d can be written as an R-linear combination of a and b, i.e., there are elements x and y in R with

$$d = ax + by.$$

3. d is unique up to multiplication by a unit of R.

Proposition 8.7: Every nonzero prime ideal in a Principal Ideal Domain is a maximal ideal.

Corollary 8.8: If R is any commutative ring such that the polynomial ring $R[x]$ is a Principal Ideal Domain (or a Euclidean Domain), then R is necessarily a field.

Definition - Dedekind-Hasse Norm: Define N to be a *Dedekind-Hasse norm* if N is a positive norm and for every nonzero $a, b \in R$ either a is an element of the ideal (b) or there is a nonzero element in the ideal (a, b) of norm strictly smaller than the norm of b (i.e., either b divides a in R or there exist $s, t \in R$ with $0 < N(sa - tb) < N(b)$).

Note that when $s = 1$ in the above definition, this is equivalent to R being a Euclidean domain.

Proposition 8.9: The integral domain R is a P.I.D. if and only if R has a Dedekind-Hasse norm.

Definition - Irreducible, Prime, Associate: Let R be an integral domain.

1. Suppose $r \in R$ is nonzero and is not a unit. Then r is called *irreducible* in R if whenever $r = ab$ with $a, b \in R$, at least one of a or b must be a unit in R. Otherwise r is said to be *reducible.*
2. The nonzero element $p \in R$ is called *prime* in R if the ideal (p) generated by p is a prime ideal. In other words, a nonzero element p is a prime if it is not a unit and whenever $p|ab$ for any $a, b \in R$, then either $p|a$ or $p|b$.
3. Two elements a and b of R differing by a unit are said to be associate in R (i.e., $a = ub$ for some unit u in R).

If R is a Principal Ideal Domain however, the notions of prime and irreducible elements are the same.

Proposition 8.10: In an integral domain a prime element is always irreducible.

Proposition 8.11: In a Principal Ideal Domain a nonzero element is a prime if and only if it is irreducible.

Definition - Unique Factorization Domain (U.F.D.): A *Unique Factorization Domain (U.F.D.)* is an integral domain R in which every nonzero element $r \in R$ which is not a unit has the following two properties:

1. r can be written as a finite product of irreducible p_i of R (not necessarily distinct): $r = p_1 p_2 \dots p_n$ and
2. the decomposition in (1) is unique up to associates: namely, if $r = q_1 q_2 \dots q_m$ is another factorization of r into irreducibles, then $m = n$ and there is some renumbering of the factors so that p_i is associate to q_i for $i = 1, 2, \dots, n$.

Proposition 8.12: In a Unique Factorization Domain a nonzero element is a prime if and only if it is irreducible.

Proposition 8.13: Let a and b be two nonzero elements of the Unique Factorization Domain R and suppose

$$a = up_1^{e_1} \dots p_n^{e_n} \text{ and } b = vp_1^{f_1} \dots p_n^{f_n}$$

are prime factorizations for a and b, where u and v are units, the primes $p_1, p_2, \dots, p_n$ are distinct and the exponents e_i and f_i are ≥ 0. Then the element

$$d = p_1^{\min(e_1, f_1)} p_2^{\min(e_2, f_2)} \dots p_n^{\min(e_n, f_n)}$$

(where $d = 1$ if all the exponents are 0) is a greatest common divisor of a and b.

Theorem 8.14: Every Principal Ideal Domain is a Unique Factorization Domain. In particular, every Euclidean Domain is a Unique Factorization Domain.

Corollary 8.15 - Fundamental Theorem of Arithmetic: The integers $\mathbb{Z}$ are a Unique Factorization Domain.

Corollary 8.16: Let R be a P.I.D. Then there exists a multiplicative Dedekind-Hasse norm on R.

Lemma 8.17: The prime number $p \in Z$ divides an integer of the form $n^2 + 1$ if and only if p is either 2 or is an odd prime congruent to 1 modulo 4.

Proposition 8.18:

1. (*Fermat's Theorem on Sums of Squares*) The prime p is the sum of two integer squares, $p = a^2+b^2, a, b \in \mathbb{Z}$, if and only if $p = 2$ or $p \equiv 1 \pmod 4$. Except for interchanging a and b or changing the signs of a and b, the representation of p as a sum of two squares is unique.

2. The irreducible elements in the Gaussian integers $Z[i]$ are as follows:

   (a) $1 + i$ (which has norm 2),

   (b) the primes $p \in \mathbb{Z}$ with $p \equiv 3 \pmod 4$ (which have norm p^2), and

   (c) $a + bi, a - bi$, the distinct irreducible factors of $p = a^2 + b^2 = (a + bi)(a - bi)$ for the primes $p \in Z$ with $p \equiv 1 \pmod 4$ (both of which have norm p).

Corollary 8.19: Let n be a positive integer and write

$$n = 2^k p_1^{a_1} \dots p_r^{a_r} q_1^{b_1} \dots q_s^{b_s}$$

where $p_1, \dots, p_r$ are distinct primes congruent to $1 \pmod 4$ and $q_1, \dots, q_s$ are distinct primes congruent to $3 \pmod 4$. Then n can be written as a sum of two squares in $\mathbb{Z}$, i.e., $n = A^2 + B^2$ with $A, B \in Z$, if and only if each b_i is even. Further, if this condition on n is satisfied. then the number of representations of n as a sum of two squares is $4(a_1 + 1)(a_2 + 1) \dots (a_r + 1)$.

In summary of all of chapter 8,

$$\text{fields} \subset \text{Euclidean Domains} \subset \text{P.I.D.s} \subset \text{U.F.D.s} \subset \text{integral domains.}$$

9. Polynomial Rings

In this chapter the ring R will always denote a commutative ring with identity $1 \neq 0$.

The polynomial ring $R[x]$ is all formal sums of the form

$$a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0, n \geq 0, a_i \in R.$$

Proposition 9.1: Let R be an integral domain and let $p(x), q(x)$ be nonzero elements of $R[x]$. Then

1. $\deg(p(x)q(x)) = \deg p(x) + \deg q(x)$,

2. the units of $R[x]$ are just the units of R,

3. $R[x]$ is an integral domain.

If R is is an integral domain then the quotient field of $R[x]$ consists of all quotients $\frac{q(x)}{p(x)}$, where $q(x)$ is not the zero polynomial, and is called the field of rational functions in x with coefficients in R. For an integral domain R, the quotient ring of $R[x]$ by a prime ideal $pR[x]$ is an integral domain.

Proposition 9.2: Let I be an ideal of the ring R and let $(I) = I[x]$ denote the ideal of $R[x]$ generated by I (the set of polynomials with coefficients in I). Then

$$R[x]/(I) \cong R/I[x].$$

In particular, if I is a prime ideal of R then (I) is a prime ideal of $R[x]$.

Definition - Multivariate Polynomial Rings: The *polynomial ring in the variables* $x_1, x_2, \ldots, x_n$ with coefficients in R, denoted $R[x_1, x_2, \ldots, x_n]$, is defined inductively by

$$R[x_1, x_2, \ldots, x_n] = R[x_1, x_2, \ldots, x_{n-1}][x_n].$$

Elements of this ring are of the form

$$ax_1^{d_1} \ldots x_n^{d_n}, d_i \geq 0$$

where $a \in R$ is the *coefficient* of the term, the exponent d_i is called the *degree in* x_i of the term and the sum $d = d_1 + d_2 + \cdots + d_n$ is called the *degree* of the term. The ordered n-tuple $(d_1, d_2, \ldots, d_n)$ is the *multidegree* of the term. A monic term $x_1^{d_1} \ldots x_n^{d_n}$ is called simply a *monomial* and is the *monomial part* of the term $ax_1^{d_1} \ldots x_n^{d_n}$. The *degree* of a nonzero polynomial is the largest degree of any of its monomial terms.
A polynomial is called *homogeneous* or a *form* if all its terms have the same degree. If f is a nonzero polynomial in n variables, the sum of all the monomial terms in f of degree k is called the *homogeneous component of* f *of degree* k.
If f has degree d then f may be written uniquely as the sum $f_0 + f_1 + \cdots + f_d$, where f_k is the homogeneous component of f of degree k, for $0 \leq k \leq$d (where some f_k may be zero).

