

MATH 113 HOMEWORK 3 SOLUTIONS

1. BASIC COMPUTATIONS

Proofs can be omitted in this section. You should still give enough explanation that your classmates could learn the technique from your calculations.

Problem 1.1. Do Judson Ch. 3 Exercises 20 and 24.

Exercise 20: Come ask at office hours if you're stuck on this one; it's best done with a picture.

Solution to Exercise 24: The element $[n] \in \mathbb{Z}/pq\mathbb{Z}$ is a generator if and only if $\gcd(n, pq) = 1$; this is equivalent to saying that $p \nmid n$ and $q \nmid n$. There are pq many integers n such that $1 \leq n \leq pq$, each of which gives a distinct class $[n]$ in $\mathbb{Z}/pq\mathbb{Z}$. Among this list, there are q multiples of p , namely $\{p, 2p, 3p, \dots, qp\}$, and there are p multiples of q , namely $\{q, 2q, \dots, pq\}$. The smallest number which is a multiple of both p and q is pq , since $\gcd(p, q) = 1$, so this is the only number n with $1 \leq n \leq pq$ which is both a multiple of p and q . Hence there are

$$pq - p - q + 1 = (p - 1)(q - 1)$$

numbers n with $1 \leq n \leq pq$ such that $\gcd(n, pq) = 1$, and hence there are $(p - 1)(q - 1)$ many generators of $\mathbb{Z}/pq\mathbb{Z}$.

Problem 1.2. Consider the permutations

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 7 & 4 & 3 & 1 & 5 & 2 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 3 & 4 & 5 & 7 & 6 & 2 \end{pmatrix}$$

in S_7 . Do the following:

- (1) Decompose σ and τ into cycles.
- (2) Compute $\sigma\tau$ and $\tau\sigma$.
- (3) Compute the order of σ , τ , $\sigma\tau$, and $\tau\sigma$.
- (4) Determine the signs of σ , τ , $\sigma\tau$, and $\tau\sigma$.

Solution to (1): We have $\sigma = (165)(27)(34)$ and $\tau = (23457)$.

Solution to (2): We have $\sigma\tau = (16524)$ and $\tau\sigma = (16735)$.

Solution to (3): The order of σ is $\text{lcm}(3, 2, 2) = 6$. The elements τ , $\sigma\tau$, and $\tau\sigma$ are all cycles of length 5, so they all have order 5.

Solution to (4): We have $\text{sgn}(\sigma) = (-1)^{3+1} \cdot (-1)^{2+1} \cdot (-1)^{2+1} = 1$, so σ is even. The elements $\tau, \sigma\tau$, and $\tau\sigma$ are all cycles of odd length, so are all even (i.e. have sign 1).

Problem 1.3. Find all possible cycle structures in S_7 . Explain which of these cycle structures correspond to elements of A_7 . Use this to calculate all possible orders of elements of A_7 .

Solution:

Cycle Type	Sign	In A_7 ?	Order
(7)	1	Yes	7
(1, 6)	-1	No	6
(1, 1, 5)	1	Yes	5
(2, 5)	-1	No	10
(1, 1, 1, 4)	-1	No	4
(1, 2, 4)	1	Yes	4
(3, 4)	-1	No	12
(1, 1, 1, 1, 3)	1	Yes	3
(1, 1, 2, 3)	-1	No	6
(2, 2, 3)	1	Yes	6
(3, 3)	1	Yes	3
(1, 1, 1, 1, 2)	-1	No	2
(1, 1, 2, 2)	1	Yes	2
(2, 2, 2)	-1	No	2
(1, 1, 1, 1, 1, 1)	1	Yes	1

So, A_7 has elements of orders 1, 2, 3, 4, 5, 6, and 7.

Note: Obviously not every divisor of $|A_7| = \frac{7!}{2} = 2^3 \cdot 3^2 \cdot 5 \cdot 7$ appears as the order of an element of A_7 . But notice that every *prime* divisor does! There's a theorem called Cauchy's theorem that says this always happens: if p divides $|G|$ and p is prime, then G has an element of order p . We'll talk about this when we talk about group actions.

