Homework 2

1. 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.

2. 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 $\mathbb{R}^\times$.)

3. Centers

(a) For any group G, the *center* of G is the set of those g such that g commutes with all elements of G. That is, $gh = hg$ for all h. Show that the center of G is a normal subgroup of G.

(b) What is the center of $GL_n(\mathbb{R})$ for $n \geq 1$?

4. Using divisibility

(a) Let G be a group of order p for some prime p. Let x be a non-identity element of G. Show that x must have order p.

(b) Let G be a group of order p^n for some prime p and $n \geq 1$. Show that G must contain an element of order p.

(c) Let G be a group (possibly infinite). Let H and H' be finite subgroups. Show that if $gcd(|H|, |H'|) = 1$, then $H \cap H' = \{1\}$.

5. Using divisibility again

(a) Let G be a finite abelian group. Show that the map $x \mapsto x^n$, for any integer $n \geq 0$, is a group homomorphism.

(b) Suppose further that $gcd(|G|, n) = 1$. Show that the map $x \mapsto x^n$ is a group automorphism of G.

6. Free groups

What does a group with a set of generators, but with *no relations* look like? If the set of generators is S, this group is called the *free group* with generating set S. You will prove its existence, and its universal property, in this exercise.

Definition 6.1. Let $S = \{a, b, c, \ldots\}$ be a set. Though I have written a, b, c as though the elements may be enumerable (i.e., countable), S need not be countable. For $n \geq 0$, a *word of length* n in S is defined to be a map of sets $\{1, \ldots, n\} \to S$. The *empty word* is the map from the empty set to S, and is the unique word of length 0.

So a word of length n is simply an ordered string of n elements of S, possibly with repetitions.

EXAMPLE 6.2. If $S = \{a, b, c\}$, then here are the words of lengths 0 to 2:

$$\emptyset \qquad \text{(the empty word)}$$

$$a, \qquad b, \qquad c$$

$$aa, \qquad bb, \qquad cc, \qquad ab, \qquad ba, \qquad bc, \qquad cb, \qquad ca, \qquad ac.$$

Here are some examples of words of length 5:

$$aaaba, \qquad ababa, \qquad acccb.$$

Given a set S, let $\overline{S}$ be the set given by adjoining a new element for every $s \in S$. We will write this new element as "s^{-1}" and call it the inverse of s. So for example, if $S = \{a, b, c, \ldots\}$, then

$$\overline{S} = \{a, a^{-1}, b, b^{-1}, c, c^{-1} \ldots\}.$$

DEFINITION 6.3. A word in $\overline{S}$ is called *reduced* if a letter in the word never appears next to its inverse.

REMARK 6.4. As an example, here are some *unreduced* words, with unreduced bits underlined.

$$abba\underline{aa^{-1}}bcb\underline{cc^{-1}}b, \qquad \underline{aa^{-1}}, \qquad a\underline{b^{-1}b}b^{-1}c, \qquad ab^{-1}\underline{bb^{-1}}c.$$

Given an unreduced word, we can make it reduced by simply removing two adjacent letters when one is the inverse of the other. For example, here are the reductions of the above words:

$$abbabcbb, \qquad \emptyset, \qquad ab^{-1}c, \qquad ab^{-1}c.$$

Note that to fully reduce a word, one may require a few steps:

$$ab^{-1}\underline{cc^{-1}}ba^{-1} \to ab^{-1}ba^{-1} \to aa^{-1} \to \emptyset.$$

Regardless, since every word is by definition of finite length, this reduction process terminates. Given any word in $\overline{S}$, there is a unique reduction of that word, in which no letter appears next to its inverse.

Given two words w_1 and w_2, we may simply concatenate them (i.e., put them side by side) to create a new word. For instance, if

$$w_1 = abc, \qquad w_2 = c^{-1}baa$$

then we have

$$w_1w_2 = abcc^{-1}baa, \qquad w_2w_1 = c^{-1}baaabc.$$

(I've been told this is a common way to create new words in German.) Note that even if two words are reduced, their concatenation may not be. Also note that w_1w_2 need not equal w_2w_1.

Definition 6.5. Let S be a set. The *free group* on S is the set of reduced words of length $n \geq 0$ in $\overline{S}$. The group multiplication is given by concatenating two words, then reducing the concatenation.

The problem:

(a) Show that any word in $\overline{S}$ admits a unique reduction.
(b) Show that the above operation is associative.
(c) Show that the free group is in fact a group.
(d) Let G be a group, and let $j : S \to G$ be a map *of sets*. Show that this extends to a group homomorphism $F(S) \to G$.
(e) Show there is a bijection of sets

$$\{\text{Group homomorphisms } F(S) \to G\} \cong \{\text{Set maps } S \to G\}.$$