Solutions Cluster A: Getting a feel for groups

1. Some basics

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

By definition, a group must contain at least one element—the identity element.

(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 $1 = 1'$.)

If 1 is the identity, then it must satisfy the equation $1g = g1 = g$ for all g. In particular, if $1' = g$, we must have $11' = 1'$. On the other hand, if 1' is also the identity element, we must have $11' = 1$. By transitivity, we conclude$1 = 1'$.

(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 $h = h'$.)

Suppose h and h' are both inverses to g. Then $gh' = 1$. By multiplying both sides of the equation by h on the left, we obtain $h(gh') = h$. But by associativity, the lefthand side becomes $h(gh') = (hg)h' = 1h' = h'$. By transitivity of equality, we have that $h' = h$.

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.

By distributivity of multiplication over addition, $k(a+b) = ka+kb$ for all $k, a, b \in \mathbb{Z}$. Hence $\phi_3(a+b) = 3(a+b) = 3a+3b = \phi_3(a)+\phi_3(b)$.

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

There are many such choices. For instance, by the division algorithm, we can uniquely write any number $a \in \mathbb{Z}$ as $a = 3k + r$ where k is an integer and r is some integer between 0 and 2. Setting $\psi(a) = k$ clearly satisfies $\psi(3k) = k$.

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

In general, note that $1 + \ldots + 1 = n$, where the addition occurs n times. Hence any group homomorphism $\psi : \mathbb{Z} \to \mathbb{Z}$ must satisfy $\psi(1) + \ldots + \psi(1) = \psi(n)$, where the addition again occurs n times on the lefthand side. But this means that $\psi(n)$ must be divisible by n. In contrast, if $\psi \circ \phi_3(1) = 1$, we must have that $\psi(3) = 1$, and 1 is not divisible by 3.

(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.

We showed that this is a homomorphism in general in part (a) above. By our solution to part (c), we see that any homomorphism ψ must send $\phi_k(1) = k$ to a number divisible by k. On the other hand, $\psi \circ \phi_k = \mathrm{id}$ means $\psi(\phi_k(1)) = 1$. The only numbers dividing 1 are $k = \pm 1$, so we conclude k must be equal to ± 1. In either case ψ_k is a bijection, as the function $n \mapsto -n$ and $n \mapsto n$ are both bijections.

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.

Let $\sigma, \sigma' \in S_n$. By definition, $\phi(\sigma)$ sends e_i to $e_{\sigma(i)}$, and likewise for $\phi(\sigma')$. Recall that if two matrices represent two linear transformations T and T', then the product of the two matrices represent the composition of the linear transformations T and T'. Hence the product matrix $\phi(\sigma')\phi(\sigma)$ sends e_i to

$$\phi(\sigma')(\phi(\sigma)(e_i)) = \phi(\sigma')(e_{(\sigma(i))}) = e_{\sigma'(\sigma(i))} = e_{(\sigma'\sigma)(i)}.$$

A linear transformation (and hence its matrix) is determined by what it does on a set of basis vectors, and we've seen that $\phi(\sigma')\phi(\sigma)$ represents the linear transformation sending e_i to $e_{\sigma'\sigma(i)}$. By definition, this is the linear transformation represented by $\phi(\sigma'\sigma)$. Hence we have a group homomorphism.

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

Now that we have cycle notation, we can list the elements as follows:

$$\text{id}, \quad (12), \quad (23), \quad (13),$$
$$(123) \quad (132).$$

In corresponding order, the matrices $\phi(\sigma)$ are given by

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix},$$
$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

Note that we see that the ith column of the matrix is given by the $\sigma(i)$ basis vector.

(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?

The determinant is a group homomorphism because $\det(AB) = \det(A)\det(B)$ for any two matrices A, B. The identity element of $\mathbb{R}^\times$ under multiplication is 1, so the kernel of this map is given by all matrices with determinant 1. The special name is the special linear group of rank n, otherwise written as $SL_n(\mathbb{R})$.

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

If $n \geq 2$, the image is the set $\{\pm 1\} = \{1, -1\} \subset \mathbb{R}^\times$. By the definition that $\phi(\sigma)$ sends e_i to $e_{\sigma(i)}$, we see that every column of $\phi(i)$ has exactly one non-zero entry, given by the number 1. Hence the determinant formula guarantees that $\det(\phi(\sigma))$ is given as some product of many copies of 1 and -1; i.e., the determinant is either 1 or -1. On the other hand, we can see that the permutation $(12) \in S_n$ for any $n \geq 2$ has determinant -1, for instance by cofactor expansion. Finally, if $n = 1$, the image is given by the determinant of the identity matrix—i.e., the image is the set $\{1\} \subset \mathbb{R}$.

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.

