Abstract Algebra

Hechen Hu

October 3, 2024

Contents

1

Groups

1.1 Semigroups, Monoids and Groups

Definition 1
A *semigroup* is a nonempty set G together with a binary operation on G which is associative.

Definition 2
A *monoid* is a semigroup G which contains a (two-sided) identity element $e \in G$ such that $ae = ea = a$ for all $a \in G$.

Definition 3
A *group* is a monoid G such that there exists a (two-sided) inverse element and the operation between the inverse element and the original element yields the identity element regardless of order of operation.

Definition 4
A semigroup G is said to be *abelian* or *commutative* if its binary operation is commutative.

Definition 5
The *order* of a group G is the cardinal number $|G|$. G is said to be finite(resp. infinite) if $|G|$ is finite(resp. infinite).

Theorem 6
If G is a monoid, then the identity element e is unique. If G is a group, then

- $c \in G$ and $(cc = c) \Rightarrow (c = e)$;
- for all $a, b, c \in G$ we have $(ab = ac) \Rightarrow (b = c)$ and $(ba = ca) \Rightarrow (b = c)$ (left and right cancellation);
- for each element in G its inverse element is unique;
- for each element in G the inverse of its inverse is itself;
- for $a, b \in G$ we have $(ab)^{-1} = b^{-1}a^{-1}$;
- for $a, b \in G$ the equation $ax = b$ and $ya = b$ have unique solutions in $G : x = a^{-1}b$ and $y = ba^{-1}$.

Let G be a semigroup. G is a group iff the following conditions hold:

- there exists an element $e \in G$ such that $ea = a$ for all $a \in G$ (left identity element);
- for each $a \in G$, there exists an element $a^{-1} \in G$ such that $a^{-1}a = e$ (left inverse).

and an analogous result holds for "right inverses" and a "right identity".

Let G be a semigroup. G is a group iff for all $a, b \in G$ the equations $ax = b$ and $ya = b$ have solutions in G.

Proof. $\square$

Let S be a nonempty set and $A(S)$ the set of all bijections $S \to S$. Under the operation of composition of functions, $\circ$, $A(S)$ is a group. The elements of $A(S)$ are called *permutations* and $A(S)$ is called the group of permutations on the set S. If $S = \{1, 2, 3, \cdots, n\}$, then $A(S)$ is called the symmetric group on n letters and denoted S_n. $|S_n| = n!$.

Definition 7
The *direct product* of two groups G and H with identities e_G and e_H is the group whose underlying set is $G \times H$ and whose binary operation is given by:

$$(a, b)(a', b') = (aa', bb'), \qquad \text{where } a, a' \in G; b, b' \in H$$

$G \times H$ is abelian if both G and H are; (e_G, e_H) is the identity and (a^{-1}, b^{-1}) is the inverse of (a, b). Clearly $|G \times H| = |G||H|$.

Theorem 8
Let $R(\sim)$ be an equivalence relation on a monoid G such that a_1 a_2 and b_1 b_2 imply a_1b_1 a_2b_2 for all $a_i, b_i \in G$. Then the set G/R of all equivalence classes of G under R is a monoid under the binary operation defined by $(\bar{a})(\bar{b}) = \overline{ab}$, where $\bar{x}$ denoted the equivalence class of $x \in G$. If G is an [abelian] group, then so is G/R.An equivalence relation on a monoid G that satisfies these hypothesis is called a **congruence relation** on G.

The following relation on the additive froup is a congruence relation:

$$a \sim b \Leftrightarrow a - b \in$$

The set of equivalence classes (denoted /) is an infinite abelian group, with addition given by $\bar{a} + \bar{b} = \overline{a + b}$, and called the *group of rationals modulo one*.

Definition 9

The *meaningful product* on any sequence of elements of a semigroup G, $\{a_1, a_2, \cdots\}$, $a_1, \cdots, a_n$(in this order), is defined inductively as below: If $n = 1$, the only meaningful product is a_1. If $n > 1$, then a meaningful product is defined to be any product of the form $(a_1 \cdots a_m)(a_{m+1} \cdots a_n)$ where $m < n$ and $(a_1 \cdots a_m)$ and $(a_{m+1} \cdots a_n)$ are meaningful products of m and $n - m$ elements respectively.

Definition 10

The *standard n product* $\prod_{i=1}^{n} a_i$ is defined as follows:

$$\prod_{i=1}^{1} a_i = a_i; \qquad \text{for } n > 1, \prod_{i=1}^{n} a_i = (\prod_{i=1}^{n-1} a_i) a_n$$

Theorem 11 (Generalized Associative Law)

If G is a semigroup and $a_1, \cdots, a_n \in G$, then any two meaningful products of $a_1, \cdots, a_n$ in this order are equal.

Theorem 12 (Generalized Commutative Law)

If G is a commutative semigroup and $a_1, \cdots, a_n \in G$, then for any permutation $i_1, \cdots, i_n$ of $1, 2, \cdots, n$, $a_1 a_2 \cdots a_n = a_{i_1} a_{i_2} \cdots a_{i_n}$.

Definition 13

Let G be a semigroup, $a \in G$ and $n \in$. The element $a^n \in G$ is defined to be the standard n product $\prod_{i=1}^{n} a_i$ with $a_i = a$ for $1 \leqslant i \leqslant n$. If G is a monoid, a^0 is defined to be the identity element e. If G is a group, then for each $n \in$, a^{-n} is defined to be $(a^{-1})^n \in G$.

Theorem 14

If G is a group(resp. semigroup, monoid) and $a \in G$, then for all $m, n \in$ (resp. and $\cup\{0\}$) :

- $a^m a^n = a^{m+n}$
- $(a^m)^n = a^{mn}$

1.2 Homomorphisms and Subgroups

Definition 15

Let G and H be semigroups. A function $f : G \to H$ is a *homomorphism* provided

$$f(ab) = f(a)f(b) \text{ for all } a, b \in G$$

If f is injective as a map of sets, f is said to be a *monomorphism*. If f is surjective, f is called an *epimorphism*. If f is bijective, f is called an *isomorphism*. In this case G and H are said to be *isomorphic* (written $G \cong H$). A homomorphism $f : G \to G$ is called an *endomorphism* of G and an isomorphism $f : G \to G$ is called an *automorphism* of G.

Definition 16

Let $f : G \to H$ be a homomorphism of groups. The *kernel* of f(denoted $\operatorname{Ker} f$) is $\{a \in G | f(a) = e \in H\}$. If A is a subset of G, then $f(A) = \{b \in H | b = f(a) \text{ for some } a \in A\}$ is the *image of* A. $f(G)$ is called the *image of* f and denoted $\operatorname{Im} f$. If B is a subset of H, $f^{-1}(B) = \{a \in G | f(a) \in B\}$ is the *inverse image* of B.

Theorem 17

Let $f : G \to H$ be a homomorphism of groups. Then

- f is a monomorphism iff $\operatorname{Ker} f = \{e\}$.
- f is an isomorphism iff there is a homomorphism $f^{-1} : H \to G$ such that $ff^{-1} = 1_H$ and $f^{-1}f = 1_G$.

Definition 18

Let G be a semigroup and H a nonempty subset of it. If for every $a, b \in H$ we have $ab \in H$, we say that H is *closed* under the product in G. This is the same as saying that the binary operation on G, when restricted to H, is a binary operation on H.

Definition 19

Let G be a group and H a nonempty subset that is closed under the product in G. If H is itself a group under the product in G, then H is said to be a *subgroup* of G, denoted $H < G$.

Definition 20

If a subgroup H is not G itself or the *trivial subgroup*, which consists only of the identity element, is called a *proper subgroup*.

Theorem 21

Let H be a nonempty subset of a group G. Then H is a subgroup of G iff $ab^{-1} \in H$ for all $a, b \in H$.

If G is a group and $\{H_i | i \in I\}$ is a nonempty family of subgroups, then $\bigcap_{i \in I} H_i$ is a subgroup of G.

Definition 22
Let G be a group and X a subset of G. Let $\{H_i | i \in I\}$ be the family of all subgroups of G which contain X. Then $\bigcap_{i \in I} H_i$ is called the *subgroup of G generated by the set X* and denoted X. The elements of X are the *generators* of X. If $G = a_1, \cdots, a_n, (a_i \in G)$, G is said to be finitely generated. If $a \in G$, the subgroup a is called the *cyclic (sub)group* generated by a.

Theorem 23
If G is a group and X a nonempty subset of G, then the subgroup X generated by X consists of all finite products $a_1^{n_1} a_2^{n_2} \cdots a_t^{n_t} (a_i \in X; n_i \in)$. In particular for every $a \in G$, $a = \{a^n | n \in\}$.

Definition 24
The subgroup $\bigcap_{i \in I} H_i$ generated by the set $\bigcap_{i \in I} H_i$ is called the *subgroup generated by the groups* $\{H_i | i \in I\}$. If H and K are subgroups, the subgroup $H \cup K$ generated by H and K is called the *join* of H and K and is denoted $H \vee K$.

1.3 Cyclic Groups

Definition 25
A *cyclic group* or *monogenous group* is a group that is generated by a single element. That is, it consists of a set of elements with a single invertible associative operation, and it contains an element such that every other element of the group may be obtained by repeatedly applying the group operation or its inverse to it.

Theorem 26
Every subgroup H of the additive group is cyclic. Either $H = 0$ or $H = m$, where m is the least positive interger in H. If $H \neq 0$, then H is infinite.

Theorem 27
Every infinite cyclic group is isomorphic to the additive group and every finite group of order m is isomorphic to the additive group $_m$.

Definition 28
Let G be a group and $a \in G$. The *order* of a is the order of the cyclic subgroup a and is denoted $|a|$.

Theorem 29

Let G be a group and $a \in G$. If a has infinite order, then

- $a^k = e$ iff $k = 0$;
- the elements $a^k (k \in)$ are all distinct.

If a has inite order $m > 0$, then

- m is the least positive integer such that $a^m = e$;
- $a^k = e$ iff $m|k$;
- $a^r = a^s$ iff $r \equiv s(\text{mod} m)$;
- a consists of the distinct elements $a, a^2, \cdots, a^{m-1}, a^m = e$;
- for each k such that $k|m$, $|a^k| = m/k$.

Theorem 30

Every homomorphic image and every subgroup of a cyclic group G is cyclic. In particular, if H is a nontrivial subgroup of $G = a$ and m is the least positive integer such that $a^m \in H$, then $H = a^m$.

Theorem 31

Let $G = a$ be a cyclic group. If G is infinite, then a and a^{-1} are the only generators of G. If G is finite of order m, then a^k is a generator of G iff $(k, m) = 1$.

Definition 32

The *center* C of a group G is defined as $C = \{a \in G | (\forall x \in G) ax = xa\}$. In other words, it contains the members of G that are commutative under the binary operation on G. The center of a group is an abelian subgroup of it.

Definition 33

The Klein Four Group, defined as the symmetries on rectangle that preserves distance, is the smallest non-cyclic group(all its elements has order 2) and is isomorphic to $Z_2 \oplus Z_2$(which says that the Klein Four Group is abelian)

1.4 Cosets and Counting

Definition 34

Let H be a subgroup of a group G and $a, b \in G$. a is *right congruent to b modulo H*, denoted $a \equiv_r b(\text{mod } H)$ if $ab^{-1} \in H$. a is *left congruent to b modulo H* , denoted $a \equiv_l b(\text{mod } H)$ if $a^{-1}b \in H$.

Theorem 35

Let H be a subgroup of a group G.

- Right(resp. left) congruence modulo H is an equivalence relation on G.
- The equivalence class of $a \in G$ under right(resp. left) congruence modolo H is the set $Ha = \{ha | h \in H\}$(resp. $aH = \{ah | h \in H\}$).
- $|Ha| = |H| = |aH|$ for all $a \in G$.

Definition 36

The set Ha above is called a *right coset* of H in G and aH is called an *left coset* of H in G.

Let H be a subgroup of a group G.

- G is the union of the right(resp. left) cosets of H in G.
- Two right(resp. left) cosets of H in G are either disjoint or equal.
- For all $a, b \in G$, $(Ha = Hb) \Leftrightarrow (ab^{-1} \in H)$ and $(aH = bH) \Leftrightarrow (a^{-1}b \in H)$.
- If $\mathcal{R}$ is the set of distinct right cosets of H in G and $\mathcal{L}$ is the set of distinct left cosets of H in G, then $|\mathcal{R}| = |\mathcal{L}|$.