Theorem 9.3: Let F be a field. The polynomial ring $F[x]$ is a Euclidean Domain. Specifically, if $a(x)$ and $b(x)$ are two polynomials in $F[x]$ with $b(x)$ nonzero, then there are *unique* $q(x)$ and $r(x)$ in $F[x]$ such that

$$a(x) = q(x)b(x) + r(x), \text{ with } r(x) = 0 \text{ or } \deg r(x) < \deg \underline{(}x).$$

Corollary 9.4: If F is a field, then $F[x]$ is a Principal Ideal Domain and a Unique Factorization Domain.

Proposition 9.5 - Gauss' Lemma: Let R be a Unique Factorization Domain with field of fractions F and let $p(x) \in R[x]$. If $p(x)$ is reducible in $F[x]$ then $p(x)$ is reducible in $R[x]$. More precisely, if $p(x) = A(x)B(x)$ for some non-constant polynomials $A(x), B(x) \in F[x]$, then there are nonzero elements $r, s \in F$ such that $rA(x) = a(x)$ and $sB(x) = b(x)$ both lie in $R[x]$ and $p(x) = a(x)b(x)$ is a factorization in $R[x]$.

Note that Gauss' Lemma is not saying that there exist R-multiples of $A(x)$ and $B(x)$, rather that there are F-multiples.

Corollary 9.6: Let R be a Unique Factorization Domain, let F be its field of fractions and let $p(x) \in R[x]$. Suppose the greatest common divisor of the coefficients of $p(x)$ is 1. Then $p(x)$ is irreducible in $R[x]$ if and only if it is irreducible in $F[x]$. In particular, if $p(x)$ is a monic polynomial that is irreducible in $R[x]$, then $p(x)$ is irreducible in $F[x]$.

Theorem 9.7: R is a Unique Factorization Domain if and only if $R[x]$ is a Unique Factorization Domain.

Corollary 9.8: If R is a Unique Factorization Domain, then a polynomial ring in an arbitrary number of variables with coefficients in R is also a Unique Factorization Domain.

Proposition 9.9: Let F be a field and let $p(x) \in F[x]$. Then $p(x)$ has a factor of degree one if and only if $p(x)$ has a root in F, i.e., there is an $\alpha \in F$ with $p(\alpha) = 0$.

Proposition 9.10: A polynomial of degree two or three over a field F is reducible if and only if it has a root in F.

Proposition 9.11: Let $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be a polynomial of degree n with integer coefficients. If $r/s \in \mathbb{Q}$ is in lowest terms, (i.e., r and s are relatively prime integers) and r/s is a root of $p(x)$, then r divides the constant term and s divides the leading coefficient of $p(x) : r|a_0$ and $s|a_n$. In particular, if $p(x)$ is a monic polynomial with integer coefficients and $p(d) \neq 0$ for all integers d dividing the constant term of $p(x)$, then $p(x)$ has no roots in $\mathbb{Q}$.

Proposition 9.12: Let I be a proper ideal in the integral domain R and let $p(x)$ be a non-constant monic polynomial in $R[x]$. If the image of $p(x)$ in $(R/I)[x]$ cannot be factored in $(R/I)[x]$ into two polynomials of smaller degree, then $p(x)$ is irreducible in $R[x]$.

Proposition 9.13 - Eisenstein's Criterion: Let P be a prime ideal of the integral domain R and let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be a polynomial in $R[x]$ (here $n \geq 1$). Suppose $a_{n-1}, \ldots, a_1, a_0$ are all elements of P and suppose a_0 is not an element of P^2. Then $f(x)$ is irreducible in $R[x]$.

Corollary 9.14 - Eisenstein's Criterion for $\mathbb{Z}[x]$): Let p be a prime in $\mathbb{Z}$ and let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x], n \geq 1$. Suppose p divides a_i for all $i \in \{0, 1, \ldots, n-1\}$ but that p^2 does not divide a_0. Then $j(x)$ is irreducible in both $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$.

Proposition 9.15: Let F denote a field. The maximal ideals in $F[x]$ are the ideals $(f(x))$ generated by irreducible polynomials $f(x)$. In particular, $F[x]/(f(x))$ is a field if and only if $f(x)$ is irreducible.

Proposition 9.16: Let $g(x)$ be a non-constant element of $F[x]$ and let

$$g(x) = f_1(x)^{n_1} f_2(x)^{n_2} \ldots f_k(x)^{n_k}$$

be its factorization into irreducibles, where the $f_i(x)$ are distinct. Then we have the following isomorphism of rings:

$$F[x]/(g(x)) \cong F[x]/(f_1(x)^{n_1}) \times F[x]/(f_2(x)^{n_2}) \times \cdots \times F[x]/(f_k(x)^{n_k}).$$

Proposition 9.17: If the polynomial $f(x)$ has roots $\alpha_1, \alpha_2, \ldots, \alpha_k \in F$ (not necessarily distinct), then $f(x)$ has $(x - a_1) \ldots (x - a_k)$ as a factor. In particular, a polynomial of degree n in one variable over a field F has at most n roots in F, even counted with multiplicity.

Proposition 9.18: A finite subgroup of the multiplicative group of a field is cyclic. In particular, if F is a finite field, then the multiplicative group $F^\times$ of nonzero elements of F is a cyclic group.

Corollary 9.19: Let p be a prime. The multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ of nonzero residue classes mod p is cyclic.

Corollary 9.20: Let $n \geq 2$ be an integer with factorization $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r} \in \mathbb{Z}$, where $p_1, \ldots, p_r$ are distinct primes. We have the following isomorphisms of (multiplicative) groups:

1. $(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^\times \times (\mathbb{Z}/p_2^{\alpha_2}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_r^{\alpha_r}\mathbb{Z})^\times$.
2. $(\mathbb{Z}/2^r\mathbb{Z})^\times$ is the direct product of a cyclic group of order 2 and a cyclic group of order $2^{\alpha-2}$, for all $\alpha \geq 2$.
3. $(\mathbb{Z}/p^r\mathbb{Z})^\times$ is a cyclic group of order $p^{\alpha-1}(p-1)$, for all odd primes p.

13. Field Theory

Recall that a field F is a commutative ring with identity in which every nonzero element has an inverse. Equivalently, the set $F^{\times} = F - \{0\}$ of nonzero elements of F is an abelian group under multiplication.

Definition - Characteristic: The *characteristic* of a field F, denoted $\mathrm{ch}(F)$, is defined to be the smallest positive integer p such that $p \cdot 1_F = 1_F + \cdots + 1_F = 0$ if such a p exists, and is defined to be 0 otherwise.

The characteristic of a field is either a prime p or 0.

Proposition 13.1: The characteristic of a field F, $\mathrm{ch}(F)$, is either 0 or a prime p. If $\mathrm{ch}(F) = p$ then for any $\alpha \in F$,

$$p \cdot \alpha = \alpha + \cdots + \alpha = 0.$$

Definition - $\mathbb{F}_p, \mathbb{F}_p(x)$: We define $\mathbb{F}_p = \mathbb{Z}/p\,\mathbb{Z}$ and $\mathbb{F}_p(x)$, the field of rational functions in x with coefficients in $\mathbb{F}_p$.

