Solutions to Homework Set 1

Eugene Lim, Tevong You, Andres Lopez Moreno

February 1, 2022

NOTE: These solutions are written in great detail and you are not expected to reproduce them (a simple few lines usually suffice); this level of detail was written to ease you into the way in which we should approach this type of problem. We will see what kind of syntax is expected from you in the problems classes I will be leading later in the semester, and subsequent solutions will be written with less text and in much more mathematical language.

Exercise 1. Consider the following maps. State which of these maps are surjective, injective, both or none.

- $A = 1, 2, 3, B = l, j, k$, and $f : A \to B; f(1) = l, f(2) = j, f(3) = k$.
- $A = 1, 2, 3, 4, 5, B = 2, 4, 6, 8, 10, 12$, and $f : A \to B; f : x \mapsto 2x, \forall x \in A$.
- $A = \mathbb{R} - 0, B = \mathbb{R} - \{0\}$, and $f : A \to B; f : x \mapsto x + 1/x, \forall x \in A$.

Solution: *The first map is both injective and surjective (we call this kind of map a "bijection"). The second map is injective, but it is not surjective (the map can never output the element "12"). The third map is both surjective and injective, (first of all, make sure it's well-defined! - in this case it is because we are removing zero. A map is not well-defined when the definition either outputs something which is not in the target set, or it breaks down for certain inputs).*

Exercise 2. Let $G = \{-1, 1\}$ be a set. Show that G is a group under the usual rule of multiplication. Is it a group under the usual rule for addition?

Solution: *To show whether something is a group, we must make sure it fulfills all the conditions in the definition of a group: it must have a (unique) identity, it must be closed under the group operation, the operation must be associative, and each element must have a (both left and right) inverse. In this case, we can check that 1 is the identity element:* $1 \cdot 1 = 1$ *and* $1 \cdot (-1) = (-1)$*. We can also see that G is closed: you will never get something other than 1 and -1 when multiplying its elements; it is also clearly associative, as integer multiplication is associative by definition. Finally, we can see that 1 is its own inverse (this is obvious because we have already established that 1 is the identity element), and -1 is its own inverse too:* $(-1) \cdot (-1) = 1 (= e)$*. Thus we have shown that G is a group under integer multiplication. G, however, is* ***not*** *a group under addition. It doesn't have an identity (the additive identity being 0), it's not closed* $(1 + 1 = 2$ *which is not in G)... It does have inverses, so there's that!.*

Exercise 3. Consider the set of complex numbers $\mathbb{C}$. Let it be a Field – describe the action and properties of the two binary operators required.

Solution: *This is a good opportunity to review the field axioms (that means, the requirements given in the definition for something to be a field. In order to* ***prove*** *that $\mathbb{C}$ is a field, it comes in very handy to assume that $\mathbb{R}$ is a field. As you will see later in the course, the complex numbers are an* ***algebra*** *over the real numbers. This means that they are a vector space with real number coordinates which preserves the normal addition and multiplication from the field $\mathbb{R}$. It is also a field in its own right, and we will look at it from very different perspectives depending on whether we consider it a field or a vector space. Allons-y with the proof!:*

$\mathbb{C}$ is a field ***if and only if*** *it is a commutative group under addition and $\mathbb{C} - \{0\}$[1] is a commutative group under multiplication (check that this is indeed equivalent to the definition given in class!) Let's start with addition: it has an identity $e = 0$, it is clearly closed (you can get this by applying the closure of $\mathbb{R}$ under addition on both the real and imaginary component of any element "$a + ib$" of $\mathbb{C}$). Finally, you get inverses in the same way as closure: it is inherited from additive inverses in $\mathbb{R}$ component-wise. Commutativity and associativity are also inherited from addition in $\mathbb{R}$; if you want to make sure, just show that $(a+ib)+(c+id) = (c+db)+(a+ib)$. Associativity, as often is, is obvious. Now for multiplication in $\mathbb{C} - \{0\}$ we can check that the multiplicative identity is $e = 1$ (duh!), and the complex numbers are clearly closed under multiplication (we can get this from the multiplication in the reals. You have to show that for two generic complex numbers "a+ib" and "c+id" their product can be written as "$x + iy$" for some real numbers x and y) and the multiplicative inverses can be easily found in polar form: let $z = re^{i\phi}$ be a complex number (note that this could be* ***any*** *complex number!), then it's inverse is $z^{-1} = 1/re{-}i\phi$. Since we didn't specify any numerical value for z, this is a "proof" of inverses for every element in $\mathbb{C}$. Commutativity can be proven in the same way as for addition.*