Let Z be the center of G. Note that the identity $gh = hg$ implies that $g = hgh^{-1}$ for any $g \in Z, h \in G$. (Just multiply by h^{-1} on the right.) To prove that Z is normal, we must show that for all $h \in G$, $hZh^{-1} = Z$. Well, for any $g \in Z$, we know that $hgh^{-1} = g$. This shows both $Z \subset hZh^{-1}$ and $hZh^{-1} \subset Z$ at the same time; hence $Z = hZh^{-1}$.

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

Let A be a matrix in the center. This means that for any invertible matrix B, we have $BAB^{-1} = A$. We now interpret the entries m_{ij} of A as a change-of-basis formula: Let $v_1, \ldots, v_n$ be the columns of B. Since B is invertible, these vectors form a basis for $\mathbb{R}^n$. Then the entries m_{ij} are numbers such that BAB^{-1} sends v_i to the linear combination $\sum_{j=1}^n m_{ij} v_j$. Importantly, these coefficients m_{ij} are the same for any basis $\{v_i\}$, because regardless of the basis given by B, we will have $(m_{ij}) = A$.

This observation proves that m_{ij} must equal zero for $i \neq j$. For if $m_{ij} \neq 0$ for some pair $i \neq j$, let B' be the matrix obtained by scaling the basis vector v_j by (for instance) 12, while keeping all other basis vectors the same. This means B' defines a new basis

$$v'_1 = v_1, \qquad \ldots, \qquad v'_j = 12v_j, \qquad \ldots, \qquad v'_n = v_n.$$

On the other hand,

$$BAB^{-1}(v_i) = \sum_{k=1}^{n} m_{ik} v_j \qquad \text{and} \qquad B'AB'^{-1}(v_i') = \sum_{k=1}^{n} m_{ik} v_k' = 12 m_{ij} v_j + \sum_{k \neq i}^{n} m_{ij} v_k.$$

Here, we have used the fact that the coefficients m_{ik} are equal in any basis because A is in the center of $GL_n(\mathbb{R})$. Moreover, since the matrices BAB^{-1} and $B'AB'^{-1}$ are both equal to A, they define the same linear transformation—since $v_i = v_i'$, and since the v_i form a basis, the coefficients above are uniquely determined. Hence we arrive at the statement that $12m_{ij} = m_{ij}$. We conclude that $m_{ij} = 0$ when $i \neq j$.

Now we are home-free. If A must be a diagonal matrix, all of its diagonal entries must be equal, as any B which simply changes the ordering of an ordered basis will swap the eigenvalues of A. QED.

Note: There are many ways to prove this face, and I chose what I think is the cleanest. You can also prove that the center of $GL_n(\mathbb{R})$ consists of matrices of the form λI by induction on n, or by explicit computations for well-chosen matrices.

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.

The subgroup $\langle x \rangle$ generated by x must have order dividing $|G|$ by Lagrange's theorem. We know $|\langle x \rangle| > 1$ since x is not the identity. But the only non-negative number that divides p aside from 1 is p because p is prime by assumption; this shows $|\langle x \rangle| = p$. By definition, the order of x is $|\langle x \rangle|$, so x has 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.

Let x be an element that is not the identity of G. The subgroup $|\langle g \rangle|$ must have some order dividing the order of G by Lagrange's theorem, so we conclude that $x^{p^k} = 1$ for some k between 1 and n. (It is a basic fact that the only numbers dividing p^n are numbers of the form p^k.) Whatever this k is, consider the element $y = x^{p^{k-1}}$. By definition, it has order p, since $y^p = x^{p(p^{k-1})} = x^{p^k} = 1$.

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

If H and H' are subgroups of G, so is $H \cap H'$. This can be seen as follows: Since H and H' are subgroups, 1_G is in both of them. Hence 1_G is in their intersection. Similarly, if both g_1 and g_2 are in both H and

H', we see that $g_1 g_2$ is in both H and H' by the closure of subgroups. This means $g_1 g_2 \in H \cap H'$. Finally, if $h \in H$ and H', then its inverse is in both H and H'. We conclude that $H \cap H'$ is a subgroup of both H and of H'. By Lagrange's Theorem, this subgroup must have an order dividing the orders of both H and of H'. However, since H and H' have greatest common divisor 1, the order of $H \cap H'$ must be 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.

Let $+$ denote the group operation in G. Then $\phi : x \mapsto x^n$ is in fact the homomorphism $x \mapsto x + \ldots + x$, where the addition occurs n times. We then have that

$$\phi(x+y) = (x+y) + \ldots + (x+y).$$

One can rearrange the terms on the righthand side because $x+y = y+x$ for an abelian group. We conclude

$$\phi(x+y) = (x + \ldots + x) + (y + \ldots + y).$$

This proof did not, in fact, rely on G being finite.

