Solutions to Homework Set 2

Eugene Lim, Tevong You, Andres Lopez Moreno

February 14, 2022

Exercise 1. Suppose H is a subset of G. Consider $b \in G$ but $b \notin H$; then does the set of all left cosets $\{bH\}$ form a group? If so, prove it. If not. explain why. Suppose now H is a *normal subgroup* of G, does the left Coset Space form a group? If so, prove it.

Solution: *Consider a subset H which contains the identity. Then the set of left cosets $\{bH\}$ might not have an identity! To exemplify this, let H be the set containing only the identity e. Then $b_1H \cdot b_2H = b_1H \ \forall b_1 \neq e$ (i.e. b_2H is an identity) iff $b_1 \cdot e \cdot b_2 \cdot e = b_1 \cdot e$ $\forall b_1 \neq e$. This implies that $b_1 \cdot b_2 = b_1 \ \forall b_1 \neq e$, which is only true if $b_2 = e$. But by assumption $b_2 \notin H$ so $b_2 \neq e$! Therefore $\{bH\}$ does not have an identity and is thus not a group.*

If H is a normal subgroup, then (in particular) it contains the identity e. It also implies that $gH = Hg \ \forall g \in G$. Therefore $bH \cdot b^{-1}H = Hb \cdot b^{-1}H = HeH = eH$ because H is closed. But $e \in H$ so $eH \notin \{bH\}$ and so $\{bH\}$ is not closed so it is not a group (note that we don't actually need the left-right coset identity to prove this; it only makes things easier. H being any subgroup is already enough for $\{bH\}$ to not be a group).

Exercise 2. Show that there exists a bijection between the left coset space and the right coset space of a normal subgroup $H \leq G$.

Solution: *Let $H \leq G$ be normal. Then $g^{-1} \cdot h \cdot g = h \; \forall g \in G, h \in H$. Suppose $a \in gH$ for some $g \in G$. Then $a = g \cdot h$ for some $h \in H$. But $g \cdot h = g \cdot (g^{-1} \cdot h \cdot g) = (g \cdot g^{-1}) \cdot h \cdot g = h \cdot g$ so $a \in gH \Leftrightarrow a \in Hg$ thus $gH = Hg$. Since we did not specify g, this is true $\forall g \in G$.*

Exercise 3. Suppose G is a group, g is an element of G whose order is n. Show that n divides $|G|$.

Solution: *This is a famous corollary of Lagrange's theorem (a corollary is a statement which follows easily from some other result. It comes from the Latin "corollarium" which means a gift or a gratuity). Consider the subset* $S = \{g^k \mid k \in \mathbb{N}\}$ *. Since* g *has order* n*, we have that* S *has* n *elements and* $g^n = e \in S$*.* S *is obviously closed, and for* $g^j \in S$*, we have an inverse* g^{n-j}*. Thus* S *is a subgroup of* G *with* n *elements and by Lagrange's theorem* $n = |S|$ *divides* $|G|$*.*

Exercise 4. Let X and Y be discrete and finite sets, and Y be a proper subset of X ($Y \subset X$). Consider the following map:

$$j : \text{Perm}(Y) \to \text{Perm}(X); (j(f))(x) = \begin{cases} f(x) \text{ , if } x \in Y \\ x \text{ , otherwise} \end{cases} \tag{1}$$

Show that j is an isomorphism of Perm(Y) into a subgroup of Perm(X)

Solution: *This is just a trivial application of the first isomorphism theorem, but lets solve the exercise without invoking it! The image of j is the set of permutations which keep $X - Y$ constant, and j is injective by construction (if two permutations of Y disagree in some element $y \in Y$ then they will also disagree in $y \in X$). We simply need to show that this image is a group and that j is a homomorphism. Have $S = Im(j)$. Then $e \in S$ because the identity permutation is constant $\forall x \in (X - Y)$. Also, $j(f)^{-1} = j(f_{-1})$ because they are the identity outside Y and inverses inside Y. Finally, $Im(j)$ is clearly closed because PermY is closed and outside Y all elements are the identity. j is a homomorphism because $j(f_1 \cdot f_2) = f_1 \cdot f_2 = j(f_1) \cdot j(f_2)$ in Y and $e \cdot e = e = j(e)$ outside Y (yes, I am abusing the notation of e, but as long as we all know which identities we are talking about we are fine).*

Exercise 5. Consider the quaternion group $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ with the group composition laws

$$-1 = i^2 = j^2 = k^2 = ijk \tag{2}$$

Show that $i = jk = -kj$, $j = ki = -ik$, $k = ij = -ji$. What is the order of this Group? Prove that it is not isomorphic to the Dihedral group D_4. Construct the product group $Z_2 \times V_4$. Is $Q_{82} \times V_4$? If so, prove it; if not, explain.

