Math6310 Algebra Homework #1

1. (Lang Exercise I.6, Aluffi Exercise II.4.8) Let G be a group, and let $g \in G$ be an element. Let $\gamma_g : G \to G$ be the function given by $h \mapsto ghg^{-1}$. Show that:

   - γ_g is an automorphism of G;
   - the function $G \to \mathrm{Aut}(G)$ given by $g \mapsto \gamma_g$ is a homomorphism;
   - the image of the homomorphism $G \to \mathrm{Aut}(G)$ is a normal subgroup of $\mathrm{Aut}(G)$.

   (The image is the group $\mathrm{Inn}(G)$ of *inner automorphisms* of G, and the quotient $\mathrm{Out}(G) = \mathrm{Aut}(G)/\,\mathrm{Inn}(G)$ is the *outer automorphism group* of G.)

1. We show that γ_g is a bijective homomorphism, for some fixed $g \in G$. Let $k, \ell \in G$ then we have

   $$\gamma_g(k \cdot \ell) = g \cdot (k \cdot \ell) \cdot g^{-1} = g \cdot k \cdot e \cdot \ell \cdot g^{-1} = (g \cdot k \cdot g^{-1}) \cdot (g \cdot \ell \cdot g^{-1}) = \gamma_g(k) \cdot \gamma_g(\ell),$$

   since group products are associative, and by definition of the identity element. Hence γ_g is a homomorphism for all $g \in G$.

   Now suppose $\gamma_g(h) = e$ for some $h \in G$ we have

   $$\begin{aligned} \gamma_g(h) &= e \\ ghg^{-1} &= e \\ (g^{-1}g)h(g^{-1}g) &= g^{-1}eg \\ h &= g^{-1}eg \\ h &= e. \end{aligned}$$

   Thus, $\gamma_g(h)$ is injective. Now let $k \in G$ and notice that $\gamma_g(g^{-1}kg) = g \cdot g^{-1}kg^{-1}g = k$. Moreover, $g^{-1}kg \in G$ since G is closed under its group operation. That is, γ_g is surjective for all $g \in G$. Hence, we have shown that γ_g is an automorphism of G.

2. Let $g, h \in G$. And let $f : G \to Aut(G)$ be the map $f(g) = \gamma_g$.

Consider the action of γ_{gh} on some group element k. We have

$$\begin{aligned}\gamma_{gh}(k) &= (gh)k(gh)^{-1} \\ &= (gh)k(h^{-1}g^{-1}) \\ &= g(hkh^{-1})g^{-1} \\ &= (\gamma_g \circ \gamma_h)(k),\end{aligned}$$

holds for all $k \in G$. That is, we have shown $f(g \cdot h) = f(g) \circ f(h)$, where $\cdot$ denotes the product in G and $\circ$ denotes function composition — the group operation in $Aut(G)$. Hence, f is a homomorphism.

3. We show directly that im f is closed under conjugation by homomorphism in $Aut(G)$. Let $h \in Aut(G)$ and $\gamma_g \in \text{im } f$. There then exists an inverse homomorphism h^{-1}, consider the action of

$$h \circ \gamma_g \circ h^{-1}.$$

This is an automorphism since the composition of group homomorphisms is again a group homomorphism.

Let $k \in G$ and consider

$$\begin{aligned}(h \circ \gamma_g \circ h^{-1})(k) &= h(g \cdot h^{-1}(k) \cdot g^{-1}) \\ &= h(g) \cdot k \cdot h(g^{-1}), \qquad \text{since } h \text{ is a homomorphism}\end{aligned}$$

Moreover, $h(g) = g' \in G$ since h is an automorphism of G. That is, we have shown $(h \circ \gamma_g \circ g^{-1}) = f(g') \in \text{im } f$. And so, im f is a normal subgroup of $Aut(G)$ by definition.

■

> 2. What is the size of the symmetry group of the cube? Explain how you got your answer.