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

Since G is finite, it suffices to show that the map $\phi : x \mapsto x^n$ is injective. To show this, it suffices to show that the kernel of ϕ is trivial. Suppose that x is in the kernel, so that $x^n = id$. Then the group generated by x must have order diving n. [1] At the same time, it is a subgroup of G, so it must have order diving n. Since the only non-negative number dividing both n and $|G|$ is 1 by hypothesis, $\langle x \rangle$ must be a subgroup of G with one element—i.e., x must be the identity. This shows that the kernel consists only of the element 1_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.

[1] To see this, suppose otherwise. Then $n = aN + r$, where N is the order of $\langle x \rangle$, and where r is between 1 and $N-1$. We then see that $x^{aN+r} = (x^N)^a x^r = x^r = 1$. Hence every element of $\langle x \rangle$ is of the form $1, x, \ldots, x^r$. This is a contradiction since $r < N$ and there must be N elements in $\langle x \rangle$ by definition.

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 $F(S) \to G$.

Let $s \in S$ be an element of the set, and $j(s) \in G$ its image in G. Let us denote by $\overline{j} : \overline{S} \to G$ the function sending $s \mapsto j(s)$ and $s^{-1} \mapsto j(s)^{-1}$. We then define a function

$$\phi_j : \text{Word}(\overline{S}) \to G$$

by sending any word $W = s_1 \ldots s_l$, with $s_i \in \overline{S}$, to the element

$$\phi_j(s_1) \cdot \phi_j(s_2) \cdot \ldots \cdot \phi_j(s_l).$$

We must prove this is well-defined on $F(S)$, and a homomorphism. Well, if w is a reduction of W, it is obtained by canceling pairs of letters appearing next to their inverses. On the other hand, if any letter s appears next to its inverse s^{-1} inside W, the above string of multiplications in G will also see an appearance of $\phi_j(s)$ appearing next to $\phi_j(s^{-1}) = \phi_j(s)^{-1}$. Hence if we cancel two inverse letters in the word W to obtain a new word w', we see that $\phi_j(W) = \phi_j(w')$. More explicitly, given a product of many elements in G, omitting an appearance of $\phi_j(s)\phi_j(s)^{-1}$ (or of $\phi_j(s)^{-1}\phi_j(s)$) does not change the value of the multiplication:

$$\phi_j(s_1)\cdot\ldots\cdot\phi_j(s)\phi_j(s)^{-1}\cdot\ldots\cdot\phi_j(s_l)) = \phi_j(s_1)\cdot\ldots\cdot 1_G\cdot\ldots\cdot\phi_j(s_l)) = \phi_j(s_1)\cdot\ldots\cdot\phi_j(s_l))$$

(and likewise for canceling the appearance of $\phi_j(s)^{-1}\phi_j(s)$). So if the words w_i' for $i = 1, \ldots, I$ are the words one passes through on reducing

W to its reduction w, we have a string of equalities:

$$\phi_j(W) = \phi_j(w'_1) = \ldots = \phi_j(w'_I) = \phi_j(w).$$

This shows that ϕ_j is well-defined on $F(S)$. To show that ϕ_j defines a homomorphism, let $W = w' \cdot w''$ be a concatenation of words, and let w be its reduction. We must prove that

$$\phi_j(w) = \phi_j(w') \cdot \phi_j(w'').$$

By well-definedness, it suffices to show $\phi_j(W) = \phi_j(w') \cdot \phi_j(w'')$. This is obvious, since if

$$w' = s'_1 \ldots s'_{l'}, \qquad w'' = s''_1 \ldots s''_{l''}$$

then

$$\begin{aligned} \phi_j(W) &= \phi_j(s'_1) \cdot \ldots \phi_j(s'_{l'}) \cdot \phi_j(s''_1) \cdot \ldots \cdot \phi_j(s''_{l''}) \\ &= (\phi_j(s'_1) \cdot \ldots \phi_j(s'_{l'})) \cdot (\phi_j(s''_1) \cdot \ldots \cdot \phi_j(s''_{l''}) \\ &= \phi_j(w') \cdot \phi_j(w''). \end{aligned}$$

(e) Show there is a bijection of sets

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

We above define a homomorphism $\phi_j : F(S) \to G$ for any function $j : S \to G$. This defines a function

$$\Phi : \{\text{Set maps } S \to G\} \to \{\text{Group homomorphisms } F(S) \to G\}$$

given by $j \mapsto \phi_j$. We define an inverse map Ψ as follows: If ϕ is a group homomorphism, it assigns a value to the reduced word s, for any $s \in S$. So we define $\Psi(\phi) := \psi_\phi$ to be the function sending s to $\phi(s)$. We must show that $\Psi \circ \Phi$ and $\Phi \circ \Psi$ are the identities. Well, given a homomorphism $\phi : F(S) \to G$, let w be the word

$$w = s_1 \ldots s_l$$

where the s_i are whatever letters of $\overline{S}$ are in w. we know that

$$\phi(w) = \phi(s_1 \cdot \ldots s_l) = \phi(s_1) \cdot \ldots \cdot \phi(s_l)$$

by the group homomorphism property, and the fact that every word is a product of one-letter words. So the value of ϕ on one-letters words—i.e., its value on S—determines its value on all elements of $F(S)$. This shows that $\Phi \circ \Psi$ is the identity. On the other hand, we have defined Φ so that $\Phi(j) = \phi_j$ simply sends one-letter words to the value $j(s)$. Hence $\Psi \circ \Phi$ is also the identity. This completes the proof.

