BASIC CONSEPTS OF GROUP THEORY

Recall that a **group** is a set G with a distinguished element e and a function $G \times G \longrightarrow G$, $(g, h) \mapsto gh$ such that

(1) $(ab)c = a(bc)$ for all $a, b, c \in G$;

(2) $ae = a = ea$ for all $a \in G$;

(3) for every $a \in G$ there is $b \in G$ such that $ab = e = ba$.

A group G is called **commutative** or **Abelian** if $ab = ba$ for all $a, b \in G$.

Remarks. 1. The element e is the unique element in G with the property $ae = a$ for some $a \in G$ (but one needs to know first that G is a group).
2. For given $a \in G$ the element b in 3) is unique. It is denoted by a^{-1} and called **the inverse of** a.

For $g \in G$ and a positive integer n define $g^n = gg...g$ ($n-$times). Furthemore, define $g^0 = e$ and $g^{-n} = (g^{-1})^n$. Then the usual rules $g^m g^n = g^{m+n}$ and $(g^m)^n = g^{mn}$ hold for any integers m, n and any $g \in G$.

An element $g \in G$ is called of **finite order** or **torsion** if there is $n \neq 0$ such that $g^n = e$; if no such n exists g is said to be of **infinite order**. If g is of finite order then the smallest positive n such that $g^n = e$ is called **the oreder of** g.

A **subgroup** of a group G is a nonempty subset $H \subseteq G$ such that for all $a, b \in H$ also ab and a^{-1} belong to H. These conditions imply that $e \in H$ and that H with mutiplication inherited from G is a group. If H is a subgroup of G we write $H < G$.

The intersection of any collection of subgroups of G is again a subgroup. In particular, if S is any subset of G then the intersection of all subgroups of G which contain S is the smallest subgroup of G which contains S. We deonote it by $< S >$ and call it the **subgroup generated** by S. It is not hard to see that $< S >$ conists exactly of those elements of G which can be written as $s_1^{u_1} s_2^{u_2} ... s_m^{u_m}$ for some $s_i \in S$ and $u_i = \pm 1$. In particular,if $S = \{g\}$ then $< S > = < g > = \{g^m : m \in \mathbb{Z}\}$ is the set of all powers of g.

Date: Aug 14.

We say that a subset S of G **generates** G if $< S >= G$. A group G is called **finitely generated** if there is a finite set $S \subseteq G$ which generates G. If $G =< g >$ for some $g \in G$ then G is called **cyclic**.

If A, B are subsets of a group G then $AB = \{ab : a \in A \text{ and } b \in B\}$.

Let $H < G$. A set of the form $gH = \{gh : h \in H\}$ for some $g \in G$ is called a **left coset** of H in G. A **right coset** of H in G is a set of the form $Hg = \{hg : h \in H\}$ for some $g \in G$. Two left (right) cosets of H in G are either disjoint or coincide. Thus the left (right) cosets of H partition the group G. If aH, bH are two left cosets then there is a bijection from aH to bH given by left multiplication by ba^{-1}. In particular, if H is finite then all left cosets have the same number of elements equal to $|H|$, and of course the same is true for right cosets. If moreover G is finite, then since the left (right) cosets partition G, we see that $|G| = |H|[G : H]$, where $[G : H]$ is the number of left (right) cosets of H. This result is usually referred to as **Lagranges Theorem**. In particular, if G is finite and $H < G$ then $|H|||G|$.

A subgroup H of G is called **normal** if $gH = Hg$ for every $g \in G$. We write $H \triangleleft G$ to indicate that H is normal in G. Here are some equivalent conditions for H to be normal:

- $gHg^{-1} = H$ for all $g \in G$;
- $gHg^{-1} \subseteq H$ for all $g \in G$;
- $ghg^{-1} \in H$ for every $g \in G$ and $h \in H$.

Exercise. Show that $H \triangleleft G$ iff the sets of right and left cosets of H coincide.

Examples of normal subgroups. In every group G, the trivial subgroup $\{e\}$ and the whole group G are normal subgroups of G. If a group does not have any other normal subgroups it is called a **simple** group.

There are many constructions of normal subgroups in a group G which often lead to a nontrivial subgroups. We will learn many of them later, but let us introduce two such constructions now, since they play a fundamental role in group theory.

If G is a group then the subset $Z(G)$ which consists of all elements which commute with every element in G is called the **center** of G. Thus $Z(G) = \{g \in G : gh = hg \text{ for all } h \in H\}$. It is an easy exercise to show that the center is a normal subgroup of G. Note that $Z(G) = G$ iff G is abelian.