Proof. The first three statements are consequences of properties of equivalence classes. For (iv) it's easy to see that the map $\mathcal{R} \to \mathcal{L}$ given by $Ha \to a^{-1}H$ is a bijection. □

Definition 37

Let H be a subgroup of a group G. The *index of H in G*, denoted $[G : H]$, is the cardinal number of the set of distince right(resp. left) cosets of H in G.

Definition 38

A *complete set of right coset representatives* of a subgroup H in a group G is a set $\{a_i\}$ consisting of precisely one element from each right coset of H in G and having cardinality $[G : H]$.

Theorem 39

If K, H, G are groups with $K < H < G$, then $[G : K] = [G : H][H : K]$. If any two of these indices are finite, then so is the third.

Proof. By previous Corollary $G = \bigcup_{i \in I} Ha_i$ with $a_i \in G$, $|I| = [G : H]$ and the cosets Ha_i are mutually disjoint. Similarly $H = \bigcup_{j \in J} Kb_j$ with $b_j \in H$, $|J| = [H : K]$ and the cosets Kb_j are mutually disjoint. Therefore $G = \bigcup_{i \in I} Ha_i = \bigcup_{i \in I}(\bigcup_{j \in J} Kb_j)a_i = \bigcup_{(i,j) \in I \times J} Kb_ja_i$. It suffices to show that the cosets Kb_ja_i are mutually disjoint, for then we must have $[G : K] = |I \times J| = |I||J| = [G : H][H : K]$. If $Kb_ja_i = Kb_ra_t$, then $b_ja_i = kb_ra_t (k \in K)$ (because $Kk = Ke = K$). Since $b_j, b_r, k \in H$ we have $Ha_i = Hb_ja_i = Hkb_ra_t = Ha_t$, hence $i = t$ and $b_j = kb_r$. Thus $Kb_j = Kkb_r = Kb_r$ and $j = r$. Therefore the cosets Kb_ja_i are mutually disjoint. The last statement of the theorem is obvious. □

[Lagrange] If H is a subgroup of a group G, then $|G| = [G : H]|H|$. In particular if G is finite, the order $|a|$ of $a \in G$ devides $|G|$.

Proof. Apply the theorem with $K = \langle e \rangle$ for the first statement. The second is a special case of the first with $H = \langle a \rangle$. $\square$

Theorem 40

If the set $\{ab | a \in H, b \in K\}$ is denoted HK, then for two finite subgroups H and K of a group G $|HK| = |H||K|/|H \cap K|$.

Proof. $C = H \cap K$ is a subgroup of K of index $n = |K|/|H \cap K|$ (apply the Lagrange Corollary) and K is the disjoint union of right cosets $Ck_1 \cup Ck_2 \cup \cdots \cup Ck_n$ for some $k_i \in K$ (because C is a subgroup of K). Since $HC = H$, this implies that $HK = HCk_1 \cup HCk_2 \cup \cdots \cup HCk_n = Hk_1 \cup Hk_2 \cup \cdots \cup Hk_n$, which are disjoint. Therefore, $|HK| = |H| \cdot n = |H||K|/|H \cap K|$. $\square$

If H and K are subgroups of a group G, then $[H : H \cap K] \leqslant [G : K]$. If $[G : K]$ is finite, then $[H : H \cap K] = [G : K]$ iff $G = KH$.

Proof. Let A be the set of all right cosets of $H \cap K$ in H and B the set of all right cosets of K in G. The map $\varphi : A \to B$ given by $(H \cap K)h \mapsto Kh (h \in H)$ is well defined since $(H \cap K)h' = (H \cap K)h$ implies $h'h^{-1} \in H \cap K \subset K$ and hence $Kh' = Kh$. To show that φ is injective, noted that for $Kh' = Kh (h \in H)$ we have $Hh' = Hh$, thus $Kh' \cap Hh' = Kh \cap Hh \Leftrightarrow (H \cap K)h' = (H \cap K)h$. Then $[H : H \cap K] = |A| \leqslant |B| = [G : K]$. If $[G : K]$ is finite, clearly $[H : H \cap K] = [G : K]$ iff φ is surjective. Suppose that φ is surjective but $G \neq KH$. Then there exist an element $g \in G$ such that $g \neq kh$ for all $k \in K, h \in H$. Then $Kg \neq K(kh) \Leftrightarrow Kg \neq Kh$. Since h is arbitrary, the non-existence of $\varphi^{-1}(Kg)$ and that $Kg \in B$ contradicts with the fact that φ is a bijection. If $G = KH$, we have that for any $Kg \in B (g \in G)$ the mapping φ^{-1} is defined, thus it must be surjective. $\square$

Let H and K be subgroups of finite index of a group G. Then $[G : H \cap K]$ is finite and $[G : H \cap K] \leqslant [G : H][G : K]$. Furthermore, $[G : H \cap K] = [G : H][G : K]$ iff $G = HK$.

Proof. This proposition is an easy consequence of previous proposition and theorem. $\square$

1.5 Normality, Quotient Groups, and Homomorphisms

Theorem 41

If N is a subgroup of a group G, then the following conditions are equivalent.

1. Left and right congruence modulo N coincide (that is, define the same equivalence relation on G);
2. every left coset of N in G is also a right coset of N in G;
3. $aN = Na$ for all $a \in G$;
4. for all $a \in G$, $aNa^{-1} \subset N$;
5. for all $a \in G$, $aN^{-1} = N$

Definition 42

A subgroup N of a group G which satisfies the equivalent conditions of the previous theorem is said to be *normal* in G (or a *normal subgroup* in G); we write $N \lhd G$ if N is normal in G.

Theorem 43

Let K and N be subgroups of a group G with N normal in G. Then

1. $N \cap K$ is a normal subgroup of K;
2. N is a normal subgroup of $N \vee K$;
3. $NK = N \vee K = KN$;
4. if K is normal in G and $K \cap N = \langle e \rangle$, then $nk = kn$ for all $k \in K$ and $n \in N$.

Proof.
1. If $n \in N \cap K$, then for an element $k \in K < G$ $knk^{-1} \in N$ and $knk^{-1} \in K$. Thus $k(N \cap K)k^{-1} \subset N \cap K$ and $N \cap K \lhd K$.
2. It is trivial.
3. All elements of $N \vee K$ are of the form $n_1k_1n_2k_2 \cdots n_rk_r$, where $n_i \in N$ and $k_i \in K$. Since $N \lhd G$, $n_ik_j = k_jn_i'$ (because $k_jn_i'k_j^{-1} \in N$) and therefore these elements can be written in the form $n(k_1 \cdots k_r), n \in N$. Thus $N \vee K \subset NK$. Since $NK \subset N \vee K$, we have $NK = N \vee K$. Similarly $KN = N \vee K$.
4. Let $k \in K$ and $n \in N$. Then $nkn^{-1} \in K$ and $kn^{-1}k^{-1} \in N$. Hence $(nkn^{-1}) = n(kn^{-1}k^{-1}) \in N \cap K = \langle e \rangle$, which implies $nk = kn$.

□

Theorem 44

If $N \lhd G$ and G/N is the set of all (left) cosets of N in G, then G/N is a group of order $[G : N]$ under the binary operation given by $(aN)(bN) = abN$.

Proof. Since the coset aN is simply the equivalence class of $a \in G$ under the equivalence relation of congruence modulo N, it suffices to show that congruence modulo N is a congruence relation, that is, that $a_1 \equiv a \pmod N$ and $b_1 \equiv b \pmod N$ imply $a_1b_1 \equiv ab \pmod N$. By assumption $a_1a^{-1} = n_1 \in N$ and $b_1b^{-1} = n_2 \in N$. Hence $(a_1b_1)(ab)^{-1} = a_1b_1b^{-1}a^{-1} = (a_1n_2)a^{-1}$. But since N is normal, $a_1N = Na_1$ which implies that $a_1n_2 = n_3a_1$ for some $n_3 \in N$. Consequently $(a_1b_1)(ab)^{-1} = (a_1n_2)a^{-1} = n_3a_1a^{-1} = n_3n_1 \in N$, whence $a_1b_1 \equiv ab \pmod N$. □

Definition 45

If N is a normal subgroup of a group G, then the group G/N as defined before is called the *quotient group* of *factor group* of G by N. If G is written additively, then the group operation in G/N is given by $(a + N) + (b + N) = (a + b) + N$.

$_m = /\langle m \rangle.$

Theorem 46

If $f : G \to H$ is a homomorphism of groups, then the kernel of f is a normal subgroup of G. Conversely, if N is normal in G, then the map $\pi : G \to G/N$ given by $\pi(a) = aN$ is an epimorphism with kernel N.

Proof. If $x \in \operatorname{Ker} f$ and $a \in G$, then clearly $f(axa^{-1}) = e$ and therefore $\ker f \lhd G$. The map π is clearly surjective and since $\pi(ab) = abN = aNbN = \pi(a)\pi(b)$, it is an epimorphism. $\operatorname{Ker} \pi = \{a \in G | \pi(a) = eN = N\} = \{a \in G | aN = N\} = \{a \in G | a \in N\} = N$. □

Definition 47

The map $\pi : G \to G/N$ is called the *canonical epimorphism* or *projection*. Unless otherwise stated $G \to G/N (N \lhd G)$ always denotes the canonical epimorphism.

Theorem 48

If $f : G \to H$ is a homomorphism of groups and N is a normal subgroup of G contained in the kernel of f, then there is a unique homomorphism $\bar{f} : G/N \to H$ such that $\bar{f}(aN) = f(a)$ for all $a \in G$. $\operatorname{Im} f = \operatorname{Im} \bar{f}$ and $\operatorname{Ker} \bar{f} = (\operatorname{Ker} f)/N$. $\bar{f}$ is an isomorphism iff f is an epimorphism and $N = \operatorname{Ker} f$.

This essential part of the conclusion may be rephrased: there exists a unique homomorphism $\bar{f} : G/N \to H$ such that the diagram

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[d] & H \\ G/H \arrow[ur, "\bar{f}"'] & \end{tikzcd}$$

is commutative.

Proof. If $b \in aN$, then $b = an$, $n \in N$, and $f(b) = f(an) = f(a)f(n) = f(a)$ since $N < \operatorname{Ker} f$. Therefore, f has the same effect on every element of the coset aN and the map $\bar{f} : G/N \to H$ given by $\bar{f}(aN) = f(a)$ is a well-defined function. Since $\bar{f}(aNbN) = \bar{f}(abN) = f(ab) = f(a)f(b) = \bar{f}(aN)\bar{f}(bN)$, $\bar{f}$ is a homomorphism. Clearly $\operatorname{Im} f = \operatorname{Im} \bar{f}$ and

$$aN \in \operatorname{Ker} \bar{f} \Leftrightarrow f(a) = e \Leftrightarrow a \in \operatorname{Ker} f$$

whence $\operatorname{Ker} \bar{f} = \{aN | a \in \operatorname{Ker} f\} = (\operatorname{Ker} f)/N$. $\bar{f}$ is unique since it is completely determined by f. It is clear that $\bar{f}$ is an epimorphism iff f is. $\bar{f}$ is a monomorphism if its kernel is the trivial subgroup of G/N, which occurs iff $\operatorname{Ker} f = N$. □

Definition 49

A *commutative diagram* is a diagram consists of arrows and objects such that all directed paths that has the same start and endpoints yield the same result.

(First Isomorphism theorem) If $f : G \to H$ is a homomorphism of groups, then f induces an isomorphism $G/(\operatorname{Ker} f) \cong \operatorname{Im} f$.

Proof. Clearly $f : G \to \operatorname{Im} f$ is an epimorphism. Apply the previous theorem with $N = \operatorname{Ker} f$ yield the desired result. $\square$

If $f : G \to H$ is a homomorphism of groups, $N \lhd G$, $M \lhd H$, and $f(N) < M$, then f induces a homomorphism $\bar{f} : G/N \to H/M$, given by $aN \mapsto f(a)M$.
$\bar{f}$ is an isomorphism iff $\operatorname{Im} f \vee M = H$ and $f^{-1}(M) \subset N$. In particular if f is an epimorphism such that $f(N) = M$ and $\operatorname{Ker} f \subset N$, then $\bar{f}$ is an isomorphism.