Homework 3

1. Cosets of S_3 with respect to S_2

Let S_3 be the symmetric group on 3 elements. Recall that this is the set of all bijections from $\underline{3}$ to itself, where $\underline{3} = \{1, 2, 3\}$. Let $H \subset S_3$ be the set of all bijections $\tau : \underline{3} \to \underline{3}$ such that $\tau(3) = 3$—i.e., the subset of all bijections that fix 3.

(a) Show H is a subgroup of S_3.

There are two ways to do this: An explicit and a non-explicit. Explicitly, one sees that the only bijections τ fixing 3 are those of the form $1_G = \mathrm{id}_{\underline{3}}$, and $\tau = (12)$. This is because any bijection of $\underline{3}$ fixing 3 must only permute the elements $1, 2 \in \underline{3}$, and τ is the only permutation of 3 doing this. One sees that $\tau^2 = \mathrm{id}$, so the set $\{1_G, \tau\}$ is a subgroup. Non-explicitly, if τ and τ' both fix 3, then $\tau \circ \tau'(3) = \tau(\tau' 3) = \tau(3) = 3$ and $\tau' \circ \tau(3) = \tau'(\tau(3) = \tau'(3) = 3$. Hence H is fixed under products. The identity obviously fixed 3, and the inverse of any function with $\tau(3) = 3$ is also a function fixing 3. This shows that H is a subgroup of S_3.

(b) So H acts on $G = S_3$. How many elements are there in the orbit space? That is, how many orbits are there?

By the proof of Lagrange's theorem, we know that $|G|$ is equal to $|H|$ times the number of orbits of the H action on G. Well, $|G| = 3!$, while H has only two elements in it (for instance, by the explicit computation in part (a)). This means that there are exactly $6/2 = 3$ orbits.

(c) Finally, write out each orbit explicitly. This means you must write out which elements of S_3 are in each orbit.

As in a previous homework, we can write the elements of S_3 as

$$\mathrm{id}, \qquad (12), \qquad (23), \qquad (13),$$

$$(123) \qquad (132).$$

We know that H is one orbit on its own, so we have an orbit given by

$$\mathcal{O}_{1_G} = H = \{\text{id}, (12)\}.$$

Arbitrarily choosing an element not in this orbit—for instance, (23),—we obtain another orbit by looking at (12)(23) and (23):

$$\mathcal{O}_{(23)} = \{(23), (231)\}.$$

Knowing there is only one orbit let, we can put the remaining elements in the third orbit:

$$\mathcal{O}_{13} = \{(13), (321)\}.$$

(d) For any $n \geq 1$, let $H \subset S_n$ be the subgroup of all elements that fix n. Exhibit an isomorphism from H to S_{n-1}.

Let us define a function $\phi : S_{n-1} \to S_n$ which sends a bijection $\sigma : \underline{n-1} \to \underline{n-1}$ to the bijection ϕ_σ defines as follows: ϕ_σ sends $n \mapsto n$, and sends $i \mapsto \sigma(i)$ for $i \neq n$. This is a group homomorphism because

$$\phi_\sigma \circ \phi_{\sigma'}(i) = \phi_\sigma(\sigma'(i)) = \sigma(\sigma'(i)) = (\sigma\sigma')(i) = \phi_{\sigma\sigma'}(i)$$

for $i \neq n$, and

$$\phi_\sigma \circ \phi_{\sigma'}(n) = n = \phi_{\sigma\sigma'}(n)$$

otherwise. This map is an injection because if $\phi_\sigma = \text{id}_{\underline{n}}$, this means that $\sigma(i) = i$ for every i. But the only such bijection is the identity bijection, hence the kernel is trivial. It is a surjection because any bijection that fixes n is determined uniquely by a bijection on the remaining elements $1, \ldots, n-1$.

(e) How many orbits are there of the action of H on S_n?

As before, the number of orbits is equal to the order of S_n divided by the order of H. Since H is isomorphic to S_{n-1}, this is $n!$ divided by $(n-1)!$. Hence the number of orbits is n.

2. Cyclic groups

A group G is called *cyclic* if there exists $g \in G$ for which $\langle g \rangle = G$.