Definition - Prime Subfield: The *prime subfield* of a field F is the subfield of F generated by the multiplicative identity 1_F of F. It is (isomorphic to) either $\mathbb{Q}$ (if $\mathrm{ch}(F) = 0$) or $\mathbb{F}_p$ (if $ch(F) = p$).

This can be proved by considering a map $\varphi : \mathbb{Z} \to F$ in which $n \mapsto n \cdot 1_F$ and considering $\ker(\varphi) = \mathrm{ch}(F)\,\mathbb{Z}$.

If a field has characteristic p, then $0 = p \cdot 1 = p$.

Definition - Extension (Field), Base Field: If K is a field containing the subfield F, then K is said to be an *extension field* (or simply an *extension*) of F, denoted K/F (which reads "K over F") or by the diagram

$$\begin{array}{c} K \\ | \\ F \end{array}$$

In particular, every field F is an extension of its prime subfield. The field F is sometimes called the *base field* of the extension.

If K/F is any extension of fields, then the multiplication defined in K makes K into a vector space over F. In particular, every field F can be considered as a vector space over its prime field.

Definition - (Relative) Degree/Index: The *degree* (or *relative degree* or *index*) of a field extension K/F, denoted $[K : F]$, is the dimension of K as a vector space over F (i.e., $[K : F] = \dim_F K$). The extension is said to be finite if $[K : F]$ is finite and is said to be infinite otherwise.

Proposition 13.2: Let $\varphi : F \to F'$ be a homomorphism of fields. Then φ is either identically 0 or is injective, so that the image of φ is either 0 or isomorphic to F.

Theorem 13.3: Let F be a field and let $p(x) \in F[x]$ be an irreducible polynomial. Then there exists a field K containing an isomorphic copy of F in which $p(x)$ has a root. Identifying F with this isomorphic copy shows that there exists an extension of F in which $p(x)$ has a root.

Theorem 13.4: Let $p(x) \in F[x]$ be an irreducible polynomial of degree n over the field F and let $K = F[x]/(p(x))$. Let $\theta = x \bmod (p(x)) \in K$. Then the elements

$$1, \theta, \theta^2, \ldots, \theta^{n-1}$$

are a basis for K as a vector space over F, so the degree of the extension is n, i.e., $[K : F] = n$. Hence

$$K = \{a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1} | a_0, a_1, \ldots, a_{n-1} \in F\}$$

consists of all polynomials of degree $< n$ in θ.

Corollary 13.5. Let K be as in Theorem 4, and let $a(\theta), b(\theta) \in K$ be two polynomials of degree $< n$ in θ. Then addition in K is defined simply by usual polynomial addition and multiplication in K is defined by

$$a(\theta)b(\theta) = r(\theta)$$

where $r(\theta)$ is the remainder (of degree $< n$) obtained after dividing the polynomial $a(x)b(x)$ by $p(x)$ in $F[x]$.

K is a field.

Definition - Field Generated By: Let K be an extension of the field F and let $\alpha, \beta, \dots \in K$ be a collection of elements of K. Then the smallest subfield of K containing both F and the elements $\alpha, \beta, \dots$ denoted $F(\alpha, \beta, \dots)$ is called the field *generated by* $\alpha, \beta, \dots$ over F.

Definition - Simple Extension, Primitive Element: If the field K is generated by a single element α over F, $K = F(\alpha)$, then K is said to be a *simple extension* of F and the element α is called a *primitive element* for the extension.

Theorem 13.6: Let F be a field and let $p(x) \in F[x]$ be an irreducible polynomial. Suppose K is an extension field of F containing a root α of $p(x) : p(\alpha) = 0$. Let $F(\alpha)$ denote the subfield of K generated over F by α. Then

$$F(\alpha) \cong F[x]/(p(x)).$$

Corollary 13.7: Suppose in Theorem 6 that p(x) is of degree n. Then

$$F(\alpha) = \{a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1} | a_0, a_1, \dots, a_{n-1} \in F\} \subseteq K.$$

Theorem 13.8: Let $\varphi : F \xrightarrow{\sim} F'$ be an isomorphism of fields. Let $p(x) \in F[x]$ be an irreducible polynomial and let $p'(x) \in F'[x]$ be the irreducible polynomial obtained by applying the map φ to the coefficients of $p(x)$. Let α be a root of $p(x)$ (in some extension of F) and let β be a root of $p'(x)$ (in some extension of F'). Then there is an isomorphism

$$\sigma : F(\alpha) \xrightarrow{\sim} F'(\beta)$$
$$\alpha \mapsto \beta$$

mapping α to β and extending φ, i.e., such that σ restricted to F is the isomorphism φ.

Definition - Algebraic, transcendental: Let F be a field and K an extension of F. The element $\alpha \in K$ is said to be *algebraic* over F if α is a root of some nonzero polynomial $f(x) \in F[x]$. If α is not algebraic over F (i.e., is not the root of any nonzero polynomial with coefficients in F) then α is said to be transcendental over F. The extension K/F is said to be *algebraic* if every element of K is algebraic over F.

Proposition 13.9: Let α be algebraic over F. Then there is a unique monic irreducible polynomial $m_{\alpha,F}(x) \in F[x]$ which has α as a root. A polynomial $f(x) \in F[x]$ has α as a root if and only if $m_{\alpha,F}(x)$ divides $f(x)$ in $F[x]$.

Corollary 13.10: If L/F is an extension of fields and α is algebraic over both F and L, then $m_{\alpha,L}(x)$ divides $m_{\alpha,F}(x)$ in $L[x]$.

Definition - Minimal Polynomial, Degree: The polynomial $m_{\alpha,F}(x)$ (or just $m_\alpha(x)$ if the field F is understood) in Proposition 9 is called the *minimal polynomial* for α over F. The degree of $m_\alpha(x)$ is called the *degree* of α.

Proposition 13.11: Let α be algebraic over the field F and let $F(\alpha)$ be the field generated by α over F. Then

$$F(\alpha) \cong F[x]/(m_\alpha(x))$$

so that in particular

$$[F(\alpha) : F] = \deg m_\alpha(x) = \deg \alpha,$$

i.e., the degree of α over F is the degree of the extension it generates over F.

Proposition 13.12: The element α is algebraic over F if and only if the simple extension $F(\alpha)/F$ is finite. More precisely, if α is an element of an extension of degree n over F then α satisfies a polynomial of degree at most n over F and if α satisfies a polynomial of degree n over F then the degree of $F(\alpha)$ over F is at most n.

Corollary 13.13: If the extension K/F is finite, then it is algebraic.

Theorem 13.14: Let $F \subseteq K \subseteq L$ be fields. Then

$$[L : F] = [L : K][K : F],$$

i.e. extension degrees are multiplicative, where if one side of the equation is infinite, the other side is also infinite.

Corollary 13.15: Suppose L/F is a finite extension and let K be any subfield of L containing $F, F \subseteq K \subseteq L$. Then $[K : F]$ divides $[L : F]$.

Definition - Finitely Generated: An extension K/F is *finitely generated* if there are elements $\alpha_1, \ldots, \alpha_k$ in K such that $K = F(\alpha_1, \ldots, \alpha_k)$.

Lemma 13.16: $F(\alpha, \beta) = (F(\alpha))(\beta)$, i.e., the field generated over F by α and β is the field generated by β over the field $F(\alpha)$ generated by α.

Theorem 13.17: The extension K/F is finite if and only if K is generated by a finite number of algebraic elements over F. More precisely, a field generated over F by a finite number of algebraic elements of degrees $n_1, n_2, \ldots, n_k$ is algebraic of degree $\leq n_1 n_2 \ldots n_k$.

Corollary 13.18: Suppose α and β are algebraic over F. Then $\alpha \pm \beta$, $\alpha\beta$, α/β (for $\beta \neq 0$), (in particular α^{-1} for $\alpha \neq 0$) are all algebraic.

