Cluster A: Getting a feel for groups

Pre-requisites.

I assume you are familiar with basic notions of sets, injections, bijections, and proof. Other than that, the only facts you need are the following:

DEFINITION 0.1 (What's a group?). A *group* is a pair (G, m) where G is a set, and m is a map

$$m : G \times G \to G.$$

We will usually write[1]

$$m(g, h) := g \cdot h := gh.$$

The pair (G, m) must satisfy the following:

- (Identity)There exists an element $1 \in G$ such that $1 \cdot g = g \cdot 1 = g$ for all $g \in G$.
- (Inverses) For every element $g \in G$, there exists an element (possibly different, possibly the same) g^{-1} such that $gg^{-1} = g^{-1}g = 1$, and
- (Associativity) $g(hk) = (gh)k$ for all $g, h, k \in G$.

The map m is called the *group multiplication*, the *multiplication*, or the *group operation*, of the group.

REMARK 0.2. Be warned that $gh \neq hg$ in general. Note that we are already writing gh instead of $g \cdot h$, or of $m(g, h)$.

REMARK 0.3. We will often write a group simply as G, and not (G, m), although m is necessarily part of the data. The notation G simply means that the group operation should be understood: For instance, $\mathbb{Z}$ is usually understood to mean the set of integers together with usual addition of integers as the group operation.

[1]Depending on context, we may sometimes write $g \cdot h$, while we may other times write gh for brevity. This is the same convention as in multiplying variables in standard high school algebra.

REMARK 0.4. The existence of inverses allows us to use the cancellation law. That is, if a, b, c are elements of a group G, we have the implication

$$ab = ac \implies b = c.$$

This is because we can multiply both sides of the equation by a^{-1} and conclude $a^{-1}(ab) = (a^{-1}a)b = 1b = b$. Notice that we are using every property of a group—the identity, inverses, and associativity—in proving the cancellation law.

DEFINITION 0.5 (Group homomorphisms and isomorphisms). Let G and H be groups. A *group homomorphism* is a map of sets

$$\phi : G \to H$$

such that

$$\phi(gg') = \phi(g)\phi(g').$$

(I.e., ϕ respects multiplication.) An *isomorphism* of groups is a group homomorphism $\phi : G \to H$ which is also a bijection of sets.

DEFINITION 0.6 (Subgroups). Let G be a group. A subset $H \subset G$ is called a *subgroup* if

- H contains the identity of G,
- If $h \in H$, then $h^{-1} \in G$ is also in H, and
- If h and h' are in H, then so are hh' and $h'h$.

0.1. Goals. The goal of these problems is to start becoming familiar with the kinds of manipulations we'll want to do computations with groups.

1. Some basics

(a) Show that the empty set does not admit a group structure.

(b) Show that the identity element of a group G is unique. (That is, if two elements 1 and $1'$ satisfy the defining property of the identity element, then $1 = 1'$.)

(c) Given an element $g \in G$, show that g^{-1} is unique. (That is, given elements h, h' satisfying the defining property of g^{-1}, show that $h = h'$.)

(d) Let G and H be two groups such that each group contains only one element. Show that G and H are isomorphic as groups. (That is, there is a unique group of cardinality 1.)

(e) Let G and H be two groups such that each group contains only two elements. Show that G and H are isomorphic as groups.

(f) If you have the free time, let G and H be two groups such that each group contains only three elements. Show that G and H are isomorphic as groups. (This will become much easier to once we have Lagrange's Theorem.)

(g) Let $\phi : G \to H$ be a group isomorphism between two groups. Since ϕ is a bijection, there is a unique inverse map of sets $\psi : H \to G$. Show that ψ must be a group homomorphism.

(h) Show $g = g^2$ in a group G if and only if $g = 1$.

(i) If $\phi : G \to H$ is a group homomorphism, show that ϕ sends the identity of G to the identity of H.

(j) If $\phi : G \to H$ is a group homomorphism, show that $\phi(g^{-1}) = \phi(g)^{-1}$.

2. Group homomorphisms versus maps of sets

Let $\phi_3 : \mathbb{Z} \to \mathbb{Z}$ be the map $\phi_3(n) = 3n$. So for instance, $\phi(2) = 6$. We think of the integers as a group under addition.

(a) Show that ϕ_3 is a group homomorphism.

(b) Show that there exists a map of *sets* $\psi : \mathbb{Z} \to \mathbb{Z}$ such that $\psi \circ \phi_3 = \mathrm{id}_{\mathbb{Z}}$.

(c) Show that no choice of such a ψ can be a group homomorphism.

(d) For any integer k, define a map of sets $\phi_k : \mathbb{Z} \to \mathbb{Z}$ by $\phi(n) = kn$. Show this defines a group homomorphism from $\mathbb{Z}$ to $\mathbb{Z}$. Determine all k for which this map is an isomorphism.

3. Orders of group elements

(a) Show that the non-zero complex numbers, written $\mathbb{C}^\times$, form a group under multiplication.

(b) For any element $g \in G$, we will always write the expression $g \cdot g \cdot \ldots \cdot g$ (with n appearances of g) as g^n. By convention, g^0 is the identity of a group. Show that for all $n \geq 0$, $\mathbb{C}^\times$ contains an element z for which $z^n = 1$.

(c) Given an element $g \in G$ of a group, the smallest, non-zero number n for which $g^n = 1$ is called the *order* of g. If g^n never equals 1, we say g is an element of infinite order. Show that $\mathbb{Z}$ only has elements of order 1 or infinity.

4. Product groups

Let G and H be groups. Define a map

$$m : (G \times H) \times (G \times H) \to G \times H, \qquad m((g,h),(g',h')) = (gg', hh').$$

Note that throughout this problem, 1 may refer to either the group unit of G, or the group unit of H.