Proof. Consider the composition $G \xrightarrow{f} H \xrightarrow{\pi} H/M$. $N \subset f^{-1}(M)$ because $f(N) < M$. Apparently $\pi f(a) = f(a)M$, then the kernel of πf consists of those elements whose image is in M, which is equivalent to $\operatorname{Ker} \pi f = f^{-1}(M)$. Apply the previous theorem to πf the map $G/N \to H/M$ given by $aN \mapsto \pi f(a) = f(a)M$ is a homomorphism that is an isomorphism iff πf is an epimorphism and $N = \operatorname{Ker} \pi f$. But the latter conditions hold iff $\operatorname{Im} f \vee M = H$ and $f^{-1}(M) \subset N$: the second part is trivial; for the first one, πf is an epimorphism implies that there exists some $g \in G$ such that $\pi f(g) = hM$ for all distinct cosets in H/M, then $H = \operatorname{Im} f M = \operatorname{Im} f \vee M$; conversely, if $\operatorname{Im} f \vee M = H$, we have $\operatorname{Im} f M = H$, which says that there exist some elements $f(a_1), f(a_2), \cdots$ in $\operatorname{Im} f$ that are the distinct cosets of M in H, which says that there must exists some a_i for any $hM \in H/M$. If f is an epimorphism, then $H = \operatorname{Im} f = \operatorname{Im} f \vee M$. If $f(N) = M$ and $\operatorname{Ker} f \subset N$, then $f^{-1}(M) \subset N$, whence $\bar{f}$ is an isomorphism. $\square$

(Second Isomorphism theorem) If K and N are subgroups of a group G with $N \lhd G$, then $K/(N \cap K) \cong NK/N$.

Proof. $N \lhd NK = N \vee K$. The composition $K \xrightarrow{h} NK \xrightarrow{\pi} NK/N$ is a homomorphism f with kernel $K \cap N$, whence $\bar{f} : K/K \cap N \cong \operatorname{Im} f$. Every element in NK/N is of the form nkN. The normality of N implies that $nk = kn_1$, whence $nkN = kn_1N = kN = f(k)$. Therefore f is an epimorphism and hence $\operatorname{Im} f = NK/N$. $\square$

(Third Isomorphism theorem) If H and K are normal subgroups of a group G such that $K < H$, then H/K is a normal subgroup of G/K and $(G/K)/(H/K) \cong G/H$.

Proof. The identity map $1_G : G \to G$ has $1_G(K) < H$ and therefore induces an epimorphism $I : G/K \to G/H$, with $I(aK) = aH$. Since $H = I(aK)$ iff $a \in H$, $\operatorname{Ker} I = \{aK | a \in H\} = H/K$. Hence $H/K \lhd G/K$ and $G/H = \operatorname{Im} I \cong (G/K)/\operatorname{Ker} I = (G/K)/(H/K)$. $\square$

Theorem 50
If $f : G \to H$ is an epimorphism of groups, then the assignment $K \mapsto f(K)$ defines a bijection between the set $S_f(G)$ of all subgroups K of G which contain $\operatorname{Ker} f$ and the set $S(H)$ of all subgroups of H. Under the bijection normal subgroups correspond to normal subgroups.

Proof. The assignment $K \mapsto f(K)$ defines a function $\varphi : S_f(G) \to S(H)$ and $f^{-1}(J)$ is a subgroup of G for every subgroup J of H. Since $J < H$ implies $\operatorname{Ker} f < f^{-1}(J)$ and $f(f^{-1}(J)) = J$, φ is surjective (since for any subgroup $J < H$ we have another subgroup $J < H$ such that it is the image of a subgroup $f^{-1}(J)$ in G). $f^{-1}(f(K)) = K \operatorname{Ker} f$ since $f(K \operatorname{Ker} f) = f(K)f(\operatorname{Ker} f)$, $f^{-1}(f(K)) = K$ iff $\operatorname{Ker} f < K$. It follows that φ is injective. If $K \lhd G$, then $f(K) = f(gKg^{-1}) = f(g)f(K)f(g)^{-1} = f(K)$. The argument for $J \lhd H$ and for $f^{-1}(J)$ is similar. $\square$

If N is a normal subgroup of a group G, then every subgroup of G/N is of the form K/N, where K is a subgroup of G that contains N. Furthermore, K/N is normal in G/N iff K is normal in G.

Proof. Apply the theorem above to the canonical epimorphism $\pi : G \to G/N$. If $N < K < G$, then $\pi(K) = K/N$. $\square$

1.6 Symmetric, Alternating, and Dihedral Groups

Definition 51

Let $i_1, i_2, \cdots, i_r$, $(r < n)$ be distinct elements of $I_n = \{1, 2, \cdots, n\}$. Then $(i_1 i_2 i_3 \cdots i_r)$ denotes the permutation that moves each element to the element on its right (i_1 to i_2, i_r to i_1, etc.) and fix elements in I_n that are not in $i_1, \cdots, i_r$. $(i_1 i_2 \cdots i_r)$ is called a *cycle* of length r or an *r-cycle*; a 2-cycle is called a *transposition*.

Definition 52

The permutations $\sigma_1, \sigma_2, \cdots, \sigma_r$ of S_n are said to be *disjoint* provided that for each $1 \leqslant i \leqslant r$, and every $k \in I_n$, $\sigma_i(k) \neq k$ implies $\sigma_j(k) = k$ for all $j \neq i$. In other words, an element of I_n will only be moved once if we apply all of σ_i to it. In this case the composition of disjoint permutations commutes.

Theorem 53

Every nonidentity permutation in S_n is uniquely a product of disjoint cycles, each of which has length at least 2.

Definition 54

Define an equivalence relation on I_n with a given permutation σ as follows: $x \sim y$ iff $y = \sigma^m(x)$ for some $m \in$. The equivalence classes are called the *orbit* for σ and form a partition of I_n. Note that if $x \in B_i$, then B_i consists of all elements $\{x, \sigma(x), \sigma^2(x), \cdots, \sigma^d(x)\}$ for some $d \in$.

The order of a permutation $\sigma \in S_n$ is the least common multiplier of the order of its disjoint cycles. Every permutation in S_n can be written as a product of (not necessarily disjoint) transpositions.

Definition 55

A permutation $\tau \in S_n$ is said to be *even* (resp. *odd*) if τ can be written as a product of an even (resp. odd) number of transpositions.

The *sign of a permutation* τ, denoted τ, is 1 or -1 according as τ is even or odd.

Theorem 56

A permutation $\tau \in S_n (n \geqslant 2)$ cannot be both even and odd.

Theorem 57
For each $n \geqslant 2$, let A_n be the set of all even permutations of S_n. Then A_n is a normal subgroup of S_n of index 2 and order $|S_n|/2 = n!/2$. Furthermore A_n is the only subgroup of S_n of index 2.

The proof proceeds from the following two lemmas.

Lemma 58
If $H < G$ and $[G : H] = 2$, then H contains all squares of elements in G.

Proof. Let $g \in G$ be arbitrary. if $gH = H$, the lemma is trivial. If $gH = aH$ for some $a \notin H$, then we have $g^2H = a^2H$; if $aH \neq a^2H = H$, the lemma obviously holds. If $aH = a^2H$, the lemma also holds. □

Lemma 59
If H is a subgroup of index 2 in G, then H contains all elements of odd order in G.

Proof. Suppose that an element $g \in G$ has order $2k + 1 (k \in)$. Then $H = g^{2k+1}H = (g^k)^2H \cdot gH = gH$. □

Then it follows that since any permutation of order 3(like all 3-cycles) is contained in any subgroup of index 2 (which must be normal) of S_n, it must be A_n.

Definition 60
A group is said to be *simple* if it has no proper normal subgroups.

Theorem 61
The alternating group A_n is simple iff $n \neq 4$.

The proof of the theorem proceeds from two lemmas below.

Lemma 62
Let r, s be distinct elements of $\{1, 2, \cdots, n\}$. Then $A_n(n \geqslant 3)$ is generated bu the 3-cycles $\{(rsk)|1 \leqslant k \leqslant n, k \neq r, s\}$.

Lemma 63
If $N \lhd A_n(n \geqslant 3)$ and N contains a 3-cycle, then $N = A_n$.

Definition 64

The subgroup D_n of $S_n (n \geqslant 3)$ generated by $a = (123 \cdots n)$ and

$$b = \begin{pmatrix} 1 & 2 & 3 & \cdots & i & \cdots & n-1 & n \\ 1 & n & n-1 & \cdots & n+2-i & \cdots & 3 & 2 \end{pmatrix}$$
$$= \prod_{2 \leqslant i < n+2-i} (i \quad n+2-i)$$

is called the *dihedral group of degree* n. The group D_n is isomorphic to and usually identified with the group of all symmetries of a regular polygon with n sides.

Theorem 65

For each $n \geqslant 3$ the dihedral group D_n is a group of order $2n$ whose generators a and b satisfy:

1. $a^n = (1)$; $b^2 = (1)$; $a^k \neq (1)$ if $0 < k < n((1)$ is the identity permutation);
2. $ba = a^{-1}b$

Any group G which is generated by elements $a, b \in G$ satisfying both conditions for some $n \geqslant 3$ is isomorphic to D_n.

1.7 Categories: Products, Coproducts, and Free Objects

Definition 66

A *category* is a class C of objects (denoted $A, B, C, \ldots$) together with

1. a class of disjoint sets, denoted $\hom(A, B)$, one(set) for each pair of objects in C; an element of $\hom(A, B)$ is called a *morphism* from A to B and denoted $f : A \to B$.
2. for each triple (A, B, C) of objects of C a function

$$\hom(B, C) \times \hom(A, B) \to \hom(A, C)$$

which is the *composite* of morphisms. The composition must be associative. An identity morphism $1_B : B \to B$ also exists and for any $f : A \to B$ and $g : B \to C$

$$1_B \circ f = f \qquad \text{and} \qquad g \circ 1_B = g$$

Definition 67

In a category C a morphism $f : A \to B$ is called an *equivalence* if there is in C a morphism $g : B \to A$ such that $g \circ f = 1_A$ and $f \circ g = 1_B$. The composite of two equivalences, when defined, is an equivalence. If $f : A \to B$ is an equivalence, A and B are said to be *equivalent*.

For S, the class of all sets, equipped with functions between these sets as morphisms, a morphism is an equivalence iff it is bijective. For G, the category of all groups, equipped with homomorphisms between these groups as morphisms, a morphism is an equivalence iff it is an isomorphism. A (multiplicative) group G can be considered as a category with one object G. Let $\hom(G, G)$ be the set of elements of G(then each morphism is an element of G); composite of morphisms is simply the composition given by the binary operation in G. Every morphism is an equivalence and 1_G is the identity element e of G. **This example shows that morphisms need not to be functions**. In this case it is said that the category is not concrete.

Definition 68

Let C be a category and $\{A_i | i \in I\}$ a family of objects of C. A *product* for the family $\{A_i | i \in I\}$ is an object P of C together with a family of morphisms $\{\pi_i : P \to A_i | i \in I\}$ such that for any object B and family of morphisms $\{\varphi_i : B \to A_i | i \in I\}$, there is a unique morphism $\varphi : B \to P$ such that $\pi_i \circ \varphi = \varphi_i$ for all $i \in I$. The product of $\{A_i | i \in I\}$ is usually denoted $\prod_{i \in I} A_i$.

$$\begin{tikzcd} & B \arrow[dl, "\varphi_1"'] \arrow[d, "\varphi"] \arrow[dr, "\varphi_2"] & \\ A_1 & P \arrow[l, "\pi_1"] \arrow[r, "\pi_2"'] & A_2 \end{tikzcd}$$

When $I = \{1, 2\}$, the product P expressed using a commutative diagram:
In the category of sets the Cartesian product $\prod_{i \in I} A_i$ is a product of the family of sets $\{A_i\}$. The map π_i would be the canonical projections onto the ith components. The map φ would be $(\varphi_1, \varphi_2, \cdots, \varphi_i)$ that takes an element of B and maps it to an element of $\prod_{i \in I} A_i$.

Theorem 69

If $(P, \{\pi_i\})$ and $(Q, \{\psi_i\})$ are both products of the family $\{A_i | i \in I\}$ of objects of a category C, then P and Q are equivalent.

Definition 70

A *coproduct* (or *sum*) for the family $\{A_i | i \in I\}$ of objects in a category C is an object S of C, together with a family of morphisms $\{\iota_i : A_i \to S | i \in I\}$ such that for any object B and family of morphisms $\{\psi_i : A_i \to B | i \in I\}$, there is a unique morphism $\psi : S \to B$ such that $\psi \circ \iota_i = \psi_i$ for all $i \in I$. Although no universal notation exists for coproducts, it is usually denoted $\coprod_{i \in I} A_i$.