Corollary 13.19: Let L/F be an arbitrary extension. Then the collection of elements of L that are algebraic over F form a subfield K of L.

Theorem 13.20: If K is algebraic over F and L is algebraic over K, then L is algebraic over F.

Definition - Composite Field: Let K_1 and K_2 be two subfields of a field K. Then the *composite field* of K_1 and K_2, denoted K_1K_2, is the smallest subfield of K containing both K_1 and K_2. Similarly, the composite of any collection of subfields of K is the smallest subfield containing all the subfields.

Note that the composite field K_1K_2 can also be defined as the intersection of all the subfields of K containing both K_1 and K_2.

Proposition 13.21: Let K_1 and K_2 be two finite extensions of a field F contained in K. Then

$$[K_1K_2 : F] \leq [K_1 : F][K_2 : F]$$

with equality if and only if an F-basis for one of the fields remains linearly independent over the other field. In other words, if $\alpha_1, \alpha_2, \ldots, \alpha_n$ and $\beta_1, \beta_2, \ldots, \beta_m$ are bases for K_1 and K_2 over F, respectively, then the elements $\alpha_i\beta_j$ for $i = 1, 2, \ldots, n$ and $j = 1, 2, \ldots, m$ span K_1K_2 over F.

Corollary 13.22: Suppose that $[K_1 : F] = n, [K_2 : F] = m$ in Proposition 21, where $(m, n) = 1$, i.e. m, n are relatively prime. Then $[K_1K_2 : F] = [K_1 : F][K_2 : F] = mn$.

Proposition 13.23: If the element $\alpha \in \mathbb{R}$ is obtained from a field $F \subset \mathbb{R}$ by a (finite) series of compass and straightedge constructions then $[F(\alpha) : F] = 2^k$ for some integer $k \geq 0$.

Theorem 13.24: None of the classical Greek problems:

(I) Doubling/Duplicating of the Cube,

(II) Trisecting an Angle, and

(III) Squaring the Circle,

are possible.

Note that the distinction between a "straight-edge" and ruler is very important. Given a ruler with unit length 1 marked and a unit compass, it would be possible to trisect a given angle. Similarly is true of doubling the cube.

Definition - Splitting Field, Splits Completely: The extension field K of F is called a *splitting field* for the polynomial $f(x) \in F[x]$ if $f(x)$ factors completely into linear factors (or *splits completely*) in $K[x]$ and $f(x)$ does not factor completely into linear factors over any proper subfield of K containing F.

Theorem 13.25: For any field F, if $f(x) \in F[x]$ then there exists an extension K of F which is a splitting field for $f(x)$.

Definition - Normal Extension: If K is an algebraic extension of F which is the splitting field over F for a collection of polynomials $f(x) \in F[x]$ then K is called a *normal extension* of F.

Proposition 13.26: A splitting field of a polynomial of degree n over F is of degree at most $n!$ over F.

Definition - Primitive nth Root of Unity: A generator of the cyclic group of all nth roots of unity is called a *primitive nth root of unity.*

Define ζ_n to be the first nth root of unity (counting counterclockwise from 1).

Definition - Cyclotomic Field of nth Roots of Unity: The field $\mathbb{Q}(\zeta_n)$ is called the *cyclotomic field of nth roots of unity.*

Theorem 13.27: Let $\varphi : F \xrightarrow{\sim} F'$ be an isomorphism of fields. Let $f(x) \in F[x]$ be a polynomial and let $f'(x) \in F'[x]$ be the polynomial obtained by applying φ to the coefficients of $f(x)$. Let E be a splitting field for $f(x)$ over F and let E' be a splitting field for $f'(x)$ over F'. Then the isomorphism φ extends to an isomorphism $\sigma : E \xrightarrow{\sim} E'$, i.e., σ restricted to F is the isomorphism φ :

$$\begin{array}{cccc} \sigma : & E & \xrightarrow{\sim} & E' \\ & | & & | \\ \varphi : & F & \xrightarrow{\sim} & F' \end{array}$$

Corollary 13.28 - Uniqueness of Splitting Fields: Any two splitting fields for a polynomial $f(x) \in F[x]$ over a field F are isomorphic.

Definition - Algebraic Closure: The field $\overline{F}$ is called an *algebraic closure* of F if $\overline{F}$ is algebraic over F and if every polynomial $f(x) \in F[x]$ splits completely over $\overline{F}$ (so that $\overline{F}$ can be said to contain all the elements algebraic over F).

Definition - Algebraically Closed: A field K is said to be *algebraically closed* if every polynomial with coefficients in K has a root in K.

$K = \overline{K}$ iff K is algebraically closed. This also means that $\overline{\overline{K}} = \overline{K}$, for any field K.

Proposition 13.29: Let $\overline{F}$ be an algebraic closure of F. Then $\overline{F}$ is algebraically closed.

Proposition 13.30: For any field F there exists an algebraically closed field K containing F.

Proposition 13.31: Let K be an algebraically closed field and let F be a subfield of K. Then the collection of elements $\overline{F}$ of K that are algebraic over F is an algebraic closure of F. An algebraic closure of F is unique up to isomorphism.

Theorem - Fundamental Theorem of Algebra: The field $\mathbb{C}$ is algebraically closed.

Corollary 13.32: The field $\mathbb{C}$ contains an algebraic closure for any of its subfields. In particular, $\overline{\mathbb{Q}}$, the collection of complex numbers algebraic over $\mathbb{Q}$, is an algebraic closure of $\mathbb{Q}$.

Definition - Separable, Inseparable: A polynomial over F is called *separable* if it has no multiple roots (i.e., all its roots are distinct). A polynomial which is not separable is called *inseparable*.

By technicality of the definition, if a polynomial has no roots, e.g. a constant polynomial, then it is separable.

Definition - Derivative: The *derivative* of the polynomial

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in F[x]$$

is defined to be the polynomial

$$D_x f(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1 \in F[x].$$

Note that while this is defined similarly to that of analysis, if F is a discrete field, then the analytic notion of derivatives defined using limits (which are continuous) may not exist.

Proposition 13.33: A polynomial $f(x)$ has a multiple root α if and only if α is also a root of $D_x f(x)$, i.e., $f(x)$ and $D_x f(x)$ are both divisible by the minimal polynomial for α. In particular, $f(x)$ is separable if and only if it is relatively prime to its derivative: $(f(x), D_x f(x)) = 1$.

Corollary 13.34: Every irreducible polynomial over a field of characteristic 0 (for example, $\mathbb{Q}$) is separable. A polynomial over such a field is separable if and only if it is the product of distinct irreducible polynomials.

Proposition 13.35: Let F be a field of characteristic p. Then for any $a, b \in F$,

$$(a+b)^p = a^p + b^p, \text{ and } (ab)^p = a^p b^p.$$

Put another way, the pth-power map defined by $\varphi(a) = a^p$ is an injective field homomorphism from F to F. If F is finite, then φ is an isomorphism.

Definition - Frobenius Endomorphism: The map in Proposition 13.35 is called the *Frobenius endomorphism* of F.

Corollary 13.36: Suppose that $\mathbb{F}$ is a finite field of characteristic p. Then every element of $\mathbb{F}$ is a pth power in $\mathbb{F}$ (notationally, $\mathbb{F} = \mathbb{F}^p$).

Proposition 13.37: Every irreducible polynomial over a finite field $\mathbb{F}$ is separable. A polynomial in $\mathbb{F}[x]$ is separable if and only if it is the product of distinct irreducible polynomials in $\mathbb{F}[x]$.

Definition - Perfect: A field K of characteristic p is called *perfect* if every element of K is a pth power in K, i.e., $K = K^P$. Any field of characteristic 0 is also called *perfect*.

