1 Quotient Groups and Homomorphisms

1.1 Definitions and Examples

Definition. If ϕ is a homomorphism $\phi\colon G \to H$, the *kernel* of ϕ is the set

$$\{g \in G \mid \phi(g) = 1\}$$

and will be denoted by kerϕ (here 1 is the identity of H).

Proposition 1. Let G and H be groups and let $\phi\colon H \to H$ be a homomorphism.

1. $\phi(1_G) = 1_H$, where 1_G and 1_H are the identities of G and H, respectively.
2. $\phi(g^{-1}) = \phi(g)^{-1}$ for all $g \in G$.
3. $\phi(g^n) = \phi(g)^n$ for all $n \in \mathbb{Z}$.
4. kerϕ is a subgroup of G.
5. imϕ, the image of G uner ϕ, is a subgorup of H.

Definition. Let $\phi\colon G \to H$ be a homomorphism with kernel K. The *quotient group* or *factor group*, G/K (read G *modulo* K or simply G *mod* K), is the group whose elements are the fibers of ϕ with the following group operation: If X is the fiber above a and Y is the fiber above b then the product XY in G/K is defined to be the fiber above the product ab in G.

Proposition 2. Let $\phi\colon G \to H$ be a homomorphism with kernel K. Let $X \in G/K$ be the fiber above a, i.e., $X = \phi^{-1}(a)$. Then

1. For any $u \in X$, $X = \{uk \mid k \in K\}$
2. For any $u \in X$, $X = \{ku \mid k \in K\}$

Definition. For any $N \leq G$ and any $g \in G$ let

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

called respectively a *left coset* and a *right coset* of N in G. Any element of a coset is called a *representative* for the coset.

Theorem 3. Let G be a group and let K be the kernel of some homomorphism from G to another group. Then the set of whose elements are ;eft coeset of K in G with operation defined by

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

forms a group, G/K. This operation is well defined and does not depend on the choice of representatives.

Proposition 4. Let N be any subgroup of the group G. The set of left cosets of N in G form a partition of G. Furthermore, for all $u, v \in G, uN = vN$ if and only if $v^{-1}u \in N$ and in particular, $uN = vN$ if and only if u and v are representatives of the same coset.

Proposition 5. Let G be a group and let N be a subgroup of G.

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

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

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

Definition. The element gng^{-1} is called the *conjugate* of $n \in N$ by g. The set $gNg^{-1} = \{gng^{-1} \mid n \in N\}$ is called the *conjugate* of N by g. The element g is said to *normalize* N if $gNg^{-1} = N$. A subgroup N of a group G is called *normal* if every element of G normalizes N, i.e., if $gNg^{-1} = N$ for all $g \in G$. If N is a normal subgoup of G we shall write $N \trianglelefteq G$.

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

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

Proposition 7. A subgroup N of the group G is normal if and only if it is the kernel of some homomorphism.

Definition. Let $N \trianglelefteq G$. The homomorphism $\pi\colon G \to G/N$ defined by $\pi(g) = gN$ is called the *natural projection (homomorphism)* of G onto G/N. If $\overline{H} \leq G/N$, then *complete preimage* of $\overline{H}$ in G is the preimage of $\overline{H}$ under the natural projection homomorphism.

1.2 More on Cosets and Lagrange's Thoerem

Theorem 8. (*Lagrange's Theorem*) If G is a fintite group and H is a subgroup of G, then the order of H divides the order of G and the number of left cosets of H in G equals $\frac{|G|}{|H|}$.

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

Corollary 9. If G is a finite group and $x \in G$, then the order of x divides the order of G. In particular, $x^{|G|} = 1$ for all x in G.

Corollary 10. If G is a group of prime order p, then G is cyclic, hence $G \cong Z_p$ (note that this text uses Z_n to denote the cyclic group of order n written in multipicative notation and that given any $n \in \mathbb{Z}$, $Z_n \cong \mathbb{Z}/n\mathbb{Z}$).

Note. For finite abelian groups the full converse of Lagrange's theorem holds, that is the group has a subgroup of order n for each n that divides the order of the group.

Theorem 11. (Cauchy's Thoerem) If G is a fintite group and p is a prime dividing $|G|$, then G has an element of order p.

Theorem 12. (Sylow) If G is a finite group of order $p^\alpha m$, where p is a prime not dividing m, then G has a subgroup of order p^α.

Definition. Let H and K be subgroups of a group and define

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

Proposition 13. If H and K are finte subgroups of a group then

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

Proposition 14. If H and K are subgroups of a group, HK is a subgroup if and only if $HK = KH$.

Note. $HK = KH$ does not imply that the elements of H commute with the elements of K

Corollary 15. If H and K are subgroups of G and $H \leq N_G(K)$, then Hk is a subgroup of G. In particular, if $K \trianglelefteq G$, Then $HK \leq G$ for any $H \leq G$ (Since if $K \trianglelefteq G$, $N_G(k) = G$).

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

1.3 The Isomorphism Thoerems

Theorem 16. (The First Isomorphism Theorem) If $\phi\colon G \to H$ is a homomorphism, then $\ker\phi \trianglelefteq G$ and $G/\ker\phi \cong \phi(G)$.

Corollary 17. Let $\phi\colon G \to H$ be a homomorphism.

1. ϕ is injective if and only if $\ker\phi = 1$.
2. $|G : \ker\phi = |\phi(G)|$.

Theorem 18.