Solution: *The order of the group is obviously 8 (it has 8 elements). To show that the roots of unity i, j, k anticommute (commute with a negative sign), we notice that $-a = a^{-1}$ $\forall a \in Q_8$ (this can be done by process of elimination) and then manipulate equation 2: $jk = -(-1)jk = -(i^2)jk = -i(ijk) = -i(-1) = i$ and $-kj = -(-ijk)kj = ij(kk)j = ij(-1)j = -ijj = -i(-1) = i$. This process can be repeated by cyclically replacing i, j, k to get the same anticommuting relation for the remaining products. We have been a bit sloppy because I am assuming that (-1) is in the center of Q_8 (i.e. that it commutes with every other element). You can try showing that on your own, or you can arrive to the same result purely through multiplying by inverses and building up a Cayley table.*

To prove that Q_8 is not isomorphic to D_4 it suffices to show that they have different subgroups. Indeed, all non-trivial elements of Q_8 have order 4, but D_4 has order 2 elements. To see if $Q_8 \cong Z_2 \times V_4$ we can notice that the latter is the product of two Abelian groups is therefore Abelian. Since Q_8 anticommutes it is not Abelian and thus they cannot be isomorphic.

Exercise 6. Suppose X and Y are subgroups of the finite group G. Consider the set $XY\{xy|x \in X, y \in Y\}$.
(a) Suppose that $a, b, c, d \in G$ and $ab = cd$. Prove that there is a unique $h \in G$ such that $c = ah$ and $d = h^{-1}b$.
(b) Suppose that $x_1, x_2 \in X$ and $y_1, y_2 \in Y$. Show that $x_1y_1 = x_2y_2$ iff $\exists a \in X \cap Y$ such that $x_2 = x_1a$ and $y_2 = a^{-1}y_1$.
(c) Show that $X \cap Y$ is a subgroup of G. (d) Show that

$$|XY| = \frac{|X||Y|}{|X \cap Y|} \tag{3}$$

(e) Now let $|G| = 256$. Suppose that $|X| = |Y| = 32$. Show that $|X \cap Y| \geq 4$, and that there are at most four possible values of $|X \cap Y|$. You may state any theorems you use in this calculation.

Solution: *(a) We need to prove existence* ***and*** *uniqueness. Existence: let $ab = cd$; then $cdd^{-1} = a(bd^{-1}) = c$ and $(bd^{-1})^{-1}b = db^{-1}b = d$, so bd^{-1} is one such h. Uniqueness: suppose both $h_1, h_2 \in G$ satisfy the assumed condition. Then $c = ah_1 = ah_2$ so $cd = (ah_1)(h_2^{-1}b) = (ah_1)(h_1^{-1}b) = ab$ so $h_1h_2^{-1} = e$ and since inverses are unique $h_1 = h_2$.*

(b) Well, from (a), since all the steps we took are reversible, we have already shown that $ab = cd$ ***iff*** *$h = bd^{-1}$ satisfies $c = ah$ and $d = h^{-1}b$. We only need to show that $h = y_1y_2^{-1}$ is in $X \cap Y$. Since h is the product of elements in Y it is clear that $h \in Y$. But h must also be in X because it is the product of elements in X: $x_2 = x_1h$ so $x_1^{-1}x_2 = eh = h$.*

(c) It is a well-known fact that the intersection of two subgroups is a subgroup, but we need to prove it. First note that $X \cap Y$ is not empty because it contains at least the identity e. To show that it is a subgroup, it remains to show that $\forall a, b \in X \cap Y, ab^{-1} \in X \cap Y$ (if you haven't seen this in lectures, you can check from the group actions that these are indeed the necessary and sufficient conditions for a subset to be a group: it contains the identity and for any two elements, the product of the first with the inverse of the second is also in the subset). Let $a, b \in X \cap Y$. Then $ab^{-1} \in X$ because both $a, b \in X$ and X is a subgroup. By the exact same argument, $ab^{-1} \in Y$ and therefore $ab^{-1} \in X \cap Y$ so $X \cap Y$ is a subgroup of G.