(a) Show that if two cyclic groups have the same order (finite or otherwise) then they must be isomorphic.

Let G and H be two cyclic groups of the same order n. Assume $G = \langle g \rangle$ for some $g \in G$, and $H = \langle h \rangle$ for some $h \in H$. Each receives a group homomorphism from $\mathbb{Z}$ by sending $1 \to g$, and $1 \to h$. The kernel of both these homomorphisms is $n\mathbb{Z}$, while the function is a surjection by the assumption that g and h generate G and H, respectively. Hence by the First Isomorphism Theorem, we have isomorphisms $G \cong \mathbb{Z}/n\mathbb{Z} \cong H$. By transitivity of group isomorphisms, we are done.

(b) Show that S_2 is cyclic.

S_2 consists of two elements: the identity, and a non-trivial element $\tau = (12)$. $\tau^2 = 1$ so we see that τ generates the whole subgroup.

(c) Show that $\mathbb{Z}$ is cyclic.

Any number n can be written as a finite sum of 1, or of -1. Specifically, we have $1 + \ldots + 1 = n$ for n positive, where the summation occurs n times. For n negative, we have $-1 + \ldots - 1 = n$. Hence $ZZ = \langle 1 \rangle$.

(d) Use Lagrange's theorem to show that any group of prime order must be cyclic. (Hint: Last homework.)

Let $g \neq 1$, and consider the subgroup $\langle g \rangle \subset G$. This must have order bigger than 1, since it contains at least two distinct elements—1 and g. On the other hand, it must have order dividing $|G|$. Since $|G|$ is prime, the only number bigger than 1 dividing $|G|$ is $|G|$ itself. This means $|\langle g \rangle| = |G|$, so $\langle g \rangle = G$.

(e) Prove that for any integer $n \geq 1$, there exists a cyclic group of order n. For instance, as a subgroup of S_n, or of $GL_2(\mathbb{R})$, or of $\mathbb{C}^\times$.

As a subgroup of S_n, one can take the subgroup generated by the cycle $\sigma = (1 \ldots n)$. As a subgroup of $GL_2(\mathbb{R})$, one can consider the subgroup generated by the matrix of rotating by $2\pi/n$ radians. Finally, as a subgroup of $\mathbb{C}^\times$, one can write the subgroup generated by the complex number $e^{2\pi i/n}$. These latter two groups are the easiest to prove as cyclic and of order n—clearly, rotation by $2\pi/n$ is an operation which becomes the identity after n iterations, so the group generated by this rotation has order at most n. We can enumerate the group elements by how much they rotate the plane: $2\pi/n, 2(2\pi/n), \ldots, (n-1)(2\pi/n)$. If the order were any smaller than n, we would conclude that a rotation of less than 2π acts as the identity on the plane, which is untrue.

3. Abelian groups

A group G is called *abelian* if for all $g_1, g_2 \in G$, we have $g_1 g_2 = g_2 g_1$.

(a) Show that S_n is not abelian for any $n \geq 3$.

For $n = 3$, the elements (12) and (123) do not commute,as

$$(12)(123) = (23), \qquad (123)(12) = (13).$$

These equations hold if we consider the above identities as taking place in S_n for any $n \geq 3$ (i.e., by considering (12), (123), (23), (23) as elements of S_n); hence the two elements do not commute.

(b) Show that any cyclic group is abelian. Conclude that S_n is not cyclic for any $n \geq 3$.

This is tantamount to showing that the map $\mathbb{Z} \to G$ given by $a \mapsto g^a$ is a group homomorphism. We'll show this fact in (excruciating) detail, only because it is so central to everything. If $G = \langle g \rangle$, any element of G is of the form g^a for some $a \in \mathbb{Z}$. By definition of the notation g^a, we have

$$g^a = g \cdot \ldots \cdot g \qquad \text{or} \qquad g^a = g^{-1} \cdot \ldots \cdot g^{-1}$$

depending on the sign of a. (In either the case, there are $|a|$ terms in the product. If $a = 0$, we take $g^a = 1$.) Then we see case by case that