Problem 1.4. Do Judson Ch. 5 Exercise 5.

Solution: These are all straightforward computations. Come ask at office hours if you're confused and I'll be more than happy to walk you through these.

2. BASIC PROBLEMS

Problem 2.1. Let G be a group and let $a, b \in G$ be arbitrary. Show that:

- (1) The order of a is equal to the order of $b^{-1}ab$.
- (2) The order of ab is equal to the order of ba .

Solution to (1): We will show this by showing that $o(a) \leq o(b^{-1}ab)$ and vice-versa. Let $n = o(a)$ and let $m = o(b^{-1}ab)$. Now, notice that for $k \in \mathbb{N}$ we have

$$(b^{-1}ab)^k = b^{-1}a^k b.$$

(To prove this rigorously, use induction. The case $k = 1$ is trivial, and to show k implies $k + 1$, we have

$$(b^{-1}ab)^{k+1} = (b^{-1}ab)^k(b^{-1}ab) = b^{-1}a^k b b^{-1}ab = b^{-1}a^{k+1}b,$$

as desired.)

Since $m = o(b^{-1}ab)$, we have

$$e = (b^{-1}ab)^m = b^{-1}a^m b.$$

Multiplying on the left by b and on the right by b^{-1} yields

$$e = beb^{-1} = bb^{-1}a^m bb^{-1} = a^m,$$

hence $o(a) \leq m = o(b^{-1}ab)$.

On the other hand, we also have $e = a^n$ since $n = o(a)$. Multiplying this equation on the left by b^{-1} and on the right by b yields

$$e = b^{-1}eb = b^{-1}a^n b = (b^{-1}ab)^n,$$

hence $o(b^{-1}ab) \leq n = o(a)$, and we are done.

Solution to (2): As in (1), we will show this by showing that $o(ab) \leq o(ba)$ and vice-versa. Let $n = o(ab)$. Then we have

$$e = (ab)^n = a(ba)^{n-1}b.$$

Multiplying on the left by b and on the right by b^{-1} gives

$$e = beb^{-1} = ba(ba)^{n-1}bb^{-1} = ba(ba)^{n-1} = (ba)^n,$$

hence $o(ba) \leq n = o(ab)$. By symmetry of a and b , we also have $o(ab) \leq o(ba)$, and we are done.

Problem 2.2. Let G be a group and let H and K be subgroups of G .

- (1) Show that $H \cap K$ is a subgroup of G . Conclude that $H \cap K$ is also a subgroup of H and a subgroup of K .
- (2) Suppose that H is cyclic of order 15 and K is cyclic of order 16. What is the order of $H \cap K$?

Solution to (1): We will use the “two-part criterion” to show that $H \cap K$ is a subgroup of G . We have that $H \cap K \neq \emptyset$ since $e \in H$ and $e \in K$ as both H and K are subgroups of G ; hence $e \in H \cap K$ also. Now, suppose $g_1, g_2 \in H \cap K$. Then $g_1, g_2 \in H$, so also $g_1 g_2^{-1} \in H$ since H is a subgroup of G . Likewise $g_1 g_2^{-1} \in K$, so $g_1 g_2^{-1} \in H \cap K$. Thus $H \cap K$ is a subgroup of G .

So, this shows that $H \cap K$ is a subset of G which is a group with the same operation as in G . Now, $H \cap K$ is also a subset of H , and

the operation in H is the same as the operation in G , so $H \cap K$ is a subset of H which is a group with the same operation as in H , i.e. $H \cap K$ is a subgroup of H . Likewise $H \cap K$ is a subgroup of K .

Solution to (2): By Lagrange's theorem, since $H \cap K$ is a subgroup of both H and K , we must have that the order of $H \cap K$ divides both $|H|$ and $|K|$. Since H and K are relatively prime, we conclude that $|H \cap K| = 1$. Hence $H \cap K = \{e\}$.