It's easy to see that by reversing the arrows in the commutative diagram above for product we obtain the diagram for coproduct.

Theorem 71

If $(S, \{\iota_i\})$ and $(S', \{\lambda_i\})$ are both products of the family $\{A_i | i \in I\}$ of objects of a category C, then S and S' are equivalent.

Definition 72

A *concrete category* is a category C together with a function σ that assigns to each object A of C a set $\sigma(A)$(called the underlying set of A) in such a way that:

1. every morphism $A \to B$ of C is a function on the underlying sets $\sigma(A) \to \sigma(B)$;
2. the identity morphism of each object A of C is the identity function on the underlying set $\sigma(A)$;
3. composition of morphisms in C agrees with composition of functions on their underlying sets.

It is worth noticing that in a concrete category morphisms are also functions on their corresponding underlying sets, but maps, functions on these underlying sets, might not be morphisms.

Definition 73

Let F be an object in a concrete category C, X a nonempty set, and $i : X \to F$ a map (of sets). F is *free on the set* X provided that for any object A of C and maps (of sets) $f : X \to A$, there exists a unique morphism of C, $\bar{f} : F \to A$, such that $\bar{f} i = f$ (as a map of sets $X \to A$).

$$\begin{tikzcd} F \arrow[dr, "\bar{f}"] & \\ X \arrow[u, "i"] \arrow[r, "f"'] & A \end{tikzcd}$$

The essential fact about a free object F is that in order to define a morphism with domain F, it suffices to specify the image of the subset $i(X)$. Let G be any group and $g \in G$. Then the map $\bar{f} :\to G$ defined by $\bar{f}(n) = g^n$ is the unique homomorphism $\to G$ such that $1 \mapsto g$. Consequently, if $X = \{1\}$ and $i : X \to$ is the inclusion map, then is free on X in the category of groups. In other words, to determine a unique homomorphism from to G we need only specify the image of $1 \in$ (that is, the image of $i(X)$).

Theorem 74

If C is a concrete category, F and F' are objects of C such that F is free on the set X and F' is free on the set X' and $|X| = |X'|$, then F is equivalent to F'.

We have seen that two products(resp. coproducts) for a given family of objects are equivalent. Likewise two free objects on the same set are equivalent. This characteristic is captured via the following definition.

Definition 75

An object I in a category C is said to be *universal* (or *initial*) if for each object C of C there exists one and only one morphism $I \to C$. An object T of C is said to be *couniversal* (or *terminal*) if for each object C of C there exists one and only one morphism $C \to T$.

Theorem 76

Any two universal (resp. couniversal) objects in a category C are equivalent.

The trivial group is both universal and couniversal in the category of groups.

Definition 77
In the category of sets, the *disjoint union* of the sets A_i is defined on a family of sets $\{A_i|i \in I\}$ as $\bigcup A_i = \{(a,i) \in (\bigcup_{i\in I} A_i) \times I | a \in A_i\}$(notice the subscript under the union sign).

1.8 Direct Products and Direct Sums

Definition 78
We extend the definition of the *product* $G \times H$ of groups G and H to an arbitrary family $\{G_i|i \in I\}$ of groups, in which the multiplication is still defined component-wise. It is called the *direct product*(or *complete direct sum*) of the family of groups. If $I = \{1, 2, \cdots, n\}$, $\prod_{i\in I} G_i$ is usually denoted $G_1 \times G_2 \times G_3 \times \cdots \times G_n$ (or in additive notation, $G_1 \bigoplus G_2 \bigoplus G_3 \bigoplus \cdots \bigoplus G_n$).

Theorem 79
If $\{G_i|i \in I\}$ is a family of groups, then

1. the direct product is a group;
2. for each $k \in I$, the map $\pi_k : \prod_{i\in I} G_i \to G_k$ given by $f \mapsto f(k)$(here $f : I \to \bigcup_{i\in I} G_i$ and $f(i) \in G_i$ for each i)[or $\{a_i\} \mapsto a_k$] is an epimorphism of groups.

Definition 80
The mappings π_k previously mentioned are called the *canonical projections* of the direct product.

Theorem 81
$\prod_{i=1} G_i$ is a product in the category of groups.

Definition 82
The *(external) weak direct product* of a family of groups $\{G_i|i \in I\}$, denoted $\prod^w_{i\in I} G_i$, is the set of all $f \in \prod_{i\in I} G_i$ such that $f(i) = e_i$ for all but a finite number of $i \in I$. In other words $\{g_i\}(g_i \in G_i)$ is e_i for all but a finite number of $i \in I$. If all the groups G_i are (additive) abelian, $\prod^w_{i\in I} G_i$ is usually called the *(external) direct sum* and is denoted $\sum_{i\in I} G_i$.

Theorem 83
If $\{G_i|i \in I\}$ is a family of groups, then

1. $\prod^w_{i\in I} G_i$ is a normal subgroup of $\prod_{i\in I} G_i$;
2. for each $k \in I$, the map $\iota_k : G_k \to \prod^w_{i\in I} G_i$ given by $\iota_k(a) = \{a_i\}_{i\in I}$, where $a_i = e$ for $i \neq k$ and $a_k = a$, is a monomorphism of groups;
3. for each $i \in I$, $\iota_i(G_i)$ is a normal subgroup of $\prod_{i\in I} G_i$.

Definition 84

The map ι_k mentioned above are called the *canonical injections*.

Theorem 85

$\sum_{i\in I} A_i$ is a coproduct in the category of abelian groups.

The theorem is false if the word abelian is omitted.

Theorem 86

Let $\{N_i | i \in I\}$ be a family of normal subgroups of a group G such that

1. $G = \bigcup_{i\in I} N_i$;
2. for each $k \in I$, $N_k \cap \bigcup_{i\neq k} N_i = e$.

Then $G \cong \prod_{i\in I}^{w} N_i$.

Definition 87

Let $\{N_i | i \in I\}$ be a family of normal subgroups of a group G such that $G = \bigcup_{i\in I} N_i$ and for each $k \in I$, $N_k \cap \bigcup_{i\neq k} N_i = e$. Then G is said to be the *internal weak direct product* of the family $\{N_i | i \in I\}$ (or the *internal direct sum* if G is (additive) abelian). Notation-wise $G = \prod_{i\in I}^{w} N_i$ means that G is the internal weak direct product of the family of its subgroups $\{N_i | i \in I\}$.

Theorem 88

Let $\{N_i | i \in I\}$ be a family of normal subgroups of a group G. G is the internal weak direct product of the family $\{N_i | i \in I\}$ iff every nonidentity element of G is a unique product $a_{i_1} a_{i_2} \cdots a_{i_n}$ with $i_1, \cdots, i_n$ distinct elements of I and $e \neq a_{i_k} \in N_{i_k}$ for each $k = 1, 2, \cdots, n$.

Theorem 89

Let $\{f_i : G_i \to H_i | i \in I\}$ be a family of homomorphisms of groups and let $f = \prod f_i$ be the map $\prod_{i=1} G_i \to \prod_{i\in I} H_i$, given by $\{a_i\} \mapsto \{f_i(a_i)\}$. Then f is a homomorphism of groups such that $f(\prod_{i\in I}^{w} G_i) \subset \prod_{i\in I}^{w} H_i$, $\operatorname{Ker} f = \prod_{i\in I} \operatorname{Ker} f_i$ and $\operatorname{Im} f = \prod_{i\in I} \operatorname{Im} f_i$. Consequently f is a monomorphism (resp. epimorphism) iff each f_i is.

Let $\{G_i | i \in I\}$ and $\{N_i | i \in I\}$ be families of groups such that N_i is a normal subgroup of G_i for each $i \in I$.

1. $\prod_{i\in I} N_i$ is a normal subgroup of $\prod_{i\in I} G_i$ and $\prod_{i\in I} G_i / \prod_{i\in I} N_i \cong \prod_{i\in I} G_i/N_i$.
2. $\prod_{i\in I}^{w} N_i$ is a normal subgroup of $\prod_{i\in I}^{w} G_i$ and $\prod_{i\in I}^{w} G_i / \prod_{i\in I}^{w} N_i \cong \prod_{i\in I}^{w} G_i/N_i$.

Proof. Use the First Isomorphism theorem. □

Definition 90

A normal subgroup H of a group G is said to be a *direct factor*(*direct summand* if G is additive abelian) if there exists a (normal) subgroup K of G such that $G = H \times K$.

Theorem 91

If $GCD(m, n) = 1$, then $_{mn} \cong_m \times_n$

Theorem 92

If in a finite group G all elements(except the identity) are of order 2, $|G| = 2^n$ for some n and

$$G \cong_2 \times \cdots \times_2$$

1.9 Free Groups, Free Products, Generators and Relations

Definition 93

Given a set X and a group F that is free on X can be constructed in the following way: If $X = \varnothing$, F is the trivial group; otherwise let X^{-1} be a set disjoint from X such that $|X| = |X^{-1}|$. Choose a bijection $X \to X^{-1}$ and denote the image of $x \in X$ by x^{-1}; finally choose a set that is disjoint from $X \cup X^{-1}$ and has exactly one element, denote this element by 1. A *word* on X is a sequence $(a_1, a_2, \cdots)$ with $a_i \in X \cup X^{-1} \cup \{1\}$ such that for some $n \in$, $a_k = 1$ for all $k \geqslant n$. The constant sequence $(1, 1, \cdots)$ is called the *empty word* and is denoted 1. A word $(a_1, a_2, \cdots)$ on X is said to be *reduced* provided that

1. for all $x \in X$, x and x^{-1} are not adjacent;
2. $a_k = 1$ implies $a_i = 1$ for all $i \geqslant k$(that is, 1s only "appear at the end" of the word).

A nonempty reduced word is denoted $x_1^{\lambda_1} x_2^{\lambda_2} \cdots x_n^{\lambda_n}$, where $n \in$, $x_i \in X$ and $\lambda_i = \pm 1$. Two reduced words are equal iff both are the empty word or they have the same length and their individual components and exponents are the same. Consequently the map from X into the set $F(X)$ of all reduced words on X given by $x \mapsto x^1 = x$ is injective. Now we define a binary operation on the set $F = F(X)$. The empty word 1 act as the identity element. The product of nonempty reduced words is given by juxtaposition(If in the final product an entry x_i is adjacent to its image x_i^{-1}, they are "cancelled"). Thus the definition ensures that the product of reduced words is a reduced word.

Theorem 94

If X is a nonempty set and $F = F(X)$ is the set of all reduced words on X, then F is a group under the binary operation defined above and $F = X$.

The group $F = F(X)$ is called the *free group on the set X*.

Theorem 95

F is free on the set X in the category of groups.

Every group G is the homomorphic image of a free group.

Definition 96

If $G = X$ is a group, F is the free group on X and N is the kernel of the epimorphism $F \to G$ of previous Corollary, the equation $x_1^{\delta_1} \cdots x_n^{\delta_n} = e \in G$(where $x_1^{\delta_1} \cdots x_n^{\delta_n} \in F$ is a generator of N) is called a *relation* on the generators x_i.

A given group G can be completely described by specifying a set X of generators of G and a suitable set R of relations on these generators.

Definition 97

Let X be a set and Y a set of (reduced) words on X. A group G is said to be the *group defined by the generators $x \in X$ and relations $w = e_G(w \in Y)$* provided $G \cong F/N$, where F is the free group on X and N the normal subgroup of F generated by Y. One says that $(X|Y)$ is a *presentation* of G.

A finite cyclic group a has presentation $(a|a^n = e)$. The presentation of a free group on that set is $(F|\varnothing)$(that's why it's called "free": the terminology comes from free of relations). The dihedral group D_n has presentation $(\{a, b\}|a^n = e, b^2 = e, abab = e(\text{or } ba = a^{-1}b))$

Theorem 98 (Van Dyck)

Let X be a set, Y a set of (reduced) words on X and G the group defined by the generators $x \in X$ and relations $w = e(w \in Y)$. If H is any group such that $H = X$ and H satisfies all the relations $w = e(w \in Y)$(that is, these two groups G and H has the same presentation), then there is an epimorphism $G \to H$.

