Abstract Algebra

Hechen Hu

June 1, 2018

Contents

1

Groups

1.1 Semigroups, Monoids and Groups

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

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

Definition. 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 1.1.1. *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 $y = ba^{-1}$.*

Proposition. 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".

Proposition. 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. Left for Exercise □

***Example* 1.1.** *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. 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 1.1.2. *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.*

***Example* 1.2.** *The following relation on the additive froup $\mathbb{Q}$ is a congruence relation:*

$$a \sim b \Leftrightarrow a - b \in \mathbb{Z}$$

The set of equivalence classes (denoted $\mathbb{Q}/\mathbb{Z}$) 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. 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. 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 1.1.3 (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 1.1.4 (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. Let G be a semigroup, $a \in G$ and $n \in \mathbb{N}$. 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 $n \in \mathbb{N}$, a^{-n} is defined to be $(a^{-1})^n \in G$.

Theorem 1.1.5. *If G is a group(resp. semigroup, monoid) and $a \in G$, then for all $m, n \in \mathbb{Z}$ (resp. $\mathbb{N}$ and $\mathbb{N} \cup \{0\}$) :*

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

1.2 Homomorphisms and Subgroups

Definition. 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. 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 $f(A) = \{b \in H | b = f(a)$ 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 1.2.1. *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. 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. 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. 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 1.2.2. *Let H be a nonempty subset of a group G. Then H is a subgroup of G iff $ab^{-1} \in H$ for all $a, b \in H$.*

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

Definition. 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 $\bigcap\limits_{i \in I} H_i$ is called the *subgroup of G generated by the set X* and denoted $\langle X \rangle$. The elements of X are the *generators* of $\langle X \rangle$. If $G = \langle a_1, \cdots, a_n \rangle, (a_i \in G)$, G is said to be finitely generated. If $a \in G$, the subgroup $\langle a \rangle$ is called the *cyclic (sub)group* generated by a.

Theorem 1.2.3. *If G is a group and X a nonempty subset of G, then the subgroup $\langle X \rangle$ generated by X consists of all finite products $a_1^{n_1} a_2^{n_2} \cdots a_t^{n_t} (a_i \in X; n_i \in \mathbb{Z})$. In particular for every $a \in G$, $\langle a \rangle = \{a^n | n \in \mathbb{Z}\}$.*

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

1.3 Cyclic Groups

Definition. 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 1.3.1. *Every subgroup H of the additive group $\mathbb{Z}$ is cyclic. Either $H = \langle 0 \rangle$ or $H = \langle m \rangle$, where m is the least positive interger in H. If $H \neq \langle 0 \rangle$, then H is infinite.*

Theorem 1.3.2. *Every infinite cyclic group is isomorphic to the additive group $\mathbb{Z}$ and every finite group of order m is isomorphic to the additive group $\mathbb{Z}_m$.*

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

Theorem 1.3.3. *Let G be a group and $a \in G$. If a has infinite order, then*

- *$a^k = e$ iff $k = 0$;*
- *the elements $a^k (k \in \mathbb{Z})$ 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 $r \equiv s (mod m)$;*
- *$\langle a \rangle$ 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 1.3.4. *Every homomorphic image and every subgroup of a cyclic group G is cyclic. In particular, if H is a nontrivial subgroup of $G = \langle a \rangle$ and m is the least positive integer such that $a^m \in H$, then $H = \langle a^m \rangle$.*

Theorem 1.3.5. *Let $G = \langle a \rangle$ 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. 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.

1.4 Cosets and Counting

Definition. 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 1.4.1. *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. The set Ha above is called a *right coset* of H in G and aH is called an *left coset* of H in G.

Corollary. *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. 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. 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 1.4.2. *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. □

Corollary (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 $H = \langle a\rangle$. □

Theorem 1.4.3. *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, $|HK| = |H| \cdot n = |H||K|/|H \cap K|$. □

Proposition. 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. □

Proposition. 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. □

1.5 Normality, Quotient Groups, and Homomorphisms

Theorem 1.5.1. *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. 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 1.5.2. *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 1.5.3. *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. 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 $(a + N) + (b + N) = (a + b) + N$.

***Example* 1.3.** $\mathbb{Z}_m = \mathbb{Z}/\langle m \rangle$.

Theorem 1.5.4. *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. 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 1.5.5. *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. 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.

Corollary. *(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. □

Corollary. *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 $H = \operatorname{Im} fM = \operatorname{Im} f \vee M$; conversely, if $\operatorname{Im} f \vee M = H$, we have $\operatorname{Im} fM = H$, 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. □

Corollary. *(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 $\operatorname{Im} f = NK/N$. □

Corollary. *(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 $G/H = \operatorname{Im} I \cong (G/K)/\operatorname{Ker} I = (G/K)/(H/K)$. □

Theorem 1.5.6. *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. □

Corollary. *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 $\pi(K) = K/N$. □

1.6 Symmetric, Alternating, and Dihedral Groups

Definition. 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. 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 1.6.1. *Every nonidentity permutation in S_n is uniquely a product of disjoint cycles, each of which has length at least* 2.