$$g^{a+b} = \begin{cases} g \cdot \cdots \ldots \cdot g \cdot g \cdot \ldots \cdot g, \ (a+b \text{ terms}) & \\ \quad = g^a \cdot g^b & \text{if } a, b \geq 0 \\ g^{-1} \cdot \ldots \cdot g^{-1} \cdot g^{-1} \cdot \ldots \cdot g^{-1}, \ (a+b \text{ terms}) & \\ \quad = g^a \cdot g^b & \text{if } a, b \leq 0 \\ g \cdot \ldots \cdot g, \ (a+b \text{ terms}) & \\ \quad = g \cdot \ldots \cdot g \cdot g^{-1} \cdot \ldots \cdot g^{-1}, \ a \text{ terms, then } |b| \text{ terms} & \\ \quad = g^a \cdot g^b & \text{if } a \geq 0, b \leq 0, \ a+b \geq 0 \\ g \cdot \ldots \cdot g, \ (a+b \text{ terms}) & \\ \quad = g^{-1} \cdot \ldots \cdot g^{-1} \cdot g \cdot \ldots \cdot g, \ |a| \text{ terms, then } b \text{ terms} & \\ \quad = g^a \cdot g^b & \text{if } a \leq 0, b \geq 0, \ a+b \geq 0 \\ g^{-1} \cdot \ldots \cdot g^{-1}, \ (|a+b| \text{ terms}) & \\ \quad = g \cdot \ldots \cdot g \cdot g^{-1} \cdot \ldots \cdot g^{-1}, \ a \text{ terms, then } |b| \text{ terms} & \\ \quad = g^a \cdot g^b & \text{if } a \geq 0, b \leq 0, \ a+b \leq 0 \\ g^{-1} \cdot \ldots \cdot g^{-1}, \ (|a+b| \text{ terms}) & \\ \quad = g^{-1} \cdot \ldots \cdot g^{-1} \cdot g \cdot \ldots \cdot g, \ |a| \text{ terms, then } b \text{ terms} & \\ \quad = g^a \cdot g^b & \text{if } a \leq 0, b \geq 0, \ a+b \leq 0 \end{cases}$$

That is, we have shown that $g^{a+b} = g^a \cdot g^b$. But $a + b = b + a$ in the integers, so this proves $g^b \cdot g^a = g^{b+a} = g^{a+b} = g^a \cdot g^b$. Finally, since S_n is not abelian for $n \geq 3$ (see above), it must not be cyclic.

(c) Show that the center of an abelian group is the whole group.

If a group is abelian, then $gh = hg$ for any pair $g, h \in G$. The center of the group is the subgroup Z consisting of those g such that $gh = hg$ for all $h \in G$. Hence $Z = G$ if G is abelian.

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 $G \times H$.

The identity is $(1_G, 1_H)$, as

$$(1_G, 1_H)(g,h) = (1_G g, 1_H h) = (g,h), \qquad \text{and} \qquad (g,h)(1_G,1_H) = (g1_G, h1_H) = (g,h)$$

for any $(g,h) \in G \times h$. The operation m is associative since G and H have associative operations:

$$\begin{aligned}(g_1,h_1)((g_2,h_2)(g_3,h_3)) &= (g_1,h_1)(g_2g_3,h_2h_3)\\ &= (g_1(g_2g_3), h_1(h_2h_3))\\ &= ((g_1g_2)g_3, (h_1h_2)h_3)\\ &= (g_1g_2, h_1h_2)(g_3,h_3)\\ &= ((g_1,h_1)(g_2,h_2))(g_3,h_3).\end{aligned}$$

Finally, the inverse to (g,h) is given by (g^{-1},h^{-1}), as

$$(g,h)(g^{-1},h^{-1}) = (gg^{-1}, hh^{-1}) = (1_G, 1_H)$$

and

$$(g^{-1},h^{-1})(g,h) = (g^{-1}g, h^{-1}h) = (1_G,1_H).$$

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

$$(g,1)(1,h) = (g1,1h) = (g,h) = (1g,h1) = (1,h)(g,1).$$

(c) Show that if G and H are abelian, then $G \times H$ is abelian (with the above group structure).

$$(g_1,h_1)(g_2,h_2) = (g_1g_2,h_1h_2) = (g_2g_1,h_2h_1) = (g_2,h_2)(g_1,h_1).$$

(d) Show that the maps

$$G \to G \times H \qquad g \mapsto (g,1)$$

and

$$G \times H \to G, \qquad (g, h) \mapsto g$$

are group homomorphisms.

Let $f : G \to G \times H$ be the first map. Then

$$f(g_1 g_2) = (g_1 g_2, 1) = (g_1, 1)(g_2, 1) = f(g_1)f(g_2).$$

Likewise, let $p : G \times H \to G$ be the second map. Then

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

Homework 4

1. Subgroups of $\mathbb{Z}$

In this problem, you will show that every subgroup of $\mathbb{Z}$ is of the form $n\mathbb{Z}$ for some $n \geq 0$.

Let $H \subset \mathbb{Z}$ be a subgroup which contains some non-zero element. Let $n \in H$ be the least, positive integer inside H. Show that $H = n\mathbb{Z}$. (Hint: Remainders.)

Assume there is some $k \in H$ for which k is not divisible by n. By the division algorithm, we know that $k = an + r$ for some integer a and some integer r between 0 and $n - 1$, inclusive. We also conclude $r =\neq 0$ since k is not divisible by n. On the other hand, if both k and n are in H, then $r = k - n - \ldots - n$ is in H. So r is some positive integer less than n, but this contradicts the assumption that n is the least positive integer in H.