Definition 99

Given a family of groups $\{G_i|i \in I\}$ we may assume (by relabeling their elements if necessary) that the G_i are mutually disjoint sets. Let $X = \bigcup_{i\in I} G_i$ and let $\{1\}$ be a one-element set disjoint from X. A *word* on X is any sequence $(a_1, a_2, \cdots)$ such that $a_i \in X \cup \{1\}$ and for some $n \in$, $a_i = 1$ for all $i \geqslant n$. A word is *reduced* provided:

1. no $a_i \in X$ is the identity element in its group G_j;
2. for all $i, j \geqslant 1$, a_i and a_{i+1} are not in the same group G_j;
3. $a_k = 1$ implies $a_i = 1$ for all $i \geqslant k$.

Let $\prod_{i\in I}^{*} G_i$(or $G_1 * G_2 * \cdots * G_n$ if I is finite) be the set of all reduced words on X. $\prod_{i\in I}^{*} G_i$ forms a group, called the *free product* of the family $\{G_i|i \in I\}$, under the binary operation defined as follows. 1 is the identity element and the product of reduced words to be given by juxtaposition and necessary cancellation as well as contraction. Finally for each $k \in I$ the map $\iota_k : G_k \to \prod_{i\in I}^{*} G_i$ given by $e \mapsto 1$ and $a \mapsto a = (a, 1, 1, \cdots)$ is a monomorphism of groups.

Theorem 100

The free product $\prod_{i\in I}^{*} G_i$ with ι_i is a coproduct in the category of groups.

2

The Structure of Groups

2.1 Free Abelian Groups

2.2 Finitely Generated Abelian Groups

2.3 The Krull-Schmidt theorem

2.4 The Action of a Group on a Set

Definition 101

An *action* of a group G on a set S is a function $G \times S \to S$(usually denoted by $(g, x) \mapsto gx$) such that for all $x \in S$ and $g_1, g_2 \in G$:

1. $ex = x$;
2. $(g_1 g_2)x = g_1(g_2 x)$.

When such an action is given, G *acts on the set* S.

Definition 102

Let G be a group and H a subgroup. An action of the group H on the set G is given by $(h, x) \mapsto hx$, where hx is the product in G. The action of $h \in H$ on G is called a *(left) translation*.

Definition 103

Let G be a group and H a subgroup. An action of H on the set G, given by $(h, x) \mapsto hxh^{-1}$, is called *conjugation by* h and hxh^{-1} is said to be a *conjugate of* x. H can also act on the set S of all subgroups of G by conjugation $(h, K) \mapsto hKh^{-1}$. The group hKh^{-1} is said to be *conjugate to* K.

Theorem 104
Let G be a group that acts on a set S.

1. The relation on S defined by

$$x \sim x' \Leftrightarrow gx = x' \qquad \text{for some} \qquad g \in G$$

   is an equivalence relation.

2. For each $x \in S$, $G_x = \{g \in G | gx = x\}$ is a subgroup of G.

Definition 105
The equivalence classes of the equivalence relation previously mentioned are called the *orbits* of G on S; the orbit of $x \in S$ is denoted $\bar{x}$. The subgroup G_x is called the *subgroup fixing* x, the *isotropy group of* x, or the *stabilizer of* x.

Lemma 106
If G acts on S, then for any $x \in S$

$$|[G : x]| = |x|$$

Theorem 107
If G acts on S, then for any $x \in S$

$$|G| = |x||x|$$

2.5 The Sylow theorem

2.6 Classification of Finite Groups

2.7 Nilpotent and Solvable Groups

2.8 Normal and Subnormal Series

3

Rings

3.1 Rings and Homomorphisms

Definition 108

A *ring* is a nonempty set R together with two binary operations (usually denoted as addition $(+)$ and multiplication) such that:

1. $(R, +)$ is an abelian group;
2. the multiplication is associative;
3. $a(b+c) = ab+ac$ and $(a+b)c = ac+bc$ (left and right distributive laws).

If in addition the multiplication is commutative, R is said to be a *commutative ring*. If R contains an identity element for multiplication, R is said to be a *ring with identity*.

The additive identity of the ring is called the zero element and denoted 0.

Theorem 109

Let R be a ring. Then

1. $0a = a0 = 0$ for all $a \in R$;
2. $(-a)b = a(-b) = -(ab)$ for all $a, b \in R$;
3. $-(a)(-b) = ab$ for all $a, b \in R$;
4. $(na)b = a(nb) = n(ab)$ for all $n \in Z$ and all $a, b \in R$;
5. $$(\sum_{i=1}^{n} a_i)(\sum_{j=1}^{m} b_j) = \sum_{i=1}^{n}\sum_{j=i}^{m} a_i b_j \qquad \text{for all} \qquad a_i, b_j \in R$$

Definition 110

A nonzero element a in a ring R is said to be *left* (resp. *right*) *zero divisor* if there exists a nonzero $b \in R$ such that $ab = 0$ (resp. $ba = 0$). A *zero divisor* is an element of R which is both a left and a right zero divisor.

A ring has no zero divisors iff the right and left cancellation laws hold in this ring.

Definition 111

An element a in a ring R with identity is said to be *left* (resp. *right*) *invertible* if there exists $c \in R$ (resp. $b \in R$) such that $ca = 1_R$ (resp. $ab = 1_R$). The element c (resp. b) is called a *left* (resp. *right*) *inverse* of a. An element $a \in R$ that is both left and right invertible is said to be *invertible* or to be a *unit*.

A unit's left and right inverses necessarily coincide. The set of units in a ring R with identity forms a group under multiplication.

Definition 112

A commutative ring R with identity $1_R \neq 0$ and no zero divisors is called an *integral domain*. A ring D with identity $1_D \neq 0$ in which every nonzero element is a unit is called a *division ring*. A *field is a commutative division ring*.

Theorem 113 (Binomial theorem)

Let R be a ring with identity, n a positive integer, and $a, b, a_1, a_2, \cdots, a_s \in R$.

1. If $ab = ba$, then
$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$
2. If $a_i a_j = a_j a_i$ for all i and j, then
$$(a_1 + a_2 + \cdots + a_s)^n = \sum \frac{n!}{(i_1!)\cdots(i_s!)} a_1^{i_1} a_2^{i_2} \cdots a_s^{i_s}$$
where the sum is over all s-tuples $(i_1, i_2, \cdots, i_s)$ such that $i_1 + i_2 + \cdots + i_s = n$.

Definition 114

A *homomorphism of rings* $f : R \to S$ between two rings R and S is a mapping that preserves the ring structure, that is

$$f(r_1)f(r_2) = f(r_1 r_2) \qquad \text{and} \qquad f(r_1 + r_2) = f(r_1) + f(r_2)$$

for all $r_1, r_2 \in R$. Because of its similarity with respect to the homomorphisms of groups, the same terminology (like monomorphisms, epimorphisms and isomorphisms for injective, surjective and bijective homomorphisms respectively) will also apply. A monomorphism of rings $R \to S$ is sometimes called an *embedding of R in S*. The *kernel* and *image* of homomorphisms of rings are defined similar to those of group homomorphisms – the only difference is that the homomorphism maps the elements in its kernel to the identity element 0 of the additive abelian group. **In fact if R and S both have identities 1_R and 1_S it is not required that a homomorphism maps 1_R to 1_S.**

The canonical map $\to_m$ defined by $k \mapsto \bar{k}$ is an epimorphism of rings.

Definition 115

Let R be a ring. If there is a least positive integer n such that $na = 0$ for all $a \in R$, then R is said to *have characteristic* n. If no such n exists R is said to *have characteristic* 0.(Notation: $R = n$)

Theorem 116

Let R be a ring with identity 1_R and characteristic $n > 0$.

1. If $\varphi : Z \to R$ is the map given by $m \mapsto m1_R$, then φ is a homomorphism with kernel n.
2. n is the least positive integer such that $n1_r = 0$.
3. If R has no zero divisors(R is an integral domain), then n is prime.

Theorem 117

Every ring R may be embedded in a ring S with identity. The ring S (which is not unique) may be chosen to be either of characteristic zero or of the same characteristic as R.

Definition 118

A ring R such that $a^2 = a$ for all $a \in R$ is called a *Boolean Ring*. Every Boolean ring is commutative and $a + a = 0$ for all $a \in R$.

Theorem 119 (a.k.a The Freshman's Dream)

If R is a commutative ring with identity of prime characteristic p and $a, b \in R$, then $(a \pm b)^{p^n} = a^{p^n} \pm b^{p^n}$ for all $n \geqslant 0 \in$ (note that $b = -b$ if $p = 2$).

Definition 120

An element a of a ring is *nilpotent* if $a^n = 0$ for some integer n.

Theorem 121

In a commutative ring $a + b$ is nilpotent if a and b are.

However, the theorem is not necessarily true in a non-commutative ring. For example, in the ring over all 2×2 matrices over where addition and multiplication are defined respectively by matrix addition and multiplication the elements $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ are nilpotent(their square equals to the additive zero in this ring), but their sum is not.

Theorem 122

A finite ring with more than one element and no zero divisors is a division ring.

Proof. For each non-zero element $a \in R$ define the map $\varphi_a : R \to R$ given by $x \mapsto ax(x \in R)$. Show that the map is a bijection and thus an identity exists as well as a is invertible. $\square$

Definition 123

The homomorphism $R \to R$ defined on a commutative ring R with identity and prime characteristic p given by $r \mapsto r^p$ is called the *Frobenius homomorphism*.

Definition 124

If R is a ring, then so is R^{op}, where R^{op} is defined as follows: their underlying set is the same; their addition coincide; the multiplication in R^{op} is defined by $a \circ b = ba$, where ba is the product in R. The ring R^{op} is called the *opposite ring* of R.

Theorem 125

If R and S are rings and R^{op} and S^{op} are their respective opposite rings, then

1. R has an identity iff R^{op} does;
2. R is a division ring iff R^{op} is;
3. $(R^{op})^{op} = R$;
4. If S is a ring, then $R \cong S$ iff $R^{op} \cong S^{op}$.

3.2 Ideals

Definition 126

Let R be a ring and S a nonempty subset of R that is closed under addition and multiplication in R. If S is itself a ring under these operations then S is called a *subring* of R. A subring I of R is a *left ideal*(resp. *right ideal*) provided for $r \in R$ and $x \in I$ we have $rx \in I$(resp. $xr \in I$). I is an *ideal* if it is both a left and right ideal.

It can be seen that ideal is the analogous definition of a normal subgroup of a group. The *center* of a ring R is the set $C = \{c \in R | cr = rc \text{ for all } r \in R\}$. C is a subring of R but it may not be an ideal. The cyclic group generated by any integer n is an ideal in .

Definition 127

The ideal of a ring that only contains 0 is called the *trivial ideal*(denoted 0). An ideal I of R such that I is not trivial and $I \neq R$ is called a *proper ideal*.

If R has an identity 1_R and I is an ideal of R, then $I = R$ iff $1_R \in I$. Consequently a nonzero ideal I is proper iff I contains no units of R. In particular, a division ring has no proper ideals.

Theorem 128

A nonempty subset I of R is a left (resp. right) ideal iff for all $a, b \in I$ and $r \in R$:

1. $a, b \in I \Rightarrow a - b \in I$;
2. $a \in I, r \in R \Rightarrow ra \in I$(resp. $ar \in I$).

Let $\{A_i | i \in I\}$ be a family of [left] ideals in a ring R. Then $\bigcap_{i \in I} A_i$ is also a [left] ideal.

Definition 129

Let X be a subset of a ring R. Let $\{A_i | i \in I\}$ be the family of all [left] ideals in R which contain X. Then $\bigcap_{i \in I} A_i$ is called the [left] *ideal generated by* X. This ideal is denoted (X). The elements of X are called *generators* of (X). If X is finite, then (X) is said to be *finitely generated*. An ideal (x) generated by a single element is called a *principal ideal*. A *principle ideal ring* is a ring in which every ideal is principal. A principal ideal ring which is an integral domain is called a *principal ideal domain*.

Theorem 130

Let R be a ring, $a \in R$ and $X \subset R$.

1. The principal ideal a consists of all elements of the form $ra + as + na + \sum_{i=1}^{m} r_i a s_i (r, s, r_i, s_i \in R;$ $m \in;$ and $n \in)$.
2. If R has an identity, then $(a) = \{\sum_{i=1}^{n} r_i a s_i | r_i, s_i \in R; n \in\}$.
3. If a is in the center of R, then $(a) = \{ra + na | r \in R, n \in Z\}$.
4. $Ra = \{ra | r \in R\}$(resp. $aR = \{ar | r \in R\}$) is a left(resp. right) ideal in R(which may not contain a). If R has an identity, then $a \in Ra$ and $a \in aR$.
5. If R has an identity and a is in the center of R, then $Ra = (a) = aR$.
6. If R has an identity and X is in the center of R, then the ideal (X) consists of all finite sums $r_1 a_1 + \cdots + r_n a_n (n \in; r_i \in R; a_i \in X)$.