(d) $|X||Y|$ corresponds to the number of possible combinations xy where $x \in Xandy \in Y$ with disregard for group structure. $|XY|$ however, corresponds to the possible combinations xy where $x \in Xandy \in Y$ up to group equivalence! So how many combinations are we missing in $|XY|$? Well, for every two equivalent combinations $x_1y_1 = x_2y_2$ we have exactly one unique element in $X \cap Y$, so basic combinatorics tells us that $|X||Y| = |XY||X \cap Y|$. Rearranging, we get the desired result.

(e) Lagrange's theorem here we go! $256 = 2^8$ *so all subgroups of* G *must have order* 2^n *for* $n \in \{0, 1, 2, 3, 4, 5\}$. *Since* $|X| = 32$ *and by definition of the intersection,* $|X \cap Y| \leq |X|$, $|X \cap Y| \in 2, 4, 8, 16, 32$. *Now,* $|XY| \leq |G|$ *so from equation 3* $|X \cap Y| \geq |X||Y|/|G| = 2^{10}/2^8 = 4$ *and thus the only four possible values are* $4, 8, 16, 32$ *as required.*

Exercise 7. prove that every subgroup of a finite cyclic subgroup Z_n is also a cyclic subgroup.

Solution *Any element $g \in Z_n$ can be written as z^k for some $z \in Z_n$ which generates Z_n. Have S be a subgroup of Z_n. Then if S contains z^i and z^j, it must contain z^p where p is the greatest common divisor of i, j. Thus if $s_0 = z^i$ is the element with the largest order in S and $|S| > |s_0|$ then there must be another element $s_1 = z^j \in S$ which is not a product of s_0. This means that there is some element $s_2 = z^p \in S$ where $p < i$ (because p divides i non-trivially). Then $|z^p| > |z^i| = |z_0|$ which is a contradiction. Thus $|z_0| = |S|$ so $|z_0|$ generates S and S is cyclic.*

Exercise 8. In class, we showed that the set of integers $\mathbb{Z}$ forms a group under the additive operation. Consider the map

$$\tau : \mathbb{Z} \to \mathbb{Z}; \tau(x) = -x \ \forall x \in \mathbb{Z} \tag{4}$$

Show that τ is an isomorphism from the additive group $\mathbb{Z}$ to itself.

Solution: *NB: An isomorphism from an object to itself is called an Automorphism, and the set of automorphisms of* ***any*** *mathematical object is a group under composition of maps!*

Anyways, this map is injective because it sends each element to its inverse and inverses are unique, and surjective because every group element is an inverse of some element in the group. To show it is a homomorphism, have $a, b \in \mathbb{Z}$. *Then* $\tau(a + b) = -(a + b) = -a - b = \tau(a) + \tau(b)$ *as required.*

Exercise 9. Let T be the set of all integer powers of 10, i.e. $T = \{10^z | z \in \mathbb{Z}\}$. Show that T forms a group under the usual multiplicative operation. Show that this group is isomorphic to the additive group of $\mathbb{Z}$, by finding the isomorphism ϕ. Show that the inverse ϕ^{-1} is the logarithm $\log_{10}$.

Solution: *Under real multiplication, T has an identity ($10^0 = 1$) and is closed ($10^a \cdot 10^b = 10^{a+b}$ where $a, b \in \mathbb{Z} \implies (a+b) \in \mathbb{Z}$ from the closure of $\mathbb{Z}$ under addition). the unique inverse of some $10^a \in T$ is 10^{-a} so that $10^{a-a} = 1$ as required. Thus T is a group under integer multiplication.*

Consider the map $\phi : \mathbb{Z} \to T$; $\phi(z) = 10^z$. This map is injective because the exponential map is injective, and surjective by construction because we have defined T to be the image of ϕ. Moreover, it is a group homomorphism because $\forall a, b \in \mathbb{Z}, \phi(a) \cdot \phi(b) = 10^a \cdot 10^b = 10^{a+b} = \phi(a+b)$. Thus ϕ is a group isomorphism and $T, \mathbb{Z}$ are isomorphic.