For any two elements g, h in a group G we define the **commutator** $[g, h]$ by the formula $[g, h] = g^{-1}h^{-1}gh$. Thus $[g, h] = e$ iff the elements g, h commute. The **derived group** or **commutator group** of G is the group $[G, G]$ generated by the set of all commutators in G. This group is often denoted by G'. More generally, if X, Y are nonempty subsets of G, one writes $[X, Y]$ for the subgroup of G generated by all commutators of the form $[x, y]$ with $x \in X$ and $Y \in Y$.

From the identity $a[g, h]a^{-1} = [aga^{-1}, aha^{-1}]$ one deduces easily that $[G, G]$ is a normal subgroup of G. Note that $[G, G] = \{e\}$ iff G is abelian. A group is called **perfect** if $[G, G] = G$.

Let $H \triangleleft G$ and set G/H for the set of left cosets of H in G (which is the same as the set of right cosets). Note that for any $a, b \in G$ we have $(aH)(bH) = (ab)H$. It follows that if $A, B \in G/H$ then $AB \in G/H$ and the operation $(A, B) \mapsto AB$ defines a group structure on the set G/H. This group is called the **quotient group** (or **factor group**) of G by H. We see that if G is finite then $|G/H| = [G : H]$. The construction of quotient groups is of fundamental importance in group theory.

Exercise. Prove that G/H is abelian iff $[G, G] \subseteq H$.

If G, H are groups then a **homomorphism** from G to H is a function $f : G \longrightarrow H$ such that $f(ab) = f(a)f(b)$ for any $a, b \in G$. This implies that $f(e_G) = e_H$ and $f(a^{-1}) = f(a)^{-1}$. An injective (surjective) homomorphism is called a **monomorphism** (**epimorphism**). A bijective homomorphism is called an **isomorphism** and an isomorphism from G to G is called an **automorphism**.

The image $f(G)$ of a homomorphism f is a subgroup of H and the set $\ker f = \{g \in G : f(g) = 0\}$ is a normal subgroup of G called the **kernel** of f. It is easy to see that f is a monomorphism iff $\ker f = \{e\}$. Moreover, if $f(g) = h$ then the preimage $f^{-1}(h)$ is the coset $g \ker f$. Note that the image $f(G)$ is abelian iff $[G, G] \subseteq \ker f$.

Suppose that $K \triangleleft G$. The natural map $\psi : G \longrightarrow G/K$ given by $\psi(a) = aK$ is an epimorphism with kernel K. The map ψ is often called the **projection** or the **quotient map** from G to G/K.

The following results are very useful when dealing with quotient groups and homomorphisms.

First Homomorphism Theorem. Let $f : G \longrightarrow H$ be a homomorphism and $K \triangleleft G$ be such that $K \subseteq \ker f$. Set ψ for the quotient map $G \longrightarrow G/K$. There is unique homomorphism $\phi : G/K \longrightarrow H$ such that $f = \phi\psi$. It is defined by $\phi(aK) = f(a)$ for all $a \in G$. Moreover, $\phi(G/K) = f(G)$ and $\ker \phi = \psi(\ker f) = \ker f/K$.

Of special interest is the case when $K = \ker f$. Then we see that $\ker \phi$ is trivial, so ϕ is a monomorphism which identifies $f(G)$ and $G/\ker f$. In particular, if f is surjective then H and $G/\ker f$ are isomorphic.

Correspondence Theorem. Let $f : G \longrightarrow H$ be an epimorphism with kernel $K = \ker f$. If $L < G$ then the image $f(L) < H$. Conversely, if N is a subgroup of H then $f^{-1}(N)$ is a subgroup of G which contains K. Note that $f^{-1}(f(L)) = KL$. This defines a bijective correspondence between subgroups of G which contain K and subgroups of H. Under this correspondence normal subgroups correspond to normal subgroups and the inclusion is preserved.

Second Homomorphism Theorem. Suppose that $K \triangleleft G$, $H < G$ and $A \triangleleft H$. The natural map $\psi : H \longrightarrow HK/AK$ given by $\psi(h) = h(AK)$ is surjective and has kernel $A(H \cap K)$. In particular, $A(H \cap K)$ is a normal subgroup of H and the groups $H/A(H \cap K)$ and HK/AK are naturally isomorphic.

A special case is when A is trivial. Then we see that $H/H \cap K$ and HK/K are naturally isomorphic.

Third Homomorphism Theorem. Let $N \triangleleft G$, $K \triangleleft G$ and $N \subseteq K$. Then K/N is a normal subgroup of G/N and the groups G/K and $(G/N)/(K/N)$ are naturally isomorphic by $gK \mapsto (gN)(K/N)$.