Definition 131

Let $A_1, A_2, \cdots, A_n$ be nonempty subsets of a ring R. Denote by $A_1 + A_2 + \cdots + A_n$ the set $\{a_1 + a_2 + \cdots + a_n | a_i \in A_i$ for all $i\}$. If A and B are nonempty subsets of R let AB denote the set of all finite sums $\{a_1 b_1 + \cdots + a_n b_n | n \in, a_i \in A, b_i \in B\}$. The definition of AB can be extended to an arbitrary number of factors. If all factors are the same set A it is denoted by A^n.

Theorem 132

Let $A, A_1, A_2, \cdots, A_n$, B and C be [left] ideals in a ring R.

1. $A_1 + A_2 + \cdots + A_n$ and $A_1 A_2 \cdots A_n$ are [left] ideals;
2. $(A + B) + C = A + (B + C)$;
3. $(AB)C = A(BC) = ABC$;
4. $B(A_1 + A_2 + \cdots + A_n) = BA_1 + BA_2 + \cdots + BA_n$ and $(A_1 + A_2 + \cdots + A_n)C = A_1 C + A_2 C + \cdots + A_n C$(distributivity).

Since R is additively abelian, any ideal of it is also a normal subgroup. Thus the quotient R/I group can be defined in which addition is given by $(a + I) + (b + I) = (a + b) + I$. Moreover, R/I can be made into a ring.

Theorem 133
Let R be a ring and I an ideal of R. Then the additive quotient group R/I is a ring with multiplication given by
$$(a+I)(b+I) = (ab+I)$$
If R is commutative or has an identity, then the same is true of R/I.

Theorem 134
If $f : R \to S$ is a homomorphism of rings, then the kernel of f is an ideal in R. Conversely if I is an ideal in R, then the map $\pi : R \to R/I$ given by $r \mapsto r + I$ is an epimorphism of rings with kernel I.

The map π is called the *canonical epimorphism*(or *projection*).

Theorem 135
If $f : R \to S$ is a homomorphism of rings and I is an ideal of R which is contained in the kernel of f, then there is a unique homomorphism of rings $\bar{f} : R/I \to S$ such that $\bar{f}(a+I) = f(a)$ for all $a \in R$. $\operatorname{Im} \bar{f} = \operatorname{Im} f$ and $\operatorname{Ker} \bar{f} = (\operatorname{Ker} f)/I$. $\bar{f}$ is an isomorphism iff f is an epimorphism and $I = \operatorname{Ker} f$.

[First Isomorphism theorem] If $f : R \to S$ is a homomorphism of rings, then f induces an isomorphism of rings $R/\operatorname{Ker} f \cong \operatorname{Im} f$. If $f : R \to S$ is a homomorphism of rings, I is an ideal in R and J is an ideal in S such that $f(I) \subset J$, then f induces a homomorphism of rings $\bar{f} : R/I \to S/J$, given by $a + I \mapsto f(a) + J$. $\bar{f}$ is an isomorphism iff $\operatorname{Im} f + J = S$ and $f^{-1}(J) \subset I$. In particular, if f is an epimorphism such that $f(I) = J$ and $\operatorname{Ker} f \subset I$, then $\bar{f}$ is an isomorphism.

Theorem 136
Let I and J be ideals in a ring R.

1. (Second Isomorphism theorem) There is an isomorphisms of rings $I/(I \cap J) \cong (I+J)/J$;
2. (Third Isomorphism theorem) if $I \subset J$, then J/I is an ideal in R/I and there is an isomorphism of rings $(R/I)/(J/I) \cong R/J$.

Theorem 137
If I is an ideal in a ring R, then there is a bijection between the set of all ideals of R which contain I and the set of all ideas of R/I, given by $J \mapsto J/I$. Hence every ideal in R/I is of the form J/I, where J is an ideal of R which contains I.

Definition 138
An ideal P in a ring R is said to be *prime* if $P \neq R$ and for any ideals A, B in R
$$AB \subset P \quad \Rightarrow \quad A \subset P \quad \text{or} \quad B \subset P$$

Theorem 139

If P is an ideal in a ring R such that $P \neq R$ and for all $a, b \in R$

$$ab \in P \quad \Rightarrow \quad a \in P \quad \text{or} \quad b \in P$$

then P is prime. Conversely if P is prime and R is commutative, then P satisfies the condition above.

The zero ideal in any integral domain is prime. If p is a prime integer, then the principal ideal (p) in is prime.

Theorem 140

In a commutative ring R with identity $1_R \neq 0$ and ideal P is prime iff the quotient ring R/P is an integral domain.

Definition 141

An ideal [resp. left ideal] M in a ring R is said to be *maximal* if $M \neq R$ and for every ideal [resp. left ideal] N such that $M \subset N \subset R$, either $N = M$ or $N = R$.

If R is a ring and S is the set of all ideals I of R such that $I \neq R$, then S is partially ordered by set-theoretic inclusion. Consequently the following theorem can be proved using Zorn's lemma.

Theorem 142

In a nonzero ring R with identity maximal [left] ideals always exist. In fact every [left] ideal in R except R itself is contained in a maximal [left] ideal.

Theorem 143

If R is a commutative ring such that $R^2 = R$(in particularly if R has an identity), then every maximal ideal M in R is prime.

Theorem 144

Let M be an ideal in a ring R with identity $1_R \neq 0$.

1. If M is maximal and R is commutative, then the quotient ring R/M is a field.

2. If the quotient ring R/M is a division ring, then M is maximal.

The following conditions on a commutative ring R with identity $1_R \neq 0$ are equivalent.

1. R is a field;

2. R has no proper ideals;

3. 0 is a maximal ideal in R;

4. every nonzero homomorphism of rings $R \to S$ is a monomorphism.

Theorem 145
Let $\{R_i | i \in I\}$ be a nonempty family of rings and $\prod_{i\in I} R_i$ the direct product of the additive abelian group R_i;

1. $\prod_{i\in I} R_i$ is a ring with multiplication defined by $\{a_i\}_{i\in I}\{a_i\}_{i\in I} = \{a_i b_i\}_{i\in I}$;
2. if R_i has an identity[resp. is commutative] for every $i \in I$, then $\prod_{i\in I} R_i$ has an identity [resp. is commutative];
3. for each $k \in I$ the canonical projection $\pi_k : \prod_{i\in I} R_i \to R_k$ given by $\{a_i\} \mapsto a_k$ is an epimorphism of rings;
4. for each $k \in I$ the canonical injection $\iota_k : R_k \to \prod_{i\in I} R_i$ given by $a_k \mapsto \{a_i\}$(where $a_i = 0$ for $i \neq k$) is a monomorphism of rings.

Definition 146
$\prod_{i\in I} R_i$ is called the *(external) direct product* of the family of rings. Its notation is analogous with it of the direct product of groups.

Theorem 147
$\prod_{i\in I} R_i$ is a product in the category of rings.

Theorem 148
Let $A_1, A_2, \cdots, A_n$ be ideals in a ring R such that

1. $A_1 + A_2 + \cdots + A_n = R$;
2. for each $k(1 \leqslant k \leqslant n)$, $A_k \cap (A_1 + \cdots + A_{k-1} + A_{k+1} + \cdots + A_n) = 0$.

Then there is a ring isomorphism $R \cong A_1 \times A_2 \times \cdots \times A_n$.

If a ring and a family of its ideals satisfies the conditions in the theorem above, the ring is said to be the *(internal) direct product* of this family of ideals. The notation of (internal) direct product for a ring is analogous to it of (internal) direct product for a group.

Definition 149
Let A be an ideal in a ring R and $a, b \in R$. The element a is said to be *congruent to b modulo A*(denoted $a \equiv b \pmod{A}$) if $a - b \in A$. Thus

$$a \equiv b \pmod{A} \Leftrightarrow a - b \in A \Leftrightarrow a + A = b + A$$

Theorem 150 (Chinese Remainder theorem)
Let $A_1, \cdots, A_n$ be ideals in a ring R such that $R^2 + A_i = R$ for all i and $A_i + A_j = R$ for all $i \neq j$. If $b_1, \cdots, b_n \in R$, then there exists $b \in R$ such that

$$b \equiv b_i \pmod{A_i} \qquad (i = 1, 2, \cdots, n)$$

Furthermore b is uniquely determined up to congruence modulo the ideal

$$A_1 \cap A_2 \cap \cdots \cap A_n$$

Let $m_1, \cdots, m_n$ be positive integers such that $(m_i, m_j) = 1$ for $i \neq j$. If $b_1, b_2, \cdots, b_n$ are any integers, then the system of congruences

$$x \equiv b_1 \pmod{m_1}; x \equiv b_2 \pmod{m_2}; \cdots; x \equiv b_n \pmod{m_n}$$

has an integral solution that is uniquely determined up to modulo $m = m_1 m_2 \cdots m_n$. If $A_1, A_2, \cdots, A_n$ are ideals in a ring R, then there is a monomorphism of rings

$$\theta : R/(A_1 \cap \cdots \cap A_n) \to R/A_1 \times R/A_2 \times \cdots \times R/A_n$$

If $R^2 + A_i = R$ for all i and $A_i + A_j = R$ for all $i \neq j$, then θ is an isomorphism of rings.

Theorem 151
The equation $ax + ny = b$ has solutions for $x, y \in$ iff $GCD(a, n)|b$.

Theorem 152
The congruence $ax \equiv b \bmod n$ has a solution iff $GCD(a, n)|b$. Moreover, if this congruence does have at least one solution, the number of noncongruent solutions modulo n is $GCD(a, n)$; that is, if $[a][x] = [b]$ has a solution in ${}_n$, then it has $GCD(a, n)$ different solutions in ${}_n$.

Definition 153
Let $m = m_1 m_2 \cdots m_r$, where the integers m_i are coprime in pairs. The *residue representation* or *modular representation* of any number x in ${}_m$ is the r-tuple $(a_1, a_2, \cdots, a_r)$ where $x \equiv a_i \bmod m_i$.

3.3 Factorization in Commutative Rings

Definition 154
A nonzero element a of a commutative ring R is said to *divide* an element b in R(written $a|b$) if there exists $x \in R$ such that $ax = b$. Elements a, b of R are said to be *associates* if $a|b$ and $b|a$.

Theorem 155

Let a, b and u be elements of a commutative ring R with identity.

1. $a|b$ iff $(b) \subset (a)$.
2. a and b are associates iff $(a) = (b)$.
3. u is a unit iff $u|r$ for all $r \in R$.
4. u is a unit iff $(u) = R$.
5. The relation "a is an associate of b" is an equivalence relation on R.
6. If $a = br$ with $r \in R$ a unit, then a and b are associates. If R is an integral domain, the converse is true.

Definition 156

Let R be a commutative ring with identity. An element c of R is *irreducible* provided that

1. c is a nonzero element;
2. $c = ab$ implies that a or b is a unit.

An element p of R is *prime* provided that

1. p is a nonzero nonunit;
2. $p|ab$ implies $p|a$ or $p|b$.

[Incomplete]

Definition 157

An integral domain R is a *unique factorization domain* provided that every nonzero nonunit element can be written as a unique finite product of irreducibles up to re arrangements and up to multiplication by units.

Definition 158

Let be the set of natural numbers and R a commutative ring. R is a *Euclidean ring* if there is a function $\varphi : R - 0 \to$ such that:

1. If $a, b \in R$ and $ab \neq 0$, then $\varphi(a) \leqslant \varphi(ab)$;
2. If $a, b \in R$ and $b \neq 0$, then there exist $q, r \in R$ such that $a = qb + r$ with $r = 0$ or $r \neq 0$ and $\varphi(r) < \varphi(b)$.

A Euclidean ring which is an integral domain is called a *Euclidean domain*.

Theorem 159

Every Euclidean ring R is a principal ideal ring with identity. Consequently every Euclidean domain is a unique factorization domain.

Let $[i]$ be $\{a+bi|a,b\in\}$. $[i]$ is an integral domain called the domain of Gaussian integers. Clearly $[i]$ is an Euclidean domain provided $\varphi(a+bi)=a^2+b^2$.

