This is a quick survey of some important elementary concepts of group theory, to prepare students for the groups that show up in Munkres' *Topology* (2nd ed), starting in Section 52.

Groups And Subgroups

In abstract algebra, a group is a set equipped with an operation that obeys a few essential algebraic rules. Formally, a *group* consists of a set G, a distinguished element $e \in G$ called the *identity*, and a function $m : G \times G \to G$, usually written like a multiplication operation

$$m(g_1, g_2) = g_1 \cdot g_2,$$

that satisfies the following three conditions.

- Associativity: For any $g_1, g_2, g_3 \in G$, $(g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3)$.
- Identity: For any $g \in G$, $e \cdot g = g \cdot e = g$.
- Inverses: For any $g \in G$ there exists an *inverse*, denoted g^{-1}, such that $g \cdot g^{-1} = g^{-1} \cdot g = e$.

It is easy to prove for any g that g^{-1} is unique, $\left(g^{-1}\right)^{-1} = g$, $(g_1 \cdot g_2)^{-1} = g_2^{-1} \cdot g_1^{-1}$, etc. Notice that commutativity $g_1 \cdot g_2 = g_2 \cdot g_1$ is not required of groups; groups that enjoy this additional property are called *commutative* or *Abelian*. If G is a group and H a subset of G that itself forms a group under the same operation, then we say that H is a *subgroup* of G.

Example: The nonzero real numbers $\mathbb{R}_{\neq 0}$ form a commutative group under ordinary multiplication, with $1 \in \mathbb{R}_{\neq 0}$ being the identity. The positive real numbers $\mathbb{R}_{>0}$ form a subgroup.

Example: Let n be a positive integer and GL_n the set of all $n \times n$ real matrices with nonzero determinant. Then GL_n is a group under matrix multiplication (because nonzero determinant guarantees an inverse), called the *general linear group*. Notice that GL_1 is just $\mathbb{R}_{\neq 0}$. For $n > 1$, GL_n is not commutative.

In general, there are many groups of real and complex matrices under multiplication that play prominent roles throughout mathematics and physics. They are simultaneously algebraic objects (groups) and geometric objects (smooth manifolds); such hybrids are known as *Lie groups*, and the matrix groups are called the *classical Lie groups*.

Example: The integers $\mathbb{Z}$ form a commutative group under addition with identity $0 \in \mathbb{Z}$. That is, we define the group operation by $g \cdot h = g + h$. The identity is 0, and $g^{-1} = -g$. (One must remember that $\cdot$ is abstract; it does not always mean "multiplication" in any traditional sense.) Similarly, the rationals $\mathbb{Q}$ and the reals $\mathbb{R}$ form commutative groups under addition; so does $\mathbb{R}^n$, under vector addition. The integers $\mathbb{Z}$ do *not* form a group under multiplication, because no integers other than ± 1 have integer inverses.

Example: Let X be any set and F the set of all bijections $f : X \to X$. Then F is a group under function composition, with the identity being the identity function. For instance, we can

view an $n \times n$ real matrix as a function $\mathbb{R}^n \to \mathbb{R}^n$, with matrix multiplication corresponding to function composition; then GL_n is a subgroup of the group of bijections of $\mathbb{R}^n$.

Products and Quotients

If G and H are two groups, then the Cartesian product $G \times H$ of sets comes with a natural group structure given by

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 \cdot g_2, h_1 \cdot h_2).$$

(Remember that the $\cdot$ on the left is for $G \times H$, the first $\cdot$ on the right is for G, and the second $\cdot$ on the right is for H.) This $G \times H$ is called a *product group*. The identity element is (e, e), and $(g, h)^{-1} = (g^{-1}, h^{-1})$.

Example: If $\mathbb{R}$ is the real numbers under addition, then $\mathbb{R} \times \mathbb{R}$ is $\mathbb{R}^2$ under vector addition.

We say that a subgroup H of G is *normal* if for any $g \in G$ and $h \in H$, $g \cdot h \cdot g^{-1} \in H$. If G is commutative, then all of its subgroups are normal. Given a normal subgroup H of G, define an equivalence relation on G by declaring $g_1 \sim g_2$ if $g_1 \cdot g_2^{-1} \in H$. Let $[g] \subseteq G$ denote the equivalence class of $g \in G$, and let G/H denote the set of equivalence classes. Define an operation $\cdot$ on G/H by

$$[g_1] \cdot [g_2] = [g_1 \cdot g_2].$$

This operation is well-defined and makes G/H a group, called a *quotient group*.