2. Conjugation actions

The conjugation action of a group on itself is by far the most important group action in representation theory. A full understanding of the conjugation action can be illusive, and in many contexts, proves quite essential for research.

(a) Fix an element $g \in G$. Define a map $C_g : G \to G$ by $h \mapsto ghg^{-1}$. Show that C_g is a group isomorphism.

If h' is some element in G, let $h = g^{-1}h'g$. Then $C_g(h) = g(g^{-1}h'g)g^{-1} = 1h'1 = h'$. This shows C_g is a surjection. If $C_g(h) = 1$, then $ghg^{-1} = 1$, so we conclude $h = g^{-1}g = 1$. This means the kernel of C_g consists only of 1, meaning C_g is injective. We now need only show that C_g is a group homomorphism:

$$C_g(h_1h_2) = g(h_1h_2)g^{-1} = gh_1g^{-1}gh_2g^{-1} = (gh_1g^{-1})(gh_2g^{-1}) = C_g(h_1)C_g(h_2).$$

Note that I am freely removing and adding parentheses in the products; this is justified by associativity.

(b) Show that $C_g \circ C_{g'} = C_{gg'}$. In other words, the assignment $g \mapsto C_g$ defines a group homomorphism $G \to \mathrm{Aut}_{\mathrm{Group}}(G)$. So this defines *another* group action of G on itself. It is quite different from the action we have considered earlier, where all we had was a group homomorphism $G \to \mathrm{Aut}_{Set}(G)$. This new map, $G \to \mathrm{Aut}_{\mathrm{Group}}(G)$, is called the *conjugation action* of G on itself.

$$C_g \circ C_{g'}(h) = C_g(g'hg'^{-1}) = g(g'hg'^{-1})g^{-1} = (gg')h(g'^{-1}g^{-1}) = (gg')h((gg')^{-1}) = C_{gg'}(h).$$

Note I'm using the property of groups that $(ab)^{-1} = b^{-1}a^{-1}$.

(c) If G is abelian, show that C_g is trivial for all $g \in G$.

Since G is abelian, $ghg^{-1} = hgg^{-1} = h$ for all g, h. Hence $C_g(h) = h$ for all $g, h \in G$. Put another way, C_g is the identity automorphism of G, for any choice g.

3. Group isomorphisms in general

Since C_g is a group isomorphism from G to itself, it tells us a lot about the subgroups and elements of G. This is because of some general properties of group isomorphisms, which we now explore. Let $\phi : G \to H$ be a group isomorphism. If $K \subset G$ is a subset, we define

$$\phi(K) = \{h \in H \text{ such that } h = \phi(g) \text{ for some } g \in K\}.$$

(a) Show that isomorphisms preserve orders of elements. That is, show that if g is an element of order n, then $\phi(g)$ is.

Note that ϕ defines a map $\langle g \rangle$ to H, simply by sending g^n to $\phi(g)^n$. By definition its image is contained in $\langle \phi(g) \rangle$, and any element inside $\langle \phi(g) \rangle$ is of the form $\phi(g)^n$, so this map is a surjection onto $\langle \phi(g) \rangle$. Moreover, ϕ is an isomorphism, so its kernel consists only of 1_G—this means the kernel of $\langle g \rangle \to H$ also consists only of 1_G. This proves that $\langle g \rangle \to H$ is an injective group homomorphism with image isomorphic to $\langle \phi(g) \rangle$. By the first isomorphism theorem, $\langle g \rangle$ and $\langle \phi(g) \rangle$ are isomorphic, hence have equal order. This shows $|g| = |\phi(g)|$.

(b) Show that if $K \subset G$ is a subgroup, it is isomorphic to $\phi(K)$.

ϕ defines a homomorphism from K to G, simply by sending $k \mapsto \phi(k)$. (If you like, this is the composition of the inclusion homomorphism $K \to G$ with the homomorphism $G \to H$.) The kernel of ϕ consists only of the identity, so the map $K \to H$ also has trivial kernel. By the first isomorphism theorem, K is isomorphic to the image of $K \to H$, which by definition is $\phi(K)$. (As an side, note that both (a) and (b) are true simply for injective homomorphisms.)

(c) Show that isomorphisms preserve normal subgroups. That is, Show that if $K \subset G$ is a normal subgroup, then $\phi(K) \subset H$ is normal.

If $K \subset G$ is normal, then for all $g \in G$, we know that $gKg^{-1} \subset K$. So for any g, we have $\phi(g)\phi(K)\phi(g^{-1}) = \{\phi(g)\phi(k)\phi(g)^{-1}, k \in K\} = \{\phi(gkg^{-1}), k \in K\} = \phi(gKg^{-1}) \subset \phi(K)$. (This last inclusion follows because if we have subsets $A \subset B$, the $\phi(A) \subset \phi(B)$ in general.) On the other hand, since any $h \in H$ can be written $\phi(g)$ for some $g \in G$, we see that $h\phi(K)h^{-1} = \phi(g)\phi(K)\phi(g)^{-1}$ for some g, and hence $h\phi(K)h^{-1} \subset \phi(K)$ for all $h \in H$. This proves that $\phi(K)$ is normal. Note that this only required that ϕ be a surjective homomorphism.