Definition - $\mathbb{F}_{p^n}$: For any integer $n > 0$, finite fields of any order p^n exist, for prime p, and are unique up to isomorphism. This field is denoted $\mathbb{F}_{p^n}$ and can be constructed as the splitting field of the equation $x^{p^n} - x$ over $\mathbb{F}_p$, the field of integers modulo p.

Proposition 13.38: Let $p(x)$ be an irreducible polynomial over a field F of characteristic p. Then there is a unique integer $k \geq 0$ and a unique irreducible separable polynomial $p_{sep}(x) \in F[x]$ such that

$$p(x) = p_{sep}\left(x^{p^k}\right).$$

Definition - (In)Separable Degree: Let $p(x)$ be an irreducible polynomial over a field of characteristic p. The degree of $p_{sep}(x)$ in proposition 13.38 is called the *separable degree* of $p(x)$, denoted $\deg_s p(x)$. The integer p^k in the proposition is called the *inseparable degree* of $p(x)$, denoted $\deg_i p(x)$.

Then a new definition for $p(x)$ is separable arises, being that the inseparable degree of p is 1, which is also equivalent to the separable degree being equal to the degree of p. Additionally, by definition, $\deg p(x) = \deg_s p(x) \deg_i p(x)$.

Definition - Separably Algebraic: The field K is said to be *separable* (or *separably algebraic*) over F if every element of K is the root of a separable polynomial over F (equivalently, the minimal polynomial over F of every element of K is separable). A field which is not separable is inseparable.

Corollary 13.39: Every finite extension of a perfect field is separable. In particular, every finite extension of either $\mathbb{Q}$ or a finite field is separable.

10. Introduction to Module Theory

Definition - Left Module Over R, Unital Modules: Let R be a ring (not necessarily commutative nor with 1). A *left R-module* or a *left module over R* is a set M together with

1. a binary operation $+$ on M under which M is an abelian group, and
2. an action of R on M (that is, a map $R \times M \to M$) denoted by rm, for all $r \in R$ and for all $m \in M$ which satisfies the following for all $r, s \in R$, and $m, n \in M$
   (a) $(r + s)m = rm + sm$
   (b) $(rs)m = r(sm)$
   (c) $r(m + n) = rm + rn$

   If R has identity 1, then we impose an additional axiom that

   (d) $1m = m$. Modules satisfying this axiom are called *unital modules*.

The notion of a right module could be defined similarly. If R is commutative, for a left R-module M, we could make M a right module by defining $mr = rm$, for all $r \in R, m \in M$. Not every left R-module is a right R-module.

Unless explicitly mentioned, a "module" will always refer to a left module. Additionally, we consider only unital modules, to avoid pathology.

When R is a field, the axioms of a module are exactly that of a vector space, so modules over a field F and vector spaces over F are the same.

Definition - R-Submodule: Let R be a ring and let M be an R-module. An *R-submodule* of M is a subgroup N of M which is closed under the action of ring elements, i.e., $rn \in N$, for all $r \in R, n \in N$. Every module M has at least 2 submodules, 0, the *trivial submodule*, and itself.

Definition - Free Module of Rank n over R: Define

$$R^n = \{(r_1, r_2, \ldots, r_n) | r_i \in R, \text{ for } i = [n]\}.$$

Then we can make R^n an R-module by defining addition component-wise and scalar multiplication by an element of R also component-wise. We call R^n the *free module of rank n over R.*

Definition - Annihilated by: If M is an R-module and for some (2-sided) ideal I of R, $im = 0$, for all $i \in I$ and all $m \in M$, we say M is *annihilated by I*. In this case, a very natural next step is to make M into a (R/I)-module by defining $(r + I)m = rm$, for coset $r + I$ in R/I and $m \in M$.

Example - $\mathbb{Z}$-Modules: For $R = \mathbb{Z}$ and A being any Abelian group (where we write the operation of A as $+$), we can make A into a $\mathbb{Z}$-module by defining the action of $n \in \mathbb{Z}$ on $a \in A$ as

$$na = \begin{cases} a + a + \cdots + a, & \text{if } n > 0 \\ 0, & \text{if } n = 0 \\ -a - a - \cdots - a, & \text{if } n < 0 \end{cases},$$

here 0 is identity of the additive group A. Thus, every Abelian group A is a $\mathbb{Z}$-module. The converse that every $\mathbb{Z}$-module M is an Abelian group is also true, so $\mathbb{Z}$-modules are the same as abelian groups.

Definition - Shift Operator: Let V be an affine n-space F^n and let T be the *shift operator*, where

$$T(x_1, x_2, \ldots, x_n) = (x_2, x_3, \ldots, x_n, 0).$$

Definition - $F[x]$-Modules, T-Stable/Invariant: Let F be a field, V be a vector space over F, x an indeterminate, and T a linear transformation from V to V. Then we can make V a $F[x]$-module by defining the action of $p(x) = a_n x^n + \cdots + a_1 x + a_0 \in F[X]$, for $a_i \in F$, on $v \in V$ by

$$p(T)(v) = a_n T^n(v) + \cdots + a_1 T(v) + a_0,$$

which clearly satisfies the module axioms. Any vector subspace $U \subseteq V$ such that $T(U) \subseteq U$ is called *T-stable* or *T-invariant.*

Additionally, there exists a bijection between $\{V \text{ a } F[x]\text{-module}\}$ and V a vector space over F and $T : V \to V$ a linear transformation. Similarly, there exists a bijection between $\{W \text{ a } F[x]\text{-submodule}\}$ and W a subspace of V and W is T-stable.

Proposition 10.1 - The Submodule Criterion: Let R be a ring and let M be an R-module. A subset N of M is a submodule of M if and only if

1. $N \neq \emptyset$, and
2. $x + ry \in N$, for all $r \in R$ and $x, y \in N$.

Definition - R-Algebra: Let R be a commutative ring with identity. An *R-algebra* is a ring A with identity together with a ring homomorphism $f : R \to A$ mapping 1_R to 1_A such that the subring $f(R)$ of A is contained in the center of A.

Definition - R-Algebra Homomorphism: If A and B are two R-algebras, an *R-algebra homomorphism* (or *isomorphism*) is a ring homomorphism (isomorphism, respectively) $\varphi : A \to B$ mapping 1_A to 1_B such that $\varphi(r \cdot a) = r \cdot \varphi(a)$ for all $r \in R$ and $a \in A$.

Definition - R-Module Homomorphism, Isomorphism, Kernel: Let R be a ring and let M and N be R-modules.

1. A map $\varphi : M \to N$ is an *R-module homomorphism* if it respects the R-module structures of M and N, i.e
   (a) $\varphi(x + y) = \varphi(x) + \varphi(y)$, for all $x, y \in M$, and
   (b) $\varphi(rx) = r\varphi(x)$, for all $r \in R, x \in M$.
2. An R-module homomorphism is an *isomorphism* (of R-modules) if it is both injective and surjective. The modules M and N are said to be isomorphic, denoted $M \cong N$, if there is some R-module isomorphism $\varphi : M \to N$.
3. If $\varphi : M \to N$ is an R-module homomorphism, let $\ker \varphi = \{m \in M | \varphi(m) = 0\}$ (the *kernel* of φ) and let $\varphi(M) = \{n \in N | n = \varphi(m) \text{ for some } m \in M\}$ (the image of φ, as usual).
4. Let M and N be R-modules and define $\hom_R(M, N)$ to be the set of all R-module homomorphisms from M into N.

An immediate corollary is that every R-module homomorphism is a homomorphism of the underlying additive groups. Additionally, kernels and images of R-modules are submodules. Additionally, when R is a field, R-module homomorphisms are called linear transformations.

Proposition 10.2: Let M, N and L be R-modules.