[1] This notation means $\mathbb{C}$ proofluding the set $\{0\}$.

Exercise 4. The group of integers $N_n = \{0, 1, 2, 3, \ldots, n-1\}$ is equipped with the composition law given by the usual "addition modulo n". Show that this forms a group. Find the identity. Find the inverses for each element.

Solution: *Here we go again. We have to show that N_n is closed and under it's associative operation, then we have to show there is an identity element, and finally we need to find inverses for all its elements. It is clearly closed because the domain of the binary operation "addition modulo n" is precisely the set $\{0, ..., n-1\}$. For associativity: $[(a+b)\ mod\ n + c\ mod\ n] = [(a+b)+c]\ mod\ n$ (because multiplication of integers is distributive - check the definition of the modulo operation), then the operation must be associative because (the usual) addition of integers is associative. The identity element is 0 (duh!) and the inverses are as follows: for any element $i \in N_n, (i \neq 0)$, $i^{-1} = n - i$. Since 0 is the identity we already know it's is own inverse.*

Exercise 5. Let S be a finite set of complex numbers without 0, i.e. $S \subset \mathbb{C} - \{0\}$. The algebra is specified such that for two elements $z, w \in S$, $zw = wz \in S$. Prove that the modulus of all the elements in S is 1. Show that an identity element in S *may* not exist. We now impose the condition that it must contain an identity. What is the identity? Show that S forms a group. Given that $|S| = n$, prove that it is isomorphic to Z_n by finding the appropriate bijective map.

Solution: *Assuming the operation they have given us is well-defined over S (which we are essentially told in the prompt), we proceed via a* ***proof by contradiction****: Suppose (to later disprove) there was some element s with a modulus different from 1. Then $s^2 = s \cdot s$ must have a modulus* ***different*** *than s, because the modulus of the product is the product of the moduli (for two complex numbers $z_1 and z_2, |z_1 \cdot z_2| = |z_1||z_2|$), and therefore (since they have different moduli) $s \neq s^2$. Similarly, s^3 will have a modulus different from both s and s^2 and thus will be a different number from either; then s^4 will be a new number, same with $s^5, s^5 ...., s^{1354432}, ...$ (etc...). Since we are told that all these products* ***are in S****, and* ***there are infinitely many of them****, we must conclude that S has infinitely many elements. This is not true (we assumed at the very beginning that S was a finite set!), so our only other assumption (that there was a number with modulus different from 1) must be wrong. Thus we have proven that such number does not exist; i.e. all elements of S have a modulus of 1.*

To prove an identity may not exist, we just have to find a counterexample. A good one is the set $S = \{e^{i\pi/4}, e^{i3\pi/4}, e^{-i\pi/4}, e^{-i3\pi/4}\}$. You can check it's a valid S, and that it doesn't contain an identity!