(d) Let K be a normal subgroup G. Show that there is a group isomorphism $G/K \cong H/\phi(K)$.

We have a quotient homomorphism $H \to H/\phi(K)$, simply because $\phi(K)$ is normal in H. On the other hand, we have the group isomorphism $\phi : G \to H$. Consider the composition $\psi : G \to H \to H/\phi(K)$. This is a surjection because both ϕ and the quotient map are. So by the first isomorphism theorem, $G/\ker\psi \cong H/\phi(K)$. But the kernel of ψ is the set of all g such that $\phi(g) \in \phi(K)$; since ϕ is an injection, this is the set of all $g \in K$. That is, the kernel is equal to K. By the first isomorphism theorem, $G/K \cong H/\phi(K)$.

Throughout the following exercises, if you have time, think about what the above results imply about elements and subgroups of G that are conjugate.

4. Conjugacy classes of elements

(a) Two elements $g, g' \in G$ are called *conjugate* if there exists some $h \in G$ such that

$$h^{-1}gh = g'.$$

Show by example that if g and g' are conjugate, the choice of h need not be unique.

Any element is conjugate to itself; in particular, we could take $g = g' = 1_G$; then any choice of $h \in G$ satisfies the equation $h^{-1}gh = g'$. For a less trivial example, consider $g = (12), g' = (34)$ inside S_4. Then either of the following choices for h exhibits g' as a conjugate of g:

$$h^{-1} = (1324), \qquad (13)(24).$$

For example,

$$(1324)(12)(4231) = (34), \qquad (13)(24)\left((12)\right)(13)(24) = (34).$$

(b) Show that being conjugate defines an equivalence relation on the set G. That is, show that the relation "$g \sim g'$ if g is conjugate to g'" is an equivalence relation. Under this relation, the equivalence class of g is called the *conjugacy class* of g.

g is conjugate to itself by choosing $h = 1$. If $g' = h^{-1}gh$, then let $k = k^{-1}$. Then we see $g = k^{-1}g'k$; hence the relation is symmetric. Finally, if $g'' = x^{-1}g'x$, then

$$g'' = x^{-1}g'x = x^{-1}h^{-1}ghx = (hx)^{-1}ghx.$$

This establishes transitivity.

(c) Show that g is the only element in its conjugacy class if and only if g is in the center of G.

If g is in the center of G, then for any $h \in G$, we have that $h^{-1}gh = h^{-1}hg = g$. Hence the only element conjugate to g is g itself. Conversely, if g is conjugate only to itself, this means that for every $h \in G$, we have $h^{-1}gh = g$. B multiplying both sides of the equation by h on the left, we see that $gh = hg$. Since this is true for any $h \in G$, this shows g is in the center of G.

5. Conjugacy classes of subgroups

Let H and H' be subgroups of G. We say H and H' are *conjugate* if there is some g such that

$$C_g(H) = H'.$$

That is, if $gHg^{-1} = \{ghg^{-1}, h \in H\} = H'$ for some g.

(a) Show that being conjugate defines an equivalence relation on the set of all subgroups of G. That is, show that the relation "$H \sim H'$ if H is conjugate to H'" is an equivalence relation. The equivalence class of H under this relation is called the *conjugacy class of* H.

Any H is conjugate to itself, since $C_1(H) = \{1h1^{-1}\} = \{h\} = H$. This shows reflexivity. If $C_g(H) = H'$, then we see that $C_{g^{-1}}(H') = H$ as follows:

$$C_{g^{-1}}(H') = \{g^{-1}h'g \text{ s.t. } h' \in H'\} = \{g^{-1}(ghg^{-1})g \text{ s.t. } h \in H\} = H.$$

The middle equality is using, of course, that any $h' \in H'$ is of the form ghg^{-1} for some $h \in H$, and that any element of the form ghg^{-1} is in H'. So we are left to show transitivity: Well, if $C_g(H) = H'$ and $C_x(H') = H''$, then $C_x \circ C_g(H) = H''$. (This is just a statement about what functions C do to subsets.) We are finished.

(b) Show that H is the only element in its conjugacy class if and only if H is normal.

If H is the only element in its conjugacy class, we see that for all $g \in G$, $C_g(H) = gHg^{-1} = H$. This is the definition of being a normal subgroup. Finally, if H is normal, then $gHg^{-1} = H$ for any g, so the only subgroup conjugate to H is H itself.