Imagine that the cube is embedded in $\mathbb{R}^3$ so that the three coordinate axes intersect three faces of the cube. I then claim that the symmetries of the cube are given by R_x, R_y, R_z, rotations about the three coordinate axes by 90°, as well as ℓ_i reflections about planes whose normal vectors are also the three coorindate axes. We have a bunch of relations between these elements. As a presentation then, the symmetry group of the cube is

$$\begin{aligned} \langle R_x, R_y, R_z, \ell_x, \ell_y, \ell_z : \\ (R_i)^4 &= e, \\ (ell_i)^2 &= e \\ [R_x, R_y] &= R_x^{-1} R_z^{-1} \\ [R_y, R_x] &= R_y^{-1} R_z \\ [R_x, R_z] &= R_y R_z \\ [R_z, R_x] &= R_x R_z^{-1} \\ [R_y, R_z] &= R_x^{-1} R_z \\ [R_z, R_y] &= R_y R_z^{-1} \\ \ell_z \ell_x &= R_y^{-2} \\ [\ell_z, \ell_x] &= e, \dots \rangle \end{aligned}$$

From these, one could also certainly simplify the relations to find a more efficient presentation. These commutation relations were found by rotating a book irl, and staring at paper for the reflections. However I will justify a bit more.

I will spend some time justifying why I believe the three rotations and three reflections are necessary for the symmetries of the cube. First, I take "symmetry" to mean transformations of the cube, such that the vertices occupy the eight positions in $\mathbb{R}^3$ given by the coordinates $(\pm 1, \pm 1, \pm 1)$.

Notice that to specify a transformation of the cube it is sufficient to specify where some distinguished vertex goes, along with where two of its three adjacent nodes go (the final adjacent vertex's position is determined by the position of the other two adjacent vertices). They must remain adjacent after the transformation also. This description then makes it clear that then the position of some distinguished vertex can be taken to any other position by some combination of the three rotations. However, we then also need the reflections to allow positions of the other adjacent vertices which could not be acquired through rotations alone.

There are eight positions our distinguished vertex could occupy. For each of those positions, there are 3×2 configurations the other adjacent vertices could occupy. This means there are at most 48 orientations the cube could occupy (and so in principle, our group above should have at most 48 non-trivial elements).

Given how symmetric the cube is and how complicated my description above is. I'm sure there must be a simpler description of the symmetries of the cube. I would be interested in hearing if there's an easier description. I admit, my description above is highly informed by my time in physics and the way they treat the angular momentum operators, and so I'm sure there must be a more elegant description possible =D

$\blacksquare$

> 3. Determine the conjugacy classes in the alternating group A_6. For each conjugacy class, you should give its size and say what its elements are.

We search for the conjugacy classes of S_n whose elements are even permutations. Note that this is a well-defined notion, since if $\sigma, \tau \in S_n$ are even permutations then $\sigma\tau\sigma^{-1}$ has a transposition decomposition whose length is a product of three even numbers, and is thus even.

Recall that the conjugacy classes are exactly given by the type of a permutation and that the number of valid conjugacy classes correspond to the number of partitions of n. And so, we will enumerate the partitions of 6 and then acquire the conjugacy classes of A_6 by choosing the classes which correspond to even partitions. The partitions of 6 are:

$$[\mathbf{1,1,1,1,1,1,1}] \qquad [2,2,2] \qquad [\mathbf{2,2,1,1}] \qquad [2,1,1,1,1] \qquad [\mathbf{3,3}] \qquad [3,2,1],$$
$$[\mathbf{3,1,1,1}] \qquad [\mathbf{4,2}] \qquad [4,1,1] \qquad [\mathbf{5,1}] \qquad [6].$$

The bolded types are those which correspond to even partitions, and so correspond to the conjugacy classes of A_6. Recall that these are the types whose number of entries have the same parity as 6 (i.e. these are the types with an even number of rows). Suppose $\sigma \in S_n$ has type $[a_1, \cdots, a_k]$ then the parity of σ is $(a_1 - 1) + \cdots (a_k - 1)$, since each a_i denotes the length of a cycle which composes σ. Now notice $(a_1 - 1) + \cdots (a_k - 1) = \sum_i a_i - \sum_{i=1}^{k}(-1) = 6 - 2\ell = 6 - 2\ell$ is even. And so indeed the chosen permutations give the conjugacy classes of A_6.