Note: In part (2), "cyclic" is a red herring; we only used that the orders of H and K were relatively prime.

Problem 2.3. Let G be a group.

- (1) Show that if G is abelian, then the set of elements of finite order in G form a subgroup of G . This is called the *torsion subgroup* of G .
- (2) Give an example that shows that if G is not assumed to be abelian, then the set of elements of finite order in G can fail to be a subgroup of G .

Solution to (1): Let H be the set of elements of finite order in G . Then H is non-empty since the identity element e has order 1, so $e \in H$. Now, let $h_1, h_2 \in H$ be arbitrary. Then by definition of H , there exist $n, m \in \mathbb{N}$ such that $h_1^n = e$ and $h_2^m = e$. We want to show that $h_1 h_2^{-1} \in H$. We have

$$\begin{aligned} (h_1 h_2^{-1})^{nm} &= h_1^{nm} h_2^{-nm} \\ &= (h_1^n)^m (h_2^m)^{-n} \\ &= e^m e^{-n} = e. \end{aligned}$$

Hence $h_1 h_2^{-1}$ has finite order, i.e. $h_1 h_2^{-1} \in H$.

Solution to (2): There are many examples. Consider, for example, the group $GL_2(\mathbb{R})$ of 2×2 invertible real matrices. Consider the two elements

$$A = \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

We have $A^2 = I$ and $B^2 = I$, where I is the identity matrix, so A and B both have order 2. But

$$AB = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

has infinite order: direct calculation shows that

$$(AB)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$$

which is not the identity matrix for any $n \in \mathbb{N}$. So A and B have finite order, whereas AB does not; thus the elements of finite order in $GL_2(\mathbb{R})$ cannot possibly form a subgroup.

Problem 2.4. (Judson Ch. 4 Exercise 6) Find all of the subgroups of A_4 . Calculate the order of each subgroup you find. Notice that there is no subgroup of order 6. Explain why you might find this surprising.

Solution: The order of a subgroup of A_4 must divide $|A_4| = 12$, so the possible orders of subgroups are 1, 2, 3, 4, 6, and 12. The only subgroup of order 1 is the trivial subgroup $\{1\}$. Any subgroup of order 2 or 3 must be cyclic; the elements of order 2 in A_4 yield the cyclic subgroups

$$\{1, (12)(34)\}, \quad \{1, (13)(24)\}, \quad \{1, (14)(23)\},$$

and the elements of order 3 yield the cyclic subgroups

$$\{1, (123), (132)\}, \quad \{1, (124), (142)\}, \quad \{1, (134), (143)\}, \quad \{1, (234), (243)\}.$$

Now, a subgroup of order 4 must consist only of elements of order dividing 4, i.e. of elements of order 2 or 4; there are no elements of order 4 in A_4 and there are exactly three elements of order 2, so the only possible subgroup of order 4 is

$$H = \{1, (12)(34), (13)(24), (14)(23)\}.$$

It is easy to check that H is actually a subgroup of A_4 . Note moreover that if K is another subgroup of A_4 and $H \subseteq K$, then by Lagrange's theorem either $H = K$ or $K = A_4$ (since the only natural numbers which are divisible by 4 and divide 12 are 4 and 12).

It remains to look at subgroups of order 6. Suppose that $K \leq A_4$ is a subgroup of order 6. Since there are eight 3-cycles in A_4 , K must contain a 3-cycle. Now, consider two possibilities separately:

- (1) K contains two 3-cycles σ_1 and σ_2 , neither of which is a power of the other, or
- (2) K contains a 3-cycle σ and an element $\rho = (ab)(cd)$ which is a product of two transpositions.

In each case, we will derive a contradiction by showing that K contains H . This is impossible by Lagrange's Theorem, since $|H| = 4$, $|K| = 6$, and 4 does not divide 6.