Definition 160

Let X be a nonempty subset of a commutative ring R. An element $d\in R$ is a *greatest common divisor* of X provided:

1. $d|a$ for all $a\in X$;
2. $c|a$ for all $a\in X$ implies that $c|d$.

If R has an identity and 1_R is the greatest common divisor of X, then elements of X are said to be *relatively prime*.

Definition 161

Let X be a nonempty subset of a commutative ring R. An element $l\in R$ is a *least common multiple* of X provided:

1. $a|l$ for all $a\in X$;
2. $a|f$ for all $a\in X$ implies that $l|f$.

Theorem 162

Let R be a Euclidean domain. Any two elements a and b in R have a greatest common divisor g. Moreover, there exist $s,t\in R$ such that

$$g=sa+tb$$

Lemma 163

If $r_{i-1}=r_iq_{i+1}+r_{i+1}$, then $GCD(r_{i-1},r_i)=GCD(r_i,r_{i+1})$.

Theorem 164

$_n$ is a field iff n is prime.

Theorem 165

Let a be an element of the Euclidean ring R. The quotient ring $R/(a)$ is a field iff a is irreducible over R.

3.4 Rings of Quotients and Localization

Definition 166

A nonempty subset S of a ring R is *multiplicative* if $a,b\in S\Rightarrow ab\in S$.

Theorem 167

Let S be a multiplicative subset of a commutative ring R. The relation defined on the set $R \times S$ by

$$(r, s) \sim (r', s') \Leftrightarrow s_1(rs' - r's) = 0 \quad \text{for some} \quad s_1 \in S$$

is an equivalence relation. Furthermore if R has no zero divisors and $0 \notin S$, then

$$(r, s) \sim (r', s') \Leftrightarrow rs' - r's = 0$$

(r, s) will be denoted as r/s from now on.

Theorem 168

Let S be a multiplicative subset of a commutative ring R and let $S^{-1}R$ be the set of equivalence classes of $R \times S$ under the equivalence relation defined previously.

1. $S^{-1}R$ is a commutative ring with identity, where addition and multiplication are defined similarly to the addition and multiplication of rationals.
2. If R is a nonzero ring with no zero divisors and $0 \notin S$, then $S^{-1}R$ is an integral domain.
3. If R is a nonzero ring with no zero divisors and S is the set of all nonzero elements in R, then $S^{-1}R$ is a field.

Definition 169

$S^{-1}R$ is called the *ring of quotients* or *ring of fractions* or *quotient ring* of R by S. If S is the nonzero elements of R, $S^{-1}R$ is called the *quotient field of the integral domain* R(as in the third statement of the previous theorem). More generally if R is any non-zero commutative ring and S is the non-empty set of all nonzero elements of R that are not zero divisors, $S^{-1}R$ is called the *complete*(or *full*) *ring of quotients*(or *fractions*) of the ring R.

Theorem 170

Let S be a multiplicative subset of a commutative ring R.

1. The map $\varphi_S : R \mapsto S^{-1}R$ given by $r \mapsto rs/s$(for any $s \in S$) is a well-defined homomorphism of rings such that $\varphi_S(s)$ is a unit in $S^{-1}R$ for every $s \in S$.
2. If $0 \notin S$ and S contains no zero divisors, then φ_S is a monomorphism. In particular, any integral domain may be embedded in its quotient field.
3. If R has an identity and S consists of units, then φ_S is an isomorphism. In particular, the complete ring of quotient, or the quotient field, of a field F is isomorphic to F.

Theorem 171

Let S be a multiplicative subset of a commutative ring R and let T be any commutative ring with identity. If $f : R \to T$ is a homomorphism of rings such that $f(s)$ is a unit in T for all $s \in S$, then there exists a unique homomorphism of rings $\bar{f} : S^{-1}R \to T$ such that $\bar{f}\varphi_S = f$. The ring $S^{-1}R$ is completely determined(up to isomorphism) by this property.

Let R be an integral domain considered as a subring of its quotient field F. If E is a field and $f : R \to E$ a monomorphism of rings, then there is a unique monomorphism of fields $\bar{f} : F \to E$ such that $\bar{f}|R = f$. In particular any field E_1 containing R contains an isomorphic copy F_1 of F with $R \subset F_1 \subset E_1$.

Theorem 172
Let S be a multiplicative subset of a commutative ring R.

1. If I is an ideal in R, then $S^{-1}I = \{a/s | a \in I; s \in S\}$ is an ideal is $S^{-1}R$.
2. If J is another ideal in R, then

$$S^{-1}(I+J) = S^{-1}I + S^{-1}J$$
$$S^{-1}(IJ) = (S^{-1}I)(S^{-1}J)$$
$$S^{-1}(I \cap J) = S^{-1}I \cap S^{-1}J$$

Definition 173
$S^{-1}I$ is called the *extension* of I in $S^{-1}R$.

Theorem 174
Let S be a multiplicative subset of a commutative ring R with identity and let I be an ideal of R. Then $S^{-1}I = S^{-1}R$ iff $S \cap I \neq \varnothing$.

Definition 175
If J is an ideal in a ring of quotients $S^{-1}R$, then $\varphi_S^{-1}(J)$ is an ideal in R and is sometimes called the *contraction* of J in R.

Incomplete

3.5 Rings of Polynomials and Formal Power Series

Theorem 176
Let R be a ring and let $R[x]$ denote the set of all sequences of elements of R $(a_0, a_1, \cdots)$ such that $a_i = 0$ for all but a finite number of indices i.

1. $R[x]$ is a ring with addition and multiplication defined similarly to the addition and multiplication of polynomials in .
2. If R is commutative(resp. a ring with identity or a ring without zero divisors or an integral domain), then so is $R[x]$.
3. The map $R \to R[x]$ given by $r \mapsto (r, 0, 0, \cdots)$ is a monomorphism of rings.

Definition 177
The ring $R[x]$ is called the *ring of polynomials* over R.

Theorem 178

Let R be a ring with identity and denote by x the element $(0, 1_R, 0, \cdots)$ of $R[x]$.

1. $x^n = (0, 0, \cdots, 0, 1^R, 0, \cdots)$, where 1_R is the $(n+1)$st coordinate.
2. If $r \in R$, then for each $n \geqslant 0$, $rx^n = x^n r = (0, \cdots, 0, r, 0, \cdots)$, where r is the $(n+1)$st coordinate.
3. For every nonzero polynomial $f \in R[x]$ there exists an integer n and elements $a_0, \cdots, a_n \in R$ such that $f = a_0x^0 + a_1x^1 + \cdots + a_nx^n$. The integer n and elements a_i are unique.

Definition 179

If $f = \sum_{i=0}^n a_i x^i \in R[x]$, then a_i are called the *coefficients* of f. a_0 is the constant term. Elements of $R[x]$ whose only nonzero coordinates is the first one are called *constant polynomials*. a_n is called the *leading coefficient* of f. If R has an identity and the leading coefficient of f is 1_R , f is said to be a *monic polynomial*. The element $x = (0, 1_R, \cdots)$ is called an *indeterminate*.

Theorem 180

Let R be a ring and denote by $R[x_1, x \cdots, x_n]$ the set of all functions $f :^n \to R$ such that $f(u) \neq 0$ for at most a finite number of elements u of ^{n}.

1. $R[x_1, \cdots, x_n]$ is a ring with addition and multiplication defined by

$$(f+g)(u) = f(u) + g(u) \quad \text{and} \quad (fg)(u) = \sum_{v+w=n; v,w\in^n} f(v)g(w)$$

   where $f, g \in R[x_1, x \cdots, x_n]$ and $u \in^n$.

2. If R is commutative(resp. a ring with identity or a ring without zero divisors or an integral domain), then so is $R[x_1, \cdots, x_n]$.
3. The map $R \to R[x_1, \cdots, x_n]$ given by $r \mapsto f_r$, where $f_r(0, 0, \cdots, 0) = r$ and $f(u) = 0$ for all other $u \in^n$, is a monomorphism of rings.

Definition 181

The ring $R[x_1, \cdots, x_n]$ is called the *ring of polynomials in n indeterminates over R*.

Incomplete Let R be a ring and denote by $R[[x]]$ the set of all sequences of elements of R $(a_0, a_1, \cdots)$.

1. $R[[x]]$ is a ring with component-wise addition and multiplication defined by

$$(a_0, a_1, \cdots)(b_0, b_1, \cdots) = (c_0, c_1, \cdots)$$

   where $c_n = \sum_{k+j=n} a_k b_j$.

2. $R[x]$ is a subring of $R[[x]]$.
3. If R is commutative(resp. a ring with identity or a ring without zero divisors or an integral domain), then so is $R[[x]]$.

Definition 182
$R[[x]]$ is called the *ring of formal power series* over the ring R.

Incomplete

3.6 Factorization in Polynomial Rings

Definition 183
Let R be a ring. The *degree of a nonzero monomial* $ax_1^{k_1}x_2^{k_2}\cdots x_n^{k_n} in R[x_1, \cdots, x_n]$ is the nonnegative integer $k_1 + k_2 + \cdots + k_n$. The *(total) degree of the polynomial* f, denoted $\deg f$, is the maximum of the degrees of the monomials $a_i x_1^{k_{i_1}} x_2^{k_{i_2}} \cdots x_n^{k_{i_n}}$ such that $a_i \neq 0$. A polynomial which is a sum of monomials, each of which has degree k, is said to be *homogeneous of degree* k. The *degree of* f *in* x_k is the degree of f considered as a polynomial in one indeterminate x_k over the ring $R[x_1, \cdots, x_{k-1}, x_{k+1}, \cdots, x_n]$.

Theorem 184
Let R be a ring and $f, g \in R[x_1, \cdots, x_n]$.

1. $\deg(f + g) \leqslant \max(\deg f, \deg g)$.
2. $\deg(fg) \leqslant \deg f + \deg g$.
3. If R has no zero divisors, $\deg(fg) = \deg f + \deg g$.
4. If $n = 1$ and the leading coefficient of f or g is not a zero divisor in $R($ in particular, if it is a unit), then $\deg(fg) = \deg f + \deg g$.

Theorem 185 (The Division Algorithm)
If R is a ring with identity and $f, g \in R[x]$ are nonzero polynomials such that the leading coefficient of g is a unit in R, there exist unique polynomials $q, r \in R[x]$ such that

$$f = qg + r \qquad \text{and} \qquad \deg r < \deg g$$

[Remainder theorem] Let R be a ring with identity and

$$f(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$$

For any $c \in R$ there exists a unique $q(x) \in R[x]$ such that $f(x) = q(x)(x - c) + f(c)$. If F is a field, then $F[x]$ is a Euclidean domain, whence $F[x]$ is a principal ideal domain and a unique factorization domain. The units in $F[x]$ are precisely the nonzero constant polynomials. $(x - \alpha)$ is a factor of $f(x)$ in $F[x]$ iff $f(\alpha) = 0$. A polynomial of degree n in $F[x]$ has at most n roots in F.

Theorem 186 (Fundamental theorem of Algebra)
If $f(x)$ is a polynomial in $[x]$ of positive degree, then $f(x)$ has a root in .

Theorem 187

1. If z is a complex root of the real polynomial $f(x) \in [x]$, then its conjugate $\overline{z}$ is also a root.
2. If $a, b, c \in$ and $a+b\sqrt{c}$ is an irrational root of the rational polynomial $f(x) \in [x]$, then $a-b\sqrt{c}$ is also a root.

Theorem 188

1. The irreducible polynomials in $[x]$ are the polynomials of degree one.
2. The irreducible polynomials in $[x]$ are the polynomials of degree 1 together with the polynomials of degree 2 of the form ax^2+bx+c, where $b^2 < 4ac$.

Theorem 189
Let $p(x) = a_0 + a_1 x + \cdots + a_n x^n \in [x]$. If r/s is a rational root of $p(x)$ and $GCD(r,s) = 1$, then $r|a_0$ and $s|a_n$.

Lemma 190 (Gauss's lemma)
Let $P(x) = a_0 + a_1 x + \cdots + a_n x^n \in [x]$. If $P(x)$ can be factored in $[x]$ as $P(x) = q(x)r(x)$, then $P(x)$ can also be factored in $[x]$.

Theorem 191 (Eisenstein's Criterion)
Let D be a unique factorization domain with quotient field F. If $f = \sum_{i=0}^{n} a_i x^i \in D[x]$, $\deg f \geqslant 1$ and p is an irreducible element of D such that

$$p \nmid a_n; \quad p|a_i \quad \text{for} \quad i = 0, 1, \cdots, n-1; \quad p^2 \nmid a_0$$

then f is irreducible in $F[x]$. If f is primitive, then f is irreducible in $D[x]$.

