Math 411—Groups 101

Fall 2017

Definition 1 *A **group** is a set G with a binary operation $\cdot : G \times G \to G$ satisfying the following properties:*

- ***associativity**: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in G$;*
- ***identity**: there is an element $1 \in G$ such that $a \cdot 1 = 1 \cdot a = a$ for all $a \in G$;*
- ***inverse**: for any $a \in G$, there is an element $b \in G$ (the **inverse** of a) such that $a \cdot b = b \cdot a = 1$.*

It is easy to check that in a group, the identity element is unique, and there is a unique inverse of any element $a \in G$; the inverse is written a^{-1}, and the inverse of 1 must be 1. Examples of groups:

- the trivial group, consisting of a single element 1 with $1 \cdot 1 = 1$;
- $(\mathbb{Z}, +)$, the integers under the operation of addition;
- $(\mathbb{Z}^n, +)$, the set of n-tuples of integers, under the operation of vector addition;
- $(\mathbb{Z}/m, +)$, the set of integers mod m for some fixed integer m, under the operation of addition.

All of these groups are **abelian**, which is to say that $a \cdot b = b \cdot a$ for all $a, b \in G$. Not all groups are abelian though. For instance, $GL_n(\mathbb{R})$, the group of invertible $n \times n$ matrices with real entries under the operation of matrix multiplication, is not commutative for $n \geq 2$.

Definition 2 *A **homomorphism** between two groups G, H is a map $\phi : G \to H$ for which $\phi(g_1 \cdot g_2) = \phi(g_1) \cdot \phi(g_2)$ for all $g_1, g_2 \in G$.*

It follows from the definition that any homomorphism ϕ must satisfy $\phi(1) = 1$ and $\phi(g^{-1}) = (\phi(g))^{-1}$ for all $g \in G$. Also, if $\phi : G \to H$ and $\psi : H \to J$ are homomorphisms, then $\psi \circ \phi : G \to J$ is a homomorphism as well.

Definition 3 *An **isomorphism** between two groups G, H is a homomorphism that is also a bijection.*

It follows from the definition of isomorphism that if $\phi : G \to H$ is an isomorphism, then the inverse map $\phi^{-1} : H \to G$ is also an isomorphism. Two groups are **isomorphic** if there exists an isomorphism between them. Note that the identity map from a group G to itself is an isomorphism.