However, we have a bit more counting to do. Recall that a conjugacy $[\sigma] \subseteq S_n$ splits into two conjugacy classes in A_n exactly when the type of σ consists of distinct odd numbers, and otherwise it splits into a single class in A_n. In our case we have $[3,3]$ and $[5,1]$ split into two clases in A_n. Hence, overall we have $1+1+2+1+1+2 = 8$ conjugacy classes in A_6.

Next we determine the sizes of each conjugacy class in A_6. Note that the classes not of type $[3,3]$ and $[5,1]$ have the same size as the corresponding classes in S_n. The classes of type $[3,3]$ and $[5,1]$ split into two classes of equal sizes in A_6. Recall that the class type gives the sizes of the cycles in cycle decomposition of $\sigma \in [\sigma]$. And so, we can determine the size of each class by counting each distinct way of writing a permutation with the given types. For example, $[2,2,1,1]$ corresponds to $\sigma = (a_1, a_2)(b_1 b_2)(c_1)(d_1)$ where $a_i, b_i, c_i, d_i \in [n]$. There are 6! ways to populate these numbers, but then we have equivalent permutations given by cycling the elements in (a_1, a_2) and (b_1, b_2), another equivalence given by interchanging the cycles, and a final equivalence given by interchanging the two trivial cycles. We do not need to consider any equivalence given by interchanging the positions of the 2-cycles and the trivial cycles, since this was included in our enumeration of the partitions of 6, by definition. And so the number of elements in the class of type $[2,2,1,1]$ is given by $\frac{6!=720}{2\cdot 2\cdot 2\cdot 2} = \frac{720}{16}$.

A similar kind of counting gives us the following data. In the following $|[t_i]|$ means the number of elements in the conjugacy class whose type is given by $[t_i]$.

$$|[1,1,1,1,1,1,1]| = 1 \qquad |[2,2,1,1]| = \frac{720}{16} \qquad |[3,3]| = \frac{720}{3\cdot 3\cdot 2}\cdot\frac{1}{2} = \frac{720}{36}$$
$$|[3,1,1,1]| = \frac{720}{3\cdot 3!} = \frac{720}{18} \qquad |[4,2]| = \frac{720}{4\cdot 2} = \frac{720}{8} \qquad |[5,1]| = \frac{720}{5}\cdot\frac{1}{2} = \frac{720}{10}$$

Here the classes with type $[3,3]$ and $[5,1]$ in S_n split into two distinct equal sized classes in A_6 and so we have denoted the size of each split class in the data above. Then we can write the class formuala

$$1 + 45 + 2(20) + 40 + 90 + 2(72) = 360 = |A_6|$$

Showing that we have counted the size of our conjugacy classes correctly.

Lastly, we write the elements of our classes. First consider the classes which do not split in A_6. These classes have the same elements in A_6 as they do in S_6. The type of the class tells us the cycle decomposition of its elements. For example the class whose type is $[2,2,1,1]$ contains even permutations whose cycle decomposition is $\sigma = (a_1, a_2)(b_1, b_2)(c_1)(d_1)$ for $a_i, b_i, c_i, d_i \in [n]$ and distinct. Since permutation type is preserved by conjugation, this argument is well defined for a given conjugacy class. The same reasoning applies to the classes whose type is $[1,1,1,1,1,1]$, $[2,2,1,1]$, $[3,1,1,1]$, or $[4,2]$.

The classes in S_6 whose type is $[3,3]$ or $[5,1]$ split into two distinct equal size classes in A_6. The two split classes must end up containing all the permutations whose type is $[3,3]$ or $[5,1]$ in S_6. Those elements have a similar form to what's argued above.

However, for these split classes, there must be representatives in S_6 which are acquired under conjugation by an odd cycle, hence giving us two classes in A_6. For $[3,3]$ I could argue one class in A_6 contains $\sigma = (1,2,3)(4,5,6)$, and then the other class has a representative given by conjugating σ with some odd permutation, and then all other representatives are given by conjugating those elements with even permutations. But this seems less concrete than I would like.