Example: Let n be a positive integer, $\mathbb{Z}$ the integers under addition, and

$$n\mathbb{Z} = \{\ldots, -2n, -n, 0, n, 2n, \ldots\}$$

the subgroup of integers divisible by n. Since $\mathbb{Z}$ is commutative, $n\mathbb{Z}$ is a normal subgroup. Two integers g_1, g_2 are equivalent iff $g_1 - g_2$ is divisible by n. There are n equivalence classes, namely $[0], [1], \ldots, [n-1]$. The group operation on these equivalence classes is essentially addition modulo n; for example, if $n = 12$ then $[5] + [9] = [14] = [2]$. This group $\mathbb{Z}/n\mathbb{Z}$ is commutative.

Example: Let $\mathbb{Z}/n\mathbb{Z}^* \subseteq \mathbb{Z}/n\mathbb{Z}$ denote the subset consisting of those $[g]$ such that g and n share no prime factors. Then $\mathbb{Z}/n\mathbb{Z}^*$ forms a commutative group under multiplication modulo n. Although $\mathbb{Z}/n\mathbb{Z}^*$ is a subset of $\mathbb{Z}/n\mathbb{Z}$, it is not a subgroup because the group operations are different.

Homomorphisms

If G and H are two groups, then a *homomorphism* $\phi : G \to H$ is a function that respects the group operations on G and H, in that

$$\phi(g_1 \cdot g_2) = \phi(g_1) \cdot \phi(g_2).$$

(Remember that the $\cdot$ on the left is for G and the $\cdot$ on the right for H.) An *isomorphism* is a bijective homomorphism. One can show that if ϕ is an isomorphism, then ϕ^{-1} is also a homomorphism and hence an isomorphism. The composition of two homomorphisms is a homomorphism, and the composition of two isomorphisms is an isomorphism. We say that G and H are *isomorphic*, written $G \cong H$, if there exists an isomorphism between them; this defines an equivalence relation on groups.

Example: The exponential function exp is a homomorphism from the reals $\mathbb{R}$ under addition to the positive reals $\mathbb{R}_{>0}$ under multiplication, since $\exp(x_1 + x_2) = \exp(x_1)\exp(x_2)$. It is bijective, so it is an isomorphism.

Example: The determinant function $\det : GL_n \to \mathbb{R}_{\neq 0}$ is a homomorphism, since $\det(AB) = \det(A)\det(B)$. It is surjective, but it is not injective for $n > 1$.

Example: $(\mathbb{R} \times \mathbb{R}) \times \mathbb{R}$ is isomorphic to $\mathbb{R}^3$ under vector addition, by $((x, y), z) \mapsto (x, y, z)$.

If $\phi : G \to H$ is any homomorphism, then the *image* $\phi(G) \subseteq H$ is a subgroup of H. Define the *kernel* of ϕ to be the subset

$$\ker \phi = \phi^{-1}(e) \subseteq G$$

of G that is sent to $e \in H$ by ϕ. It turns out that $\ker \phi$ is a normal subgroup of G.

Kernels, quotients, and homomorphisms are closely related. A homomorphism is injective if and only if its kernel is $\{e\}$. If H is a subgroup of G, then the inclusion map $H \hookrightarrow G$ defined by $h \mapsto h$ is an injective homomorphism. If H is a normal subgroup of G, then the quotient map $G \to G/H$ that sends $g \mapsto [g]$ is a surjective homomorphism with kernel H. If $\phi : G \to H$ is any homomorphism, then $\ker \phi$ is normal, and so we can form the quotient $G/\ker \phi$. The map

$$\psi : G/\ker \phi \to \phi(G)$$

described by $\psi([g]) = \phi(g)$ is well-defined and in fact an isomorphism. In summary, any homomorphism $\phi : G \to H$ can be written as a composition of homomorphisms

$$G \to G/\ker \phi \xrightarrow{\cong} \phi(G) \hookrightarrow H,$$

where the first map is surjective, the second bijective, and the third injective.

Some jargon now: A surjective homomorphism is called an *epimorphism* and an injective homomorphism a *monomorphism*. A homomorphism from a group G to itself is called an *endomorphism* of G; if it is an isomorphism as well, then it is called an *automorphism*. Notice that the set of automorphisms of G forms a group under function composition. Automorphism groups of various kinds are found throughout mathematics.