If we impose the condition that an identity does exist, it becomes clear that the identity must be $1 (= 1e^0 = 1 + 0i$, because that is the multiplicative identity in the complex numbers. Under these assumptions, we get closure from the definition, and associativity from exercise 3. We are assuming the identity exists so the only thing remaining is to show that all the elements must contain an inverse. This is simple after noticing the following trick: write some generic element of S as $s = e^{i\phi}$ (remember that the modulus is 1 so no factor precedes the exponential), then the element $s^2 = ss$ must be in S (this comes from our definition of S). Now notice that we can write s^n as $e^{in\phi}$ for any integer n; since S has only finitely many elements, eventually, for some unknown number j, we must have $s^j = s$, because otherwise we would keep generating new numbers forever and the group would not be finite. Now observe that $s^{j-1} \cdot s = s^j = s \cdot s^{j-1}$; this means that $s^{j-1} = 1$!! It then follows that s^{j-2} is the inverse of s because $s^{j-2} \cdot s = s^{j-1} = 1$. This set of groups is what we call the ***roots of unity*** *and, geometrically, they correspond to evenly distributed points along the unit circle in the complex plane containing the point $(1, 0)$. Another way of picturing these groups is as the set of vertices of a regular polygon with n sides, centered at $(0, 0)$ and with one vertex at $(1, 0)$. Finally, an algebraic (rather than geometric) way of interpreting them, is as the zeros of polynomials of the form $p(z) = z^n - 1$ where z is allowed to take values in the complex numbers.*

Finding the bijection to Z_n is easy if you solved the exercise in the same way I did: the bijection is simply $e^{ia\phi} \mapsto a \in Z_n$ (this is also intuitive when looking at S as the vertices of a regular polygon, as this is the same representation we use for the cyclic group Z_n).

Exercise 6. Construct the product group $Z_2 \times Z_4$ by finding all the group elements and the group composition laws. You might find explicitly building a Cayley Table helpful. What is $|Z_2 \times Z_4|$? Is it isomorphic to Z_6? If so, prove it. If not, explain why. Which element has the largest order, and what is the order?

Solution: *The definition of a group product is:* $G_1 \times G_2 = \{(g_1, g_2) \mid g_1 \in G_1, g_2 \in G_2\}$. *Since our groups are* $Z_2 = \{0, 1\}$ *and* $Z_4 = \{0, 1, 2, 3\}$*, our product contain all possible combinations* (a, b) *where* a *can take values* $0, 1$ *and* b *can take values* $0, 1, 2, 3$*. I.e, our new group is* $\{(0,0), (0,1), (0,2), (0,3), (1,0), (1,1), (1,2), (1,3)\}$*. The group operation is component-wise inherited from our parent groups* Z_2 *and* Z_4*, so* $(a, b)(c, d) = (a + b \ mod 2, c + d \ mod 4)$*. Its order is just its number of elements, so* $|Z_2 \times Z_4| = 8$*. Moreover,* $|Z_2 \times Z_4|$ *is* ***not*** *isomorphic to* $|Z_6|$*, because* $|Z_6|$ *only has* 6 *elements and therefore there are no injective maps from* $|Z_2 \times Z_4|$ *to* $|Z_6|$*. The highest order elements are* $(0, 1), (1, 1), (0, 3)$ *and* $(1, 3)$*, which have order* 4*. The identity has order* 1 *and* $(1, 0), (0, 2)$ *and* $(1, 2)$ *have order* 2*.*

Exercise 7. 7. Find all the proper subgroups of the Klein four-group V_4. Which if any is a normal proper subgroup?

Solution: *There are 2 order 4 groups: the cyclic group Z_4 and $Z_2 \times Z_2$. Since V_4 is not the cyclic group, it must be isomorphic to $Z_2 \times Z_2$[2]. Now, if you read the footnote, you already know that the proper subgroups are exactly 3, corresponding to each combination of the identity with one of the remaining 3 elements. Indeed, if we have $V_4 = \{e, a, b, c\}$, the proper subgroups are $\{e, a\}, \{e, b\}$ and $\{e, c\}$. Now, to figure out which subgroups are normal, we go back to the isomorphism with $Z_2 \times Z_2$: this tells us that V_4 must be Abelian (a product of group is Abelian* ***iff*** *every element in the product is Abelian. Since Z_2 is famously Abelian, so is $Z_2 \times Z_2$). Now, in an Abelian group, conjugation is a trivial operation ($aba^{-1} = baa^{-1} = be = b$, $\forall a, b$), so every subgroup is normal! (because* ***everything*** *is invariant under conjugation in an Abelian group). Finally, since we have shown taht V_4 is Abelian, it follows that every subgroup is normal.*

[2]The fact that there are exactly two distinct order 4 groups [up to isomorphism] comes as a consequence of Lagrange's theorem: 2 is the only integer larger than 1 which divides 4, so subgroups of an order 4 group must be of order 2 or 4. If the group has 1 element of order 4, then it's easy to see that it must be the cyclic group with 4 elements. Otherwise all elements must be of order 2, and since there is only 1 group of order 2, these are uniquely defined, giving rise to the only other posibility: the Klein 4-group.