Definition. Define an equivalence relation on I_n with a given permutation σ as follows: $x \sim y$ iff $y = \sigma^m(x)$ for some $m \in \mathbb{Z}$. 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 $d \in \mathbb{Z}$.

Corollary. *The order of a permutation $\sigma \in S_n$ is the least common multiplier of the order of its disjoint cycles.*

Corollary. *Every permutation in S_n can be written as a product of (not necessarily disjoint) transpositions.*

Definition. 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 $\operatorname{sgn} \tau$, is 1 or -1 according as τ is even or odd.

Theorem 1.6.2. *A permutation $\tau \in S_n (n \geqslant 2)$ cannot be both even and odd.*

Theorem 1.6.3. *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. *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. *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 $2k + 1 (k \in \mathbb{N})$. 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. A group is said to be *simple* if it has no proper normal subgroups.

Theorem 1.6.4. *The alternating group A_n is simple iff $n \neq 4$.*

The proof of the theorem proceeds from two lemmas below.

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

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

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

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 1.6.5. *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. A *category* is a class $\mathcal{C}$ of objects (denoted $\mathbf{A}, \mathbf{B}, \mathbf{C}, \ldots$) together with

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

2. for each triple $(\mathbf{A}, \mathbf{B}, \mathbf{C})$ of objects of $\mathcal{C}$ a function
$$\hom(\mathbf{B}, \mathbf{C}) \times \hom(\mathbf{A}, \mathbf{B}) \to \hom(\mathbf{A}, \mathbf{C})$$
which is the *composite* of morphisms. The composition must be associative. An identity morphism $1_{\mathbf{B}} : \mathbf{B} \to \mathbf{B}$ also exists and for any $f : \mathbf{A} \to \mathbf{B}$ and $g : \mathbf{B} \to \mathbf{C}$
$$1_{\mathbf{B}} \circ f = f \qquad \text{and} \qquad g \circ 1_{\mathbf{B}} = g$$

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

***Example* 1.4.** *For $\mathcal{S}$, the class of all sets, equipped with functions between these sets as morphisms, a morphism is an equivalence iff it is bijective.*

***Example* 1.5.** *For $\mathcal{G}$, the category of all groups, equipped with homomorphisms between these groups as morphisms, a morphism is an equivalence iff it is an isomorphism.*

Example* 1.6.** *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. Let $\mathcal{C}$ be a category and $\{\mathbf{A}_i | i \in I\}$ a family of objects of $\mathcal{C}$. A *product* for the family $\{\mathbf{A}_i | i \in I\}$ is an object $\mathbf{P}$ of $\mathcal{C}$ together with a family of morphisms $\{\pi_i : \mathbf{P} \to \mathbf{A_i} | i \in I\}$ such that for any object $\mathbf{B}$ and family of morphisms $\{\varphi_i : \mathbf{B} \to \mathbf{A_i} | i \in I\}$, there is a unique morphism $\varphi : \mathbf{B} \to \mathbf{P}$ such that $\pi_i \circ \varphi = \varphi_i$ for all $i \in I$. The product of $\{\mathbf{A}_i | i \in I\}$ is usually denoted $\prod_{i \in I} \mathbf{A_i}$.

When $I = \{1, 2\}$, the product $\mathbf{P}$ expressed using a commutative diagram:

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

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

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

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

Theorem 1.7.2. *If* $(\mathbf{S}, \{\iota_i\})$ *and* $(\mathbf{S}', \{\lambda_i\})$ *are both products of the family* $\{\mathbf{A_i} | i \in I\}$ *of objects of a category* $\mathcal{C}$*, then* $\mathbf{S}$ *and* $\mathbf{S}'$ *are equivalent.*

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

1. every morphism $\mathbf{A} \to \mathbf{B}$ of $\mathcal{C}$ is a function on the underlying sets $\sigma(\mathbf{A}) \to \sigma(\mathbf{B})$;

2. the identity morphism of each object $\mathbf{A}$ of $\mathcal{C}$ is the identity function on the underlying set $\sigma(\mathbf{A})$;

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

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

The essential fact about a free object $\mathbf{F}$ is that in order to define a morphism with domain $\mathbf{F}$, it suffices to specify the image of the subset $i(X)$.