Let $f(x) = \sum_{i=0}^{n} a_i x^i \in [x]$. If, for some prime p,

1. $p|a_i, \quad i = 0, 1, \cdots, n-1;$
2. $p \nmid a_n;$
3. $p^2 \nmid a_0.$

then $f(x)$ is irreducible over . For any prime p the polynomial $\varphi(x) = x^{p-1} + x^{p-1} + \cdots + x + 1$ is irreducible over . This polynomial is called a *cyclotomic polynomial* and can be written $\varphi(x) = \frac{(x^p-1)}{x-1}$.

Theorem 192
Let P be the ideal $(p(x))$ in the polynomial ring of the field $F[x]$, in which $p(x)$ has a positive degree. The different elements of $F[x]/(p(x))$ are those of the form

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

where $a_i \in F$.

4

Modules

4.1 Modules, Homomorphisms and Exact Sequences

4.2 Free Modules and Vector Spaces

4.3 Projective and Injective Modules

4.4 Hom and Duality

4.5 Tensor Products

4.6 Modules over a Principal Ideal Domain

4.7 Algebras

5

Fields and Galois Theory

5.1 Field Extensions

Definition 193
A field F is said to be an *extension field* of K(or simply an *extension* of k) provided that K is a subfield of F.

If F is an extension field of K, F is a vector space over K. The *dimension* of the K-vector space F will be denoted by $[F : K]$. F is said to be a *finite dimensional extension* or *infinite dimensional extension* of K according as $[F : K]$ is finite or infinite.

Theorem 194
Let F be an extension field of E and E an extension field of K. Then $[F : K] = [F : E][E : K]$. $[F : K]$ is finite iff $[F : E]$ and $[E : K]$ are finite.

$[:] = 2$. If $p(x)$ is irreducible over the field F, then $K = F[x]/(p(x))$ is an extension field of F. Furthermore $[K : F] = \deg p(x)$. **[Incomplete]**

Definition 195
Let F be an extension of K. An element u of F is said to be *algebraic* over K if u is a root of some nonzero polynomial $f \in K[x]$. Otherwise u is *transcendental* over K. F is called an *algebraic extension* of K if every element of F is algebraic over K. F is called a *transcendental extension* if at least one element of F is transcendental over K.

If K is a field, then $K[x_1, \cdots, x_n]$ is an integral domain. The quotient field of $K[x_1, \cdots, x_n]$ is denoted $K(x_1, \cdots, x_n)$, which consists of all fractions of elements in $K[x_1, \cdots, x_n]$. $K(x_1, \cdots, x_n)$ is called the *field of rational fractions* in $x_1, \cdots, x_n$ over K. Every element of $K(x_1, \cdots, x_n)$ is transcendental over K.

Theorem 196
If F is an extension field of K and $u \in F$ is algebraic over K, then

1. $K(u) = K[u]$;
2. $K(u) \cong F[x]/(p(x))$, where $f \in K[x]$ is an irreducible monic polynomial of degree $n \geqslant 1$ uniquely determined by the conditions that $f(u) = 0$ and $g(u) = 0 (g \in K[x])$ iff f divides g;
3. $[K(u) : K] = n$;
4. $\{1_K, u, u^2, \cdots, u^{n-1}\}$ is a basis of the vector space $K(u)$ over K;

Lemma 197
Let $p(x)$ be an irreducible polynomial over the field F. Then F has a finite extension field K in which $p(x)$ has a root.

Theorem 198
If $f(x)$ is any polynomial over the field F, there is an extension field K of F over which $f(x)$ splits into linear factors.

If $[K : F] = 2$ where $F \subset$, then $K = F(\sqrt{\gamma})$ for some $\gamma \in F$. If F is an finite extension of , then F is isomorphic to or . $[R :]$ is infinite.

5.2 The Fundamental theorem

5.3 Splitting Fields, Algebraic Closure and Normality

5.4 The Galois Group of a Polynomial

5.5 Finite Fields

The characteristic of an integral domain is either zero or prime. If F is a finite field, then $F = p \neq 0$ for some prime p and $|F| = p^n$ for some integer $n \geqslant 1$.

Theorem 199
If F is a field and G is a finite subgroup of the multiplicative group of nonzero elements of F, then G is a cyclic group.

If the field F has prime characteristic p, then F contains a subfield isomorphic to $_p$. If the field F has zero characteristic, then F contains a subfield isomorphic to the rational numbers.

Definition 200

A finite field with p^m elements is called a *Galois field* of order p^m and is denoted by $GF(p^m)$. It can be shown that for a given prime p and positive integer m, a Galois field $GF(p^m)$ exists and that all fields of order p^m are isomorphic. Moreover

$$GF(p^m) =_p [x]/(q(x))$$

where $q(x)$ is a degree m polynomial irreducible in $_p[x]$.

Definition 201

Elements of a Galois field $GF(p^m)$ can be written as

$$\{a_0 + a_i\alpha + \cdots + a_{m-1}\alpha^{m-1} | a_i \in_p\}$$

where α is a root of a polynomial $q(x)$ of degree m irreducible over $_p$. With judicious choice of α the elements of $GF(p^m)$ can be written as

$$\{0, 1, \alpha, \alpha^2, \alpha^3, \cdots, \alpha^{p^m-2}\} \quad \text{where} \quad \alpha^{p^m-1} = 1$$

The element α is called a *primitive element* of $GF(p^m)$. Equivalently a generator of the cyclic group $(GF(q)^*, \cdot)$ is called a *primitive element of* $GF(q)$.

Definition 202

An irreducible polynomial $g(x)$ of degree m over $_p$ is called a *primitive polynomial* if $g(x)|x^k - 1$ for $k = p^m - 1$ and for no smaller k.

The irreducible polynomial $g(x) \in_p [x]$ is primitive iff x is a primitive element in $_p[x]/(g(x)) = GF(p^m)$.

5.6 Separability

5.7 Cyclic Extensions

5.8 Cyclotomic Extensions

5.9 Radical Extensions

6

The Structure of Fields

6.1 Transcendence Bases

6.2 Linear Disjointness and Separability

7

Commutative Rings and Modules

7.1 Chain Conditions

7.2 Prime and Primary Ideals

7.3 Primary Decomposition

7.4 Noetherian Rings and Modules

7.5 Ring Extensions

7.6 Dedekind Domains

7.7 The Hilbert Nullstellensatz

8

The Structure of Rings

8.1 Simple and Primitive Rings

8.2 The Jacobson Radical

8.3 Semisimple Rings

8.4 The Prime Radical; Prime and Semiprime Rings

8.5 Algebras

8.6 Division Algebras

9

Categories

9.1 Functors and Natural Transformations

9.2 Adjoint Functors

9.3 Morphisms

10

Applications

10.1 Euclidean Motions

Definition 203

An *isometry* of ^{n} is a transformation $f: ^n \to ^n$ which is continuous and a symmetry(bijection). An isometry preserves the inner product(dot product on ^{n}), thus preserves length and angle. Isometries are "Rigid Motions" os ^{n}. The group of all isometries of ^{n} is called the *Euclidean Group of* ^{n} and is denoted $E(n)$.

Definition 204

The *orthogonal group*, denoted $O(n)$, is a subgroup of $E(n)$ consisting of all linear transformations that preserves inner products, which says that it is a group of matrices. The fact that these matrices preserve length implies that they have orthonormal columns: each column has unit length and two different columns have their dot product equal to zero.

Lemma 205

If $A \in O(n)$, then $A \times A^T = I$.

$O(n) = \{A \in E(n), A(\vec{0}) = (\vec{0})\}$(If an isometry maps $\vec{0}$ to $\vec{0}$, then it is a linear transformation).

Definition 206

Let $T(n)$, the *group of translations*, be the subgroup of $E(n)$ such that if $\alpha(\vec{v}) = \vec{v} - \vec{v_0}$ for some fixed $\vec{v_0} \in ^n$.

There is a epimorphism from $E(n)$ to $O(n)$, defined by $\varphi : E(n) \to O(n)$ and $\varphi(\alpha)(\vec{v}) = \alpha(\vec{v}) - \alpha(\vec{0})$, whose kernel is $T(n)$. $T(n)$ is a normal subgroup of $E(n)$ and $E(n)/T(n) \cong O(n)$. Every finite subgroup G of $E(n)$ fixes at least one point, i.e. there exists a vector $\vec{v} \in ^n$ such that $g(\vec{v}) = \vec{v}$ for all $g \in G$.

10.2 Matrix Groups

Definition 207
Let $GL(n,)$ denote the set of all nonsingular matrices with real entries and $GL(n,)$ be the set of all nonsingular matrices with complex entries. These groups are called *General Linear Groups*(and hence the derivation of the abbreviations).

Let G be a finite subgroup of $GL(n,)$(or $GL(n,)$). Then $\det(g)$ is a root of unity for any $g \in G$. The function $\det : O(n) \to \{1, -1\} \cong_2$, mapping a matrix to its determinant, is an epimorphism between groups.

Definition 208
$SO(n)$, or the *Special Orthogonal Group*, is the subgroup of $O(n)$ such that $\det(a) = 1$ for $a \in SO(n)$(an equivalent way is that $SO(n)$ is the kernel of $\det : O(n) \to \{1, -1\} \cong_2$ defined above). It is the group of proper rotations in ^{n}.

Definition 209
Let $U(n)$ be the subgroup of $GL(n,)$ of complex unitary transformations

$$U(n) = \{A \in GL(n,) | A(\vec{u}), A(\vec{v}) = \vec{u}, \vec{v}\}$$

where $(x_1, \cdots, x_n), (y_1, \cdots, y_n) = x_1\bar{y}_1 + \cdots + x_n\bar{y}_n$, $\bar{y}$ denotes the complex conjugate of y. $A \in U(n)$ iff $A\overline{A^T} = I$. The length of $\det(A)$ is an element of the circle group $S^1 \subset$. The function $\det : U(n) \to S^1$ is in fact an epimorphism. The kernel of this epimorphism is those matrices having determinant 1, which composed of the set of *Special Unitary Matrices* $SU(n)$, a subgroup of $U(n)$.

Definition 210
The *representation* of a group G is a homomorphism from G to $GL(n, K)$, where $K =$ or . Every $g \in G$ is represented as a matrix acting on ^{n} or ^{n}. The homomorphism is called *faithful* if it is injective.

10.3 The 2×2 Matrix Group

Theorem 211
$O(2)$ consists of matrices of the form

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}$$

where $0 \leqslant \theta \leqslant 2\pi$. Moreover $SO(2) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}, 0 \leqslant \theta \leqslant 2\pi$, and $SO(2) \cong S^1$.

Theorem 212
If G is a finite subgroup of $SO(2)$, then $G \cong_n$ for some n.

Theorem 213
If G is a finite subgroup of $O(2)$, then $G \cong_n$ or $G \cong D_n$ for some n.

10.4 Rotation of Regular Solids

Theorem 214
If $A \in SO(3)$, then A has a fixed axis(a line through the origin) and A is just rotation about the axis.

Theorem 215
The group G of proper rotations of the tetrahedron is isomorphic to A_4.

Theorem 216
The group of proper rotations of a cube is isomorphic to S_4.

The group of proper rotations of a regular dodecahedron and the group of proper rotations of a regular icosahedron are both isomorphic to A_5. The group of proper rotations of a octahedron is isomorphic to S_4.

10.5 Finite Rotation Groups and Crystallographic Groups

Theorem 217
Any finite subgroup of $SO(3)$ is isomorphic to one of the following: ${}_n(n \geqslant 1)$, $D_n(n \geqslant 2)$, A_4, S_4, A_5.

Definition 218
An *ideal crystallite lattice* L is a subset of ^{3} of the form

$$L = \{n_1\vec{v}_1 + n_2\vec{v}_2 + n_3\vec{v}_3 | n_i \in\}$$

where $\vec{v}_i$ is a fixed basis of ^{3}.

Definition 219
A subgroup of $SO(3)$ or $O(3)$ that leaves a crystallite lattice invariant is called a *crystallographic point group*.

10.6 Polya-Burnside Method

Theorem 220 (Burnside)

Let G be a finite group acting on a finite set X. For $g \in G$ let g be the set $\{x \in X | g(x) = x\}$. If N is the number of orbits of X under G, then

$$N = \frac{1}{|G|} \sum_{g \in G} |g|$$