(a) Show that m defines a group structure on $G \times H$.

(b) Show that $(g,1) \cdot (1,h) = (1,h) \cdot (g,1)$.

(c) Recall that a group A is called abelian if for all $a, a' \in A$, we have $aa' = a'a$. Show that if G and H are abelian, then $G \times H$ is abelian (with the above group structure).

(d) Show that $\mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z}$ is a subgroup of $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$.

(e) Show that the maps $G \to G \times H, g \mapsto (g,1)$ and $G \times H \to G, (g,h) \mapsto g$ are group homomorphisms.

5. The set of automorphisms is a group

We mentioned in class that groups are a useful language for describing *symmetries* of an object. What do we mean by a symmetry? A symmetry is an invertible operation from a mathematical object to itself, preserving some structure. Here we explore examples of this idea.

(a) Fix a set S. Let $\mathrm{Aut}(S)$ be the set of all bijections $S \to S$. Note there is a map $\mathrm{Aut}(S) \times \mathrm{Aut}(S) \to \mathrm{Aut}(S)$ given by composing bijections. Show that this gives a group structure on $\mathrm{Aut}(S)$. (Using the above philosophy, the mathematical object is a set S, and we view it as having no structure save the fact that S is a set.)

(b) Now fix a group G. Let $\mathrm{Aut}_{\mathrm{Group}}(G)$ be the set of all *group isomorphisms* from G to itself. Show that $\mathrm{Aut}_{\mathrm{Group}}(G)$ is itself a group. (Using the above philosophy, the mathematical object is G, and the structure we're preserving is its group structure—i.e., the identity and multiplication.)

(c) (*) If you know what a topological space is, let X be a topological space, and $\mathrm{Aut}(X)$ the set of homeomorphisms from X to itself. Show that $\mathrm{Aut}(X)$ is a group.

(d) Fix $n \geq 1$. Show that $GL_n(\mathbb{C})$—the the set of $n \times n$ complex, invertible matrices—form a group. Show the same is true for $GL_n(\mathbb{R})$. (Using the

philosophy above, this is the set of all operations on an n-dimensional vector space that preserve the structure of *linearity*.)

(e) Fix $n \geq 1$. Show that $SL_n(\mathbb{C})$—the set of $n \times n$ complex matrices with determinant 1—form a group. Likewise for $SL_n(\mathbb{R})$. (Using the philosophy above, this is the set of all operations on an n-dimensional vector space that preserve the structure of *linearity and oriented volume*.)

(f) For any $n \geq 1$, show that $O(n)$—the set of $n \times n$ real orthogonal matrices—form a group. (Using the philosophy above, this is the set of all operations on an n-dimensional vector space that preserve the structure of *linearity and inner product*.)

6. Extras

(a) Let H and K be subgroups of G. Show their intersection is a subgroup.

(b) Given a group $G = (G, m)$, define the *opposite group* $G^{\text{op}} = (G, w)$ by the operation

$$w(g, h) := m(h, g).$$

That is, G^{op} as a set is the same set as G, but its multiplication happens in the opposite order. Show that G^{op} is a group.

(c) Show that the map $G \to G^{\text{op}}$ given by $g \mapsto g^{-1}$ is a group isomorphism.

(d) Let $\phi : G \to H$ be a group homomorphism. The *kernel of* ϕ, written $\ker \phi$, is the set of all g for which $\phi(g) = 1$. Show that the kernel of any group homomorphism is a subgroup of G.

(e) The *image of* ϕ is the set of all $h \in H$ such that $h = \phi(g)$ for some $g \in G$. Show that for any group homomorphism $\phi : G \to H$, the image of ϕ is a subgroup of H.

7. The sign representation

(a) Let S_n be the symmetric group on n elements. (Automorphisms of a set of n elements.) For every element $\sigma \in S_n$, let $\phi(\sigma)$ be the $n \times n$ matrix which sends the standard basis vector $e_i \in \mathbb{R}^n$ to the vector $e_{\sigma(i)}$. Show that the assignment $\phi : S_n \to GL_n(\mathbb{R})$ is a group homomorphism.

(b) List every element $\sigma \in S_3$ and write out the matrix $\phi(\sigma)$ for each of them.

(c) Show that the determinant defines a group homomorphism $\det : GL_n \to \mathbb{R}^\times$, which sends $A \mapsto \det A$. (You may use properties of determinants you learned from linear algebra class.) What is the special name we usually give to the kernel of this map?

(d) Consider the composite group homomorphism $S_n \to GL_n \to \mathbb{R}^\times$. We call this the *sign representation* of S_n. What is its image? (It is a subgroup of $\mathbb{R}^\times$.)

8. Linear maps of integers

By the above exercise, the set $\mathbb{Z}^2 := \mathbb{Z} \times \mathbb{Z}$ is a group. (In fact, an abelian group.) Consider a 2x2 integer matrix

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

which defines a map $\mathbb{Z}^2 \to \mathbb{Z}^2$ in the usual way that matrices do. Specifically, given an element $(x, y) \in \mathbb{Z}^2$, the map sends

$$(x, y) \mapsto (ax + cy, bx + dy).$$

(a) Show that the above map is always a group homomorphism from $\mathbb{Z}^2$ to $\mathbb{Z}^2$.

(b) Determine when A is an injective group homomorphism, using the determinant of A.

(c) Determine when A is a group isomorphism, using the determinant of A.

9. Some fun linear algebra

(a) Let n be an odd, non-zero integer. Show that every element of $O(n)$ has 1 as an eigenvalue. (Hint: What happens when you apply A^T to $A - I$?)