■

4. Let G be a group and $H \leq G$ a subgroup of index 2. Show that H is a normal subgroup of G.

Recall that a subgroup $H \leq G$ is normal if the set of its left cosets are equal to the set of its right cosets, by definition of normality. That is if $\{gH : g \in G\} = \{Hg : g \in H\}$.

Recall that $[G : H] = 2$ means that H has exactly two left/right cosets[1]. Since $e \in G$, $e \cdot H = H$, and $H \cdot e = H$, it must be that H is one of the left cosets of H and also one of the right cosets of H. Also recall that the left/right cosets of a subgroup partition G as a set. It follows then that the non-H left coset is $G \setminus H$, and the non-H right coset is also $G \setminus H$.

That is, we have shown that the left cosets of H are equal to the right cosets of H and so H must be normal.

Lang proves this using a lot of machinary of the orbits of group actions and the kernel of group actions. That all seems more technical than what I've done here. So I'm a bit worried that I've missed something. ∎

[1] Recall that there's a bijection between the left cosets of a subgroup and the right cosets of a subgroup, and so, this is a well-defined quantity.

5. (Lang Exercise I.15) Let G be a finite group acting transitively on a finite set X, with $\#X \geq 2$. Show that there exists an element $g \in G$ which acts on X without fixed points (i.e. $g \cdot x \neq x$ for all $x \in X$).

Note that the same exercise is given in Aluffi IV.1.18, I will be using the hint given in that version of this problem. The hint gives the following information: (1) The action of G on X is isomorphic to G acting on G/H where $H = \text{Stab}(x)$ for some $x \in X$. Here, G acts on G/H by left multiplication. (2) If $H \lneq G$ for finite G then G is not the union of conjugates of H. If time, come back and prove at least the second one.

First, we show that, since G acts transitively on X, if $x \in X$ then $\text{Stab}(x)$ is conjugate to $\text{Stab}(y)$ for all $y \in X$. Suppose g stabilizes x, that is $gx = x$. Since G acts transitively on X we have $y = \overline{g}x$ for some $\overline{g} \in G$. Consider the following

$$\begin{aligned} gx &= x \\ g(\overline{g}y) &= \overline{g}y \\ (\overline{g}^{-1}g\overline{g}) &= y. \end{aligned}$$

That is, a conjugate of g stabilizes y for each $g \in \text{Stab}(x)$. In other words, $g \cdot \text{Stab}(x) \cdot g^{-1} \subseteq \text{Stab}(y)$ for some $g \in G$. A similar calculation gives the reverse inclusion.

Now suppose that, for contradiction, every $g \in G$ fixes some $x \in X$. Then $G \subseteq \bigcup_{x \in X} \text{Stab}(x)$, and so, $G = \bigcup_{x \in X} \text{Stab}(x)$. Let $H = \text{Stab}(x')$ for some $x' \in X$. Notice that $H \lneq G$ because $|X| \geq 2$ and because G acts transitively on X. If H were not proper then we would have $gx' = x'$ for all $g \in G$, however, we know there exists some $x'' \neq x' \in X$ and then no $g \in G$ satisfies $gx' = x''$, a contradiction. From the preceding paragraph, we can rewrite $\text{Stab}(x) = g_x H g_x^{-1}$ for some $g_x \in G$. Then we have

$$G = \bigcup_{x \in X} \text{Stab}(x) = \bigcup_{x \in X} g_x H g_x^{-1},$$

a contradiction of fact (2) above.

∎

6. (Lang Exercise I.35) Show that there are exactly two non-abelian groups of order 8, up to isomorphism.

Big apologies ∎

7. (Goursat's Lemma, Lang Exercise I.5) Let G_1 and G_2 be groups, and let H be a subgroup of $G_1 \times G_2$ such that the two projections $p_1 : H \to G_1$ and $p_2 : H \to G_2$ are surjective. Let N_1 be the kernel of p_2, and let N_2 be the kernel of p_1. We can view N_1 and N_2 as subgroups of G_1 and G_2.
   - Show that N_1 is normal in G_1 and N_2 is normal in G_2.
   - Prove that the image of H in $(G_1/N_1) \times (G_2/N_2)$ is the graph of an isomorphism $G_1/N_1 \cong G_2/N_2$.