1. A map $\varphi : M \to N$ is an R-module homomorphism if and only if $\varphi(rx + y) = r\varphi(x) + \varphi(y)$ for all $x, y \in M$ and all $r \in R$.
2. Let φ, ψ be elements of $\hom_R(M, N)$. Define $\varphi + \psi$ by
   $$(\varphi + \psi)(m) = \varphi(m) + \psi(m), \text{ for all } m \in M.$$
   Then $\varphi + \psi \in \hom_R(M, N)$ and with this operation $\hom_R(M, N)$ is an abelian group under addition. If R is a commutative ring then for $r \in R$ define $r\varphi$ by
   $$(r\varphi)(m) = r(\varphi(m)), \text{ for all } m \in M.$$
   Then $r\varphi \in \hom_R(M, N)$ and with this action of the commutative ring R the abelian group $\hom_R(M, N)$ is an R-module.
3. If $\varphi \in \hom_R(L, M)$ and $\psi \in \hom_R(M, N)$, then $\psi \circ \varphi \in \hom_R(L, N)$.
4. With addition as above and multiplication defined as function composition, $\hom_R(M, M)$ is a ring with 1. When R is commutative $\hom_R(M, M)$ is an R-algebra.

Definition - Endomorphism Ring, Endomorphism: The ring $\hom_R(M, M)$ is called the *endomorphism ring of* M and will often be denoted by $\mathrm{End}_R(M)$, or just $\mathrm{End}(M)$ when the ring R is clear from the context. Elements of $\mathrm{End}(M)$ are called *endomorphisms*.

Proposition 10.3: Let R be a ring, let M be an R-module and let N be a submodule of M. The (additive, abelian) quotient group M/N can be made into an R-module by defining an action of elements of R by

$$r(x + N) = (rx) + N, \text{ for all } r \in R, x + N \in M/N.$$

The natural projection map $\pi : M \to M/N$ defined by $\pi(x) = x + N$ is an R-module homomorphism with kernel N.

Definition - Sum of Modules: Let A, B be submodules of the R-module M. The *sum* of A and B is the set $A + B = \{a + b | a \in A, b \in B\}$.

Theorem 10.4 - Isomorphism Theorems:

1. (*The First Isomorphism Theorem for Modules*) Let M, N be R-modules and let $\varphi : M \to N$ be an R-module homomorphism. Then $\ker \varphi$ is a submodule of M and $M/\ker \varphi \cong \varphi(M)$.
2. (*The Second Isomorphism Theorem*) Let A, B be submodules of the R-module M. Then $(A+B)/B \cong A/(A \cap B)$.
3. (*The Third Isomorphism Theorem*) Let M be an R-module, and let A and B be submodules of M with $A \subseteq B$. Then $(M/A)/(B/A) \cong M/B$.
4. (*The Fourth or Lattice Isomorphism Theorem*) Let N be a submodule of the R-module M. There is a bijection between the submodules of M which contain N and the submodules of M/N. The correspondence is given by $A \leftrightarrow A/N$, for all $A \supseteq N$. This correspondence commutes with the processes of taking sums and intersections (i.e., is a lattice isomorphism between the lattice of submodules of M/N and the lattice of submodules of M which contain N).

Definition - Finite Sums, (Finitely) Generated by, Minimal, Cyclic: Let M be an R-module and let $N_1, \ldots, N_n$ be submodules of M.

1. The *sum* of $N_1, \ldots, N_n$ is the set of all finite sums of elements from the sets N_i, i.e. $\{a_1+a_2+\cdots+a_n | a_i \in N_i, \text{ for all } i\}$. Denote this sum by $N_1 + \cdots + N_n$.
2. For any subset A of M let

$$RA = \{r_1a_1 + r_2a_2 + \cdots + r_ma_m | r_1, \ldots, r_m \in R, a_1, \ldots, a_m \in A, m \in \mathbb{Z}^+\}$$

   (where by convention $RA = \{0\}$ if $A = \emptyset$). If A is the finite set $\{a_1, a_2, \ldots, a_n\}$ we shall write $Ra_1 + Ra_2 + \cdots + Ra_n$ for RA. Call RA *the submodule of* M *generated by* A. If N is a submodule of M (possibly $N = M$) and $N = RA$, for some subset A of M, we call A a *set of generators* or *generating set* for N, and we say N is *generated* by A.
3. A submodule N of M (possibly $N = M$) is *finitely generated* if there is some finite subset A of M such that $N = RA$, that is, if N is generated by some finite subset. Additionally, if N if finitely generated, then there exists a smallest integer $d > 0$ such that N is generated by some set of d elements.

   Any generating set consisting of d elements will be called a *minimal set of generators* for N (this minimal set will not be unique in general).
4. A submodule N of M (possibly $N = M$) is *cyclic* if there exists an element $a \in M$ such that $N = Ra$, that is, if N is generated by one element, i.e. $N = Ra = \{ra | r \in R\}$.

RA is a submodule of M and is, in fact, the smallest submodule of M which contains A.

Definition - Direct Product/External Direct Sum: Let $M_1, \ldots, M_k$ be a collection of R-modules. The collection of k-tuples $(m_1, m_2, \ldots, m_k)$ where $m_i \in M_i$ with addition and action of R defined component-wise is called the *direct product* of $M_1, \ldots, M_k$, denoted $M_1 \times \cdots \times M_k$. A direct product of R-modules may also sometimes be referred to as the *external direct sum* of $M_1, \ldots, M_k$.

Proposition 10.5 - Internal Direct Sum: Let $N_1, N_2, \ldots, N_k$ be submodules of the R-module M. Then the following are equivalent:

1. The map $\pi : N_1 \times N_2 \times \cdots \times N_k \to N_1 + N_2 + \cdots + N_k$ defined by
$$\pi(a_1, a_2, \ldots, a_k) = a_1 + a_2 + \cdots + a_k$$
is an isomorphism (of R-modules): $N_1 + N_2 + \cdots + N_k \cong N_1 \times N_2 \times \cdots \times N_k$.
2. $N_j \cap (N_1 + N_2 + \cdots + N_{j-1} + N_{j+1} + \cdots + N_k) = 0$, for all $j \in [k]$.
3. Every $x \in N_1 + N_2 + \cdots + N_k$ can be written uniquely in the form $a_1 + a_2 + \cdots + a_k$ with $a_i \in N_i$.

If $M = N_1 + N_2 + \cdots + N_k$ satisfying condition 3 above, then M is said to be the internal direct sum of $N_1, N_2, \ldots, N_k$, written
$$M = N_1 \oplus N_2 \oplus \cdots \oplus N_k.$$

Definition - Free, Basis/Set of Free Generators, Rank: An R-module F is said to be *free* on the subset A of F if for every nonzero element x of F, there exist unique nonzero elements $r_1, r_2, \ldots, r_n$ of R and unique $a_1, a_2, \ldots, a_n$ in A such that $x = r_1a_1 + r_2a_2 + \cdots + r_na_n$, for some $n \in \mathbb{Z}^+$. In this situation we say A is a *basis* or *set of free generators* for F. If R is a commutative ring the cardinality of A is called the *rank* of F.

Theorem 10.6: For any set A there is a free R-module $F(A)$ on the set A and $F(A)$ satisfies the following *universal property*: if M is any R-module and $\varphi : A \to M$ is any map of sets, then there is a unique R-module homomorphism $\phi : F(A) \to M$ such that $\phi(a) = \varphi(a)$, for all $a \in A$, that is, the following diagram commutes.

$$\begin{tikzcd} A \arrow[r, "\text{inclusion}"] \arrow[dr, "\varphi"'] & F(A) \arrow[d, "\Phi"] \\ & M \end{tikzcd}$$

When A is the finite set $\{a_1, a_2, \ldots, a_n\}$, $F(A) = Ra_1 \oplus Ra_2 \oplus \cdots \oplus Ra_n \cong R^n$.