Exercise 8. Let $S = \mathbb{N}$ equipped with the binary operators $\star$ such that $m \star n = \max(m, n)$. State whether (a) $\star$ is associative (b) $\star$ is commutative (c) an identity exist (d) inverses exist.

Solution: *To check if $\star$ is associative we need to show that, for any generic natural numbers a,b and c, $(a \star b) \star c = a \star (b \star c)$. This is true because the operation max is defined via comparisons under the relation $\geq$ which is transitive, therefore $max(a, max(a, b)) = max(a, b, c) = max(a, max(b, c))$.*

To show that it is commutative, we again resort to the definition of $max(a, b)$: if $x \geq y$ is true it returns x, otherwise it returns y. Suppose (without loss of generality) that $a \geq b$; then $max(a, b) = a$ because $a \geq b$ is true, and $max(b, a) = a$ because $b \geq a$ is false. Thus $\star$ is commutative.

It is simple to see that identity is the smallest element of the set $\mathbb{N}$. There is actually a lot of disagreement in mathematics on whether $\mathbb{N}$ is defined as containing the number 0 or not. If we decide to include it, the identity is 0. Otherwise it is 1.

Clearly, inverses cannot exists: if the identity is 1 and I input the number 4 into $max(a, b)$, I will never get anything smaller than 4 as an output, so I will never be able to get the identity (for those not paying attention, $1 < 4$), so 4 has no inverse.

Exercise 9. Let $A = \{1, 2\}$, $B = \{3, 4\}$, $C = \{5, 6\}$. Calculate the following Cartesian products (a) $A \times B \times C$ (b) $A \times B$ (c) $B \times A$ (d) $(A \times B) \times C$ (e) $A \times (B \times C)$. Is $A \times B = B \times A$? Is $(A \times B) \times C = A \times (B \times C)$?

Solution: *This is just an exercise in knowing what the Cartesian product is, so instead of boringly listing a bunch of sets lets talk about the geometric significance of a Cartesian product. First of all, this exercise depends on what we mean by equality. Do we mean equivalence of sets? equivalence up to relabeling?. Unsurprisingly, if you allow for relabeling, all sets with the same number of elements are the same, so lets not assume that. We could also ignore bracket structure (so $((a, b), c) = (a, b, c)$), which would make sense if our sets represent vectors.* ***As far as this exercise is concerned, since both bracket structure and ordering are important, all of these products are different sets****, but it is interesting to see what happens when we assign more importance to things like ordering rather than set structure. We can use geometry to identify how the different sets are related!*

If your sets are discrete, or comparable to the real numbers $\mathbb{R}$, you can think of the Cartesian product as placing your sets along perpendicular axes and looking at the space generated between said axes. If your sets are discrete (i.e have only finitely many elements), you can just take them to be integers along your axis, and you may reorder them however you want!). Therefore we can think of $A \times B \times C$ as the vertices of a unit cube centered at $(1.5, 3.5, 5.5)$. Similarly, we can think of $A \times B$ as a unit square centered at $(1.5, 3.5)$. $A \times B$ a unit square centered at $(3.5, 1.5)$. For sets (d) and (e), the order of applying the Cartesian product essentially distinguishes how the cube is produced: we first create a square and then "lift" it into a cube by adding a 3rd axis, so that our original square becomes one of the faces. Both (d) and (e) lead to the same cube, but the original square corresponds to a different face in the cube (what I'm discussing in this solution is not part of the course, but don't hesitate to come to one of my office hours if you have trouble visualising what I'm talking about!).