- First, we can view $N_i \leq G_i$ as say $p_1(N_1 = \ker p_2 = \{(x, e_{G_2}) \in H\}) \leq G_1$. This is indeed a subgroup of G_1 becuase if $x, y \in p_1(N_1)$ then this means $(x, e), (y, e) \in N_2$ and so, since H is a subgroup, $(x +_{G_1} y, e) \in N_1$ hence $x +_{G_1} y \in p(N_1)$. And a similar argument holds for inverses and the identity. Put another way, $p_1(N_1) \leq G_1$ since $N_1 \leq H$. The same reasoning shows that we can view $N_2 \leq G_2$.

  Now we show that $N_1 \trianglelefteq G_1$. Let $x \in N_1 \leq G_1$ and let $g \in G_1$. Since $p_1 : H \to G_1$ is surjective there exists $(g, y) \in H$ and $(g, y)^{-1} = (g^{-1}, y^{-1}) \in H$ since H is a subgroup. Lastly $(x, e) \in H$ by definition of $\ker p_2$. Now consider

  $$(g, y) \cdot_{(G_1 \times G_2)} (x, e) \cdot_{(G_1 \times G_2)} (g^{-1}, y^{-1}) = (gxg^{-1}, e) \in H$$

  since H is closed under $\cdot_{G_1 \times G_2}$. But then we have shown $gxg^{-1} \in N_1 \leq G_1$. Thus, N_1 is closed under conjugation and is normal in G_1. A very similar argument holds to show that $N_2 \trianglelefteq G_2$.

- Let $\overline{H}$ be the image of H in $G_1/N_1 \times G_2/N_2$. We want to show that $(\overline{x}, \overline{y}) \in \overline{H}$ associates elements $\overline{x} \in G_1/N_1$ to $\overline{y} \in G_2/N_2$, as a function, in a bijective manner, and as a group homomorphism.

  To be clear, $\overline{H} = \overline{H}_1 \times \overline{H}_2$ where $\overline{H}_i = \text{im}\,(H \twoheadrightarrow^{p_i} G_i \twoheadrightarrow^{\pi_i} G_i/N_i)$. First we show that $\overline{H}$ defines a function. That is, we need to show that there is exactly one element of the form $(\overline{x}, -) \in \overline{H}$ for each $\overline{x} \in G_1/N_1$. Notice that if $(x, y_1), (x, y_2) \in H$ then we have $y_1 - y_2 \in N_2$ and so $\overline{y}_1 = \overline{y}_2 \in G_2/N_2$. That is, any elements of G_2 which are associated with x in H end up in the same class in G_2/N_2. And likewise for any $x' \in G_1$ with $\overline{x'} = \overline{x}$. It then follows that there is at most one element of the form $(\overline{x}, -) \in \overline{H}$ for each $\overline{x} \in G_1/N_1$. Moreover, $H \twoheadrightarrow G_1 \twoheadrightarrow G_1/N_1$ is surjective since it is the composition of surjective maps. It then follows that for all $\overline{x} \in G_1/N_1$ there is some element $(\overline{x}, -) \in \overline{H}$. Thus $\overline{H}$ defines a function $f : G_1/N_1 \to G_2/N_2$.

Next we show that f is bijective. First notice that $H \twoheadrightarrow G_2 \twoheadrightarrow G_2/N_2$ again is surjective. Thus for each $\overline{y} \in G_2/N_2$ we have some $(-, \overline{y}) \in \overline{H}$. That is, f is surjective. Now notice that if $(x_1, y), (x_2, y) \in H$ then we have $x_1 - x_2 \in N_1$. Hence, again, all elements which are associated to y in H end up in the same class in G_1/N_1. And likewise for $x' \in G_1$ which associate to some $y' \in G_2$ such that $\overline{y'} = \overline{y}$. That is, there is at most one element of the form $(-, \overline{y}) \in \overline{H}$. That is, f is injective.

Lastly, f is a group homomorphism because $\overline{H}$ is a subgroup of $G_1/N_1 \times G_2/N_2$; this follows since H is a subgroup of $G_1 \times G_2$. There's some unpacking and deatil checking to do here, but I currently believe this follows from unpacking all the definitions of the objects.

∎