Since ϕ is bijective, the inverse map ϕ^{-1} such that $\phi^{-1} \circ \phi = Id_{\mathbb{Z} \to T}$ and $\phi \circ \phi^{-1} = Id_{T \to \mathbb{Z}}$. Consider the map $\log_{10} : T \to \mathbb{Z}$; we can see that $\log_{10} \circ \phi(z) = \log_{10}(10^z) = z \ \forall z \in \mathbb{Z}$ and $\phi \circ \log_{10}(10^a) = \phi(a) = 10^a \ \forall 10^a \in T$ as required. Thus $\log_{10}$ is the inverse of ϕ.

Exercise 10. Consider the Tetrahedron. Explain why the symmetry group of the tetrahedron is the symmetric group S_4, i.e. it is the permutation group of 4 objects. Geometrically describe all symmetry operations. Is D_3 a subgroup of S_4? Find the isomorphic map if it is. Explain if it is not.

Solution: *The geometric symmetries of a tetrahedron are the group of transformations of 3-dimensional euclidean space that map the tetrahedron to itself. Since a tetrahedron is uniquely defined by its vertices, this corresponds to the group of transformations which send the set of vertices to itself. I.e. all possible ways of rearranging the set of vertices. Since a tetrahedron has 4 vertices, this group must be the set of permutations of 4 elements* S_4.

There are two types of transformations a tetrahedron is symmetric under: rotations and mirrorings (and the combination of both). Since non-trivial rotations in 3D keep a single line invariant, they may keep at most one vertex in place. Mirrorings, on the other hand, may keep two vertices in place, as their invariant corresponds to a whole plane. (This is all under the assumption that the tetrahedron is centered at the origin and these rotations and mirrorings are by the origin too. Thus out of the 24 elements in S_4*, the identity is just the "null" rotation; the 8 3-cycles (i.e. (123)) are rotations; the 6 transpositions (i.e.(12)) are mirrorings; the 3 double-transpositions (i.e. (12)(34)) are combinations of 2 mirrorings by different planes and the 6 4-cycles (i.e. (1234)) are combinations of a rotation and a mirroring.*

D_3 *is a subgroup of* S_4 *because it corresponds to the rigid transformations of a triangle (i.e. the subset of* S_4 *containing all the transformations which leave some specific vertex fixed). An isomorphism can be constructed as follows: choose an element from the set of 4 elements, for example* $\{4\}$*, then consider the map* $\phi : D_3 \to T_4$ *the subset (subgroup! - you can check this) of* S_4 *which keeps* $\{4\}$ *invariant. Then have* $\phi((abc)) = (abc)(4)$*. You can check that this is indeed a valid isomorphism.*

Exercise 11. Prove the theorem that all prime orer finite groups are cyclic groups.

Solution: *This is another famous corollary of Lagrange's theorem:*

By Lagrange's theorem, prime ordered groups may only have subgroups of order 1 or of the order of the group. The generator of an element is a subgroup, thus every element in a prime ordered group either only generates itself or generates the whole group. The identity element is the unique element in a group which only generates itself (every other element at least generates the identity), thus every non-trivial element must generate the whole group and so the group is cyclic.

Exercise 12. Let H_1, H_2 be *normal* subgroups of G. Prove that the intersection $H_1 \cap H_2$ is also a *normal* subgroup of G. (*Hint:* First prove that the intersection of two subgroups is also a subgroup. Then prove that the normality property gets inherited).

Solution: *We already proved that the intersection of two subgroups in the solutions for Exercise 6 (refer to that proof if you want to reproduce it here). It remains to show that the intersection is normal. There are many alternative (and equivalent) definitions of what a normal subgroup is, and any of them can be used to prove this statement.*

Fancy proof: *(this is fancy because it proves both that the intersection is a group and that it is normal at the same time) A subgroup is normal* ***iff*** *it is a union of conjugacy classes in G. Since distinct conjugacy classes are non-intersecting, $H_1 \cap H_2$ must be either empty or a union of conjugacy classes. We know it is not empty because it contains the identity, therefore it is firstly a group and secondly a normal subgroup.*

Alternate proof: *(this is less powerful because it only proves normality, and you would have to prove that the intersection is a group beforehand) A subgroup is normal* ***iff*** *every of its elements is invariant under conjugation by any element in the group. Let $x \in H_1 \cap H_2$ and have $g \in G$. Then, since in particular $x \in H_1$, $gxg^{-1} = x$ so, assuming $H_1 \cap H_2$ is a subgroup, it is normal.*