Corollary 10.7 - Extend by Linearity:

1. If F_1 and F_2 are free modules on the same set A, there is a unique isomorphism between F_1 and F_2 which is the identity map on A.
2. If F is any free R-module with basis A, then $F \cong F(A)$. In particular, F enjoys the same universal property with respect to A as $F(A)$ does in Theorem 6.

We often define R-module homomorphisms from F into other R-modules simply by specifying their values on the elements of A, then saying "extend by linearity."

When $R = \mathbb{Z}$, the free module on a set A is called the free abelian group on A. If $|A| = n, F(A)$ is called the free abelian group of rank n and is isomorphic to $\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$ (n times).

Tensor Product of Modules

Let R be a subring of a ring S and $f : R \to S$ is a ring homomorphism with $f(1_R) = 1_S$. Then for some left S-module N, we can make N an R-module if $rn = f(r)n$, for defining the action of $f(r)n = sn$, when $f(r) = s$, the same way as was defined for N a left S-module. In this case S is considered as an *extension* of the ring R and the resulting R-module is said to be obtained from N by *restriction of scalars* from S to R.

Definition - Tensor Product: Starting with a subring R of a ring S and N a left R-module. We call $S \otimes_R N$ (or just $S \otimes N$ is R is clear from context) the *tensor product* of S and N over R. The elements of $S \otimes_R N$ are called *tensors* and can be written as finite sums of the form $s \otimes n$ with $s \in S, n \in N$. Then $S \otimes_R N$ is naturally a left S-module under the action defined by

$$s\left(\sum s_i \otimes n_i\right) = \sum (ss_i) \otimes n_i.$$

In this case, $S \otimes_R N$ is called the *(left) S-module obtained by extension of scalars from the (left) R-module N*.

Less formally, a tensor product $S \otimes_R N$ can be seen simply as an extension of the left R-module N to an S-module.

Properties of Tensor Products: Given a tensor product $S \otimes_R N$ (for R is a subring of S), elements $s_1, s_2 \in S$, $n_1, n_2 \in N$, and $r \in RS$,

1. $(s_1 + s_2) \otimes n = s_1 \otimes n + s_2 \otimes n$,
2. $s \otimes (n_1 + n_2) = s \otimes n_1 + s \otimes n_2$, and
3. $sr \otimes n = s \otimes rn$.

Theorem 10.8: Let R be a subring of S, let N be a left R-module and let $\iota : N \to S \otimes_R N$ be the R-module homomorphism defined by $\iota(n) = 1 \otimes n$. Suppose that L is any left S-module (hence also an R-module) and that $\varphi : N \to L$ is an R-module homomorphism from N to L. Then there is a unique S-module homomorphism $\phi : S \otimes_R N \to L$ such that φ factors through ϕ, i.e. $\varphi = \phi \circ \iota$ and the diagram

$$\begin{tikzcd}
N \arrow[r, "\iota"] \arrow[dr, "\varphi"'] & S \otimes_R N \arrow[d, "\Phi"] \\
& L
\end{tikzcd}$$

commutes. Conversely, if $\phi : S \otimes_R N \to L$ is an S-module homomorphism then $\varphi = \phi \circ i$ is an R-module homomorphism from N to L.

Corollary 10.9: Let $\iota : N \to S \otimes_R N$ be the R-module homomorphism in Theorem 8 above. Then $N/\ker \iota$ is the unique largest quotient of N that can be embedded into any S-module. In particular, N can be embedded as an R-submodule of some left S-module iff ι is injective (in which case N is isomorphic to the R-submodule $\iota(N)$ of the S-module $S \otimes_R N$).

Definition - Tensor Product of Two R-Modules: For a right R-module M, and left R-module N, we denote the *tensor product of M and N over R*, as $M \otimes_R N$ (or $M \otimes N$) and have the following relations:

$$(m_1 + m_2) \otimes n = m_1 \otimes n + m_2 \otimes n,$$
$$m \otimes (n_1 + n_2) = m \otimes n_1 + m \otimes n_2, \text{ and}$$
$$mr \otimes n = m \otimes rn.$$

The elements of $M \otimes_R N$ are called *tensors*, and the coset of (m, n) in $M \otimes_R N$, $m \otimes n$, is called a *simple tensor*.

A tensor product can be understood alternatively as quotienting out by the subgroup generated by the above relations as follows:

$$(m_1 + m_2) \otimes n = m_1 \otimes n + m_2 \otimes n \quad \leftrightarrow \quad (m_1 + m_2, n) - (m_1, n) - (m_2, n).$$

Definition - R-balanced, Middle Linear: Let M be a right R-module, let N be a left R-module and let L be an abelian group (written additively). A map $\varphi : M \times N \to L$ is called *R-balanced* or *middle linear with respect to R* if

$$\begin{aligned}
\varphi(m_1 + m_2, n) &= \varphi(m_1, n) + \varphi(m_2, n) \\
\varphi(m, n_1 + n_2) &= \varphi(m, n_1) + \varphi(m, n_2) \\
\varphi(m, rn) &= \varphi(mr, n)
\end{aligned}$$

for all $m, m_1, m_2 \in M$, $n, n_1, n_2 \in N$, and $r \in R$.

Theorem 10.10: Suppose R is a ring with 1, M is a right R-module, and N is a left R-module. Let $M \otimes_R N$ be the tensor product of M and N over R and let $\iota : M \times N \to M \otimes_R N$ be the R-balanced map defined above.

1. If $\phi : M \otimes_R N \to L$ is any group homomorphism from $M \otimes_R N$ to an abelian group L, then the composite map $\varphi : \phi \circ \iota$ is an R-balanced map from $M \times N$ to L.
2. Conversely, suppose L is an Abelian group and $\varphi : M \times N \to L$ is any R-balanced map. Then there is a unique group homomorphism $\phi : M \otimes_R N \to L$ such that φ factors through ι, i.e. $\varphi = \phi \circ \iota$ as in (1).

Equivalently, the correspondence $\varphi \leftrightarrow \phi$ in the commutative diagram

$$\begin{tikzcd}
M \times N \arrow[r, "\iota"] \arrow[dr, "\varphi"'] & M \otimes_R N \arrow[d, "\Phi"] \\
& L
\end{tikzcd}$$

establishes a bijection

$$\left\{ \begin{matrix} R\text{-balanced maps} \\ \varphi : M \times N \to L \end{matrix} \right\} \leftrightarrow \left\{ \begin{matrix} \text{group homomorphisms} \\ \phi : M \otimes_R N \to L \end{matrix} \right\}.$$

Corollary 10.11: Suppose D is an abelian group and $\iota' : M \times N \to D$ is an R-balanced map such that

(i) the image of ι' generates D as an abelian group, and

(ii) every R-balanced map defined on $M \times N$ factors through ι' as in Theorem 10.

Then there is an isomorphism $f : M \otimes_R N \cong D$ of abelian groups with $\iota' = f \circ \iota$.

Definition - Bimodule: Let R and S be any rings with 1. An abelian group M is called an *(S, R)-bimodule* if M is a left S-module, a right R-module, and $s(mr) = (sm)r$ for all $s \in S$, $r \in R$ and $m \in M$.

Definition - Standard R-Module: Suppose M is a left (or right) R-module over the commutative ring R. Then the (R, R)-bimodule structure on M defined by letting the left and right R-actions coincide, i.e., $mr = rm$ for all $m \in M$ and $r \in R$, will be called the *standard R-module structure* on M.