***Example* 1.7.** *Let G be any group and $g \in G$. Then the map $\bar{f} : \mathbb{Z} \to G$ defined by $\bar{f}(n) = g^n$ is the unique homomorphism $\mathbb{Z} \to G$ such that $1 \mapsto g$. Consequently, if $X = \{1\}$ and $i : X \to \mathbb{Z}$ is the inclusion map, then $\mathbb{Z}$ is free on X in the category of groups. In other words, to determine a unique homomorphism from $\mathbb{Z}$ to G we need only specify the image of $1 \in \mathbb{Z}$ (that is, the image of $i(X)$).*

Theorem 1.7.3. *If $\mathcal{C}$ is a concrete category, $\mathbf{F}$ and $\mathbf{F}'$ are objects of $\mathcal{C}$ such that $\mathbf{F}$ is free on the set X and $\mathbf{F}'$ is free on the set X' and $|X| = |X'|$, then $\mathbf{F}$ is equivalent to $\mathbf{F}'$.*

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

Theorem 1.7.4. *Any two universal (resp. couniversal) objects in a category $\mathcal{C}$ are equivalent.*

***Example* 1.8.** *The trivial group is both universal and couniversal in the category of groups.*

Definition. 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. 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 1.8.1. *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. The mappings π_k previously mentioned are called the *canonical projections* of the direct product.

Theorem 1.8.2. $\prod_{i=1} G_i$ *is a product in the category of groups.*

Definition. The *(external) weak direct product* of a family of groups $\{G_i | i \in I\}$, denoted $\prod_{i\in I}^{w} G_i$, 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, $\prod_{i\in I}^{w} G_i$ is usually called the *(external) direct sum* and is denoted $\sum_{i\in I} G_i$.

Theorem 1.8.3. *If $\{G_i | i \in I\}$ is a family of groups, then*

1. *$\prod_{i\in I}^{w} G_i$ is a normal subgroup of $\prod_{i\in I} G_i$;*

2. *for each $k \in I$, the map $\iota_k : G_k \to \prod_{i\in I}^{w} G_i$ 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. The map ι_k mentioned above are called the *canonical injections.*

Theorem 1.8.4. $\sum_{i\in I} A_i$ *is a coproduct in the category of abelian groups.*

The theorem is false if the word abelian is omitted.

Theorem 1.8.5. *Let $\{N_i | i \in I\}$ be a family of normal subgroups of a group G such that*

1. *$G = \langle \bigcup_{i\in I} N_i \rangle$;*

2. *for each $k \in I$, $N_k \cap \langle \bigcup_{i\neq k} N_i \rangle = \langle e \rangle$.*

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

Definition. Let $\{N_i | i \in I\}$ be a family of normal subgroups of a group G such that $G = \langle \bigcup_{i\in I} N_i \rangle$ and for each $k \in I$, $N_k \cap \langle \bigcup_{i\neq k} N_i \rangle = \langle e \rangle$. 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 1.8.6. *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 1.8.7. *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.*

Corollary. *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. 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 $G = H \times K$.

1.9 Free Groups, Free Products, Generators and Relations

Definition. 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 $n \in \mathbb{N}$, $a_k = 1$ 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 $n \in \mathbb{N}$, $x_i \in X$ 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 1.9.1. *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 $F = \langle X \rangle$.*

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

Theorem 1.9.2. *F is free on the set X in the category of groups.*

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

Definition. If $G = \langle X \rangle$ 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. 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.

***Example* 1.9.** *A finite cyclic group $\langle a \rangle$ has presentation $(a|a^n = e)$.*

***Example* 1.10.** *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).*

***Example* 1.11.** *The dihedral group D_n has presentation $(\{a, b\}|a^n = e, b^2 = e, abab = e(or\ ba = a^{-1}b))$*

Theorem 1.9.3 (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 $H = \langle X \rangle$ 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. 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 $n \in \mathbb{N}$, $a_i = 1$ 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 1.9.4. *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

3

Rings

3.1 Rings and Homomorphisms

Definition. 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 3.1.1. *Let R be a ring. Then*

1. $0a = a0 = 0$ *for all* $a \in R$*;*
2. $(-a)b = a(-b) = -(ab)$ *for all* $a, b \in R$*;*
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. $$(\sum_{i=1}^{n} a_i)(\sum_{j=1}^{m} b_j) = \sum_{i=1}^{n}\sum_{j=i}^{m} a_i b_j \qquad \textit{for all} \qquad a_i, b_j \in R$$

Definition. 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. 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. 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 3.1.2 (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. 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.**

***Example* 3.1.** *The canonical map $\mathbb{Z} \to \mathbb{Z}_m$ defined by $k \mapsto \bar{k}$ is an epimorphism of rings.*

Definition. 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: $\operatorname{char} R = n$)

Theorem 3.1.3. *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 $\langle n \rangle$.*
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 3.1.4. *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.*

3.2 Ideals

3.3 Factorization in Commutative Rings

3.4 Rings of Quotients and Localization

3.5 Rings of Polynomials and Formal Power Series

3.6 Factorization in Polynomial Rings

4

Modules

5

Fields and Galois Theory

5.1 Field Extensions

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

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

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