Definition - R-bilinear: Let R be a commutative ring with 1 and let M, N, and L be left R-modules. The map $\varphi : M \times N \to L$ is called *R-bilinear* if it is R-linear in each factor, i.e., if

$$\begin{aligned}
\varphi(r_1 m_1 + r_2 m_2, n) &= r_1 \varphi(m_1, n) + r_2 \varphi(m_2, n), \text{ and} \\
\varphi(m, r_1 n_1 + r_2 n_2) &= r_1 \varphi(m, n_1) + r_2 \varphi(m, n_2)
\end{aligned}$$

for all $m, m_1, m_2 \in M$, $n, n_1, n_2 \in N$ and $r_1, r_2 \in R$.

Corollary 10.12: Suppose R is a commutative ring. Let M and N be two left R-modules and let $M \otimes_R N$ be the tensor product of M and N over R, where M is given the standard R-module structure. Then $M \otimes_R N$ is a left R-module with

$$r(m \otimes n) = (rm) \otimes n = (mr) \otimes n = m \otimes (rn),$$

and the map $\iota : M \times N \to M \otimes_R N$ with $\iota(m, n) = m \otimes n$ is an R-bilinear map. If L is any left R-module then there is a bijection

$$\left\{ \begin{array}{c} R\text{-bilinear maps} \\ \varphi : M \times N \to L \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} R\text{-module homomorphisms} \\ \phi : M \otimes_R N \to L \end{array} \right\}$$

where the correspondence between φ and ϕ is given by the commutative diagram

$$\begin{tikzcd} M \times N \arrow[r, "\iota"] \arrow[dr, "\varphi"'] & M \otimes_R N \arrow[d, "\Phi"] \\ & L \end{tikzcd}$$

Theorem 10.13 - The "Tensor Product" of Two Homomorphisms: Let M, M' be right R-modules, let N, N' be left R-modules, and suppose $\varphi : M \to M'$ and $\psi : N \to N'$ are R-module homomorphisms.

1. There is a unique group homomorphism, denoted by $\varphi \otimes \psi$, mapping $M \otimes_R N$ into $M' \otimes_R N'$ such that $(\varphi \otimes \psi)(m \otimes n) = \varphi(m) \otimes \psi(n)$ for all $n \in N, m \in M$.
2. If M, M' are also (S, R)-bimodules for some ring S and φ is also an S-module homomorphism, then $\varphi \otimes \psi$ is a homomorphism of left S-modules. In particular, if R is commutative then $\varphi \otimes \psi$ is always an R-module homomorphism for the standard R-module structures.
3. If $\lambda : M' \to M''$ and $\lambda : N' \to N''$ are R-module homomorphisms then $(\lambda \otimes \mu) \circ (\varphi \otimes \psi) = (\lambda \circ \varphi) \otimes (\mu \circ \psi)$.

Theorem 10.14 - Associativity of the Tensor Product: Suppose M is a right R-module, N is an (R, T)-bimodule, and L is a left T-module. Then there is a unique isomorphism

$$(M \otimes_R N) \otimes_T L \cong M \otimes_R (N \otimes_T L)$$

of abelian groups such that $(m \otimes n) \otimes l \mapsto m \otimes (n \otimes l)$. If M is an (S, R)-bimodule then this is an isomorphism of S-modules.

Corollary 10.15: Suppose R is commutative and $M, N,$ and L are left R-modules. Then

$$(M \otimes N) \otimes L \cong M \otimes (N \otimes L)$$

as R-modules for the standard R-module structures on M, N and L.

Definition - Multilinear: Let R be a commutative ring with 1 and let $M_1, M_2, \ldots, M_n$ and L be R-modules with the standard R-module structures. A map $\varphi : M_1 \times \cdots \times M_n \to L$ is called *n-multilinear over R* (or simply multilinear if n and R are clear from the context) if it is an R-module homomorphism in each component when the other component entries are kept constant, i.e., for each i

$$\varphi(m_1, \ldots, m_{i-1}, rm_i + r'm_i', m_{i+1}, \ldots, m_n) = r\varphi(m_1, \ldots, m_i, \ldots, m_n) + r'\varphi(m_1, \ldots m_i' \ldots, m_n)$$

for all $m_i, m_i' \in M_i$ and $r, r' \in R$. When n $= 2$ (respectively, 3) one says φ is *bilinear* (respectively *trilinear*) rather than 2-multilinear (or 3-multilinear).

Corollary 10.16: Let R be a commutative ring and let $M_1, \ldots, M_n, L$ be R-modules. Let $M_1 \otimes \cdots \otimes M_n$ denote any bracketing of the tensor product of these modules and let

$$\iota : M_1 \times \cdots \times M_n \to M_1 \otimes \cdots \otimes M_n$$

be the map defined by $\iota(m_1, \ldots, m_n) = m_1 \otimes \cdots \otimes m_n$. Then

1. for every R-module homomorphism $\phi : M_1 \otimes \cdots \otimes M_n \to L$, the map $\varphi = \phi \circ \iota$ is n-multilinear from $M_1 \times \cdots \times M_n$ to L, and
2. if $\varphi : M_1 \times \cdots \times M_n \to L$ is an n-multilinear map then there is a unique R-module homomorphism $\phi : M_1 \otimes \cdots \otimes M_n \to L$ such that $\varphi = \phi \circ \iota$.

Hence there is a bijection

$$\left\{ \begin{matrix} n\text{-multilinear maps} \\ \varphi : M_1 \times \cdots \times M_n \to L \end{matrix} \right\} \leftrightarrow \left\{ \begin{matrix} R\text{-module homomorphisms} \\ \phi : M_1 \otimes \cdots \otimes M_n \to L \end{matrix} \right\}$$

with respect to which the following diagram commutes:

$$\begin{tikzcd} M \times \cdots \times M_n \arrow[r, "\iota"] \arrow[dr, "\varphi"'] & M \otimes \cdots \otimes M_n \arrow[d, "\Phi"] \\ & L \end{tikzcd}$$

Theorem 10.17 - Tensor Products of Direct Sums: Let M, M' be right R-modules and let N, N' be left R-modules. Then there are unique group isomorphisms

$$(M \oplus M') \otimes_R N \cong (M \otimes_R N) \oplus (M' \otimes_R N)$$
$$M \otimes_R (N \oplus N') \cong (M \otimes_R N) \oplus (M \otimes_R N')$$

such that $(m, m') \otimes n \mapsto (m \otimes n, m' \otimes n)$ and $m \otimes (n, n') \mapsto (m \otimes n, m \otimes n')$ respectively. If M, M' are also (S, R)-bimodules, then these are isomorphisms of left S-modules. In particular, if R is commutative, these are isomorphisms of R-modules.

Corollary 10.18 - Extension of Scalars for Free Modules: The module obtained from the free R-module $N \cong R^n$ by extension of scalars from R to S is the free S-module S^n, i.e.,

$$S \otimes_R R^n \cong S^n$$

as left S-modules.

Corollary 10.19: Let R be a commutative ring and let $M \cong R^s$ and $N \cong R^t$ be free R-modules with bases $m_1, \ldots, m_s$ and $n_1, \ldots, n_t$ respectively. Then $M \otimes_R N$ is a free R-module of rank st, with basis $m_i \otimes n_j, 1 \leq i \leq s$ and $1 \leq j \leq t$, i.e.

$$R^s \otimes_R R^t \cong R^{st}.$$

More generally, the tensor product of two free modules of arbitrary rank over a commutative ring is free.

Proposition 10.20: Suppose R is a commutative ring and M, N are left R-modules, considered with the standard R-module structures. Then there is a unique R-module isomorphism

$$M \otimes_R N \cong N \otimes_R M$$

mapping $m \otimes n$ to $n \otimes m$.

Proposition 10.21: Let R be a commutative ring and let A and B be R-algebras. Then the multiplication $(a \otimes b)(a' \otimes b') = aa' \otimes bb'$ is well defined and makes $A \otimes_R B$ into an R-algebra.