First consider case (1); since σ_1 is not a power of σ_2 and vice-versa, the three elements permuted by σ_1 cannot be the same three elements as permuted by σ_2 . Since these are both permutations of $\{1, 2, 3, 4\}$, the only possibility is that there are two elements which both σ_1 and σ_2 permute, one element which is permuted by σ_1 but fixed by σ_2 , and one element that is permuted by σ_2 and fixed by σ_1 . Renaming the numbers $\{1, 2, 3, 4\}$, we can assume WLOG that σ_1 permutes $\{1, 2, 3\}$ and σ_2 permutes $\{2, 3, 4\}$. So either $\sigma_1 = (123)$ or (132) , and in the second case, $(123) = (132)^2 \in K$; likewise we deduce that $(234) \in K$. So it remains to show that if K contains (123) and (234) , then K contains H .

We have

$$(123)(234) = (12)(34), \quad (234)(123) = (13)(24),$$

so K contains $(12)(34)$ and $(13)(24)$, hence must also contain

$$(12)(34)(13)(24) = (14)(23).$$

Thus K contains the subgroup H of A_4 . Thus case (1) cannot occur.

Now consider case (2); the 3-cycle σ permutes three of the four elements of $\{1, 2, 3, 4\}$, while ρ consists of two disjoint transpositions of these elements. Hence one of the two transpositions must transpose elements permuted by σ , whereas the other transposition transposes an element permuted by σ with the unique element fixed by σ . Renaming the elements $\{1, 2, 3, 4\}$, we can assume WLOG that σ permutes $\{1, 2, 3\}$ and that $\rho = (12)(34)$. As in part (1), we can in fact assume $\sigma = (123)$. So it remains to show that if K contains (123) and $(12)(34)$, then K contains H .

We have $(12)(34)(123) = (243)$, so K contains (243) and hence also contains $(243)^2 = (234)$. But our computation in part (1) showed that if K contains (123) and (234) , then K contains all of H . Thus case (2) also does not occur, so A_4 has no subgroup of order 6.

Finally, the subgroup of order 12 is of course all of A_4 , and we are done.

Note: In class we will use quotient groups to give a nicer proof of the fact that A_4 contains no subgroup of order 6.

Problem 2.5. (Judson Ch. 4 Exercise 18) Show that A_n is nonabelian for $n \geq 4$.

Solution: For $n \geq 4$, A_n contains the 3-cycles (123) and (234) . We have

$$(123)(234) = (12)(34) \neq (13)(24) = (234)(123),$$

so A_n is not abelian.

Problem 2.6. (Judson Ch. 4 Exercise 26) Show that any permutation in S_n can be written as a product of the transpositions $(12), (13), \dots, (1n)$. Show likewise that it can be written as a product of the transpositions $(12), (23), \dots, ((n-1) n)$. Finally, show that it can be written as a product of the two permutations (12) and $(12 \dots n)$.

Solution to First Part: Since any permutation in S_n can be written as a product of transpositions, it suffices to show that every transposition can be written as a product of the transpositions $(12), (13), \dots, (1n)$.

Let $(ab) \in S_n$ be an arbitrary transposition. If $a = 1$ or $b = 1$ then (ab) already appears in the list $(12), (13), \dots, (1n)$. Otherwise,

$$(ab) = (1a)(1b)(1a),$$

by direct calculation, as desired.

Solution to Second Part: By the first part, it suffices to show that every transposition of the form $(1k)$ can be written as a product of the transpositions $(12), (23), \dots, ((n-1)n)$. I claim that

$$(1k) = ((k-1)k) \cdots (23)(12)(23) \cdots ((k-1)k).$$

Prove this by induction; the statement is obvious for $k = 2$. Suppose that it is true for k . Then we have

$$\begin{aligned} (1(k+1)) &= (k(k+1))(1k)(k(k+1)) \\ &= (k(k+1))((k-1)k) \cdots (23)(12)(23) \cdots ((k-1)k)(k(k+1)), \end{aligned}$$

as desired.

Solution to Third Part: By the second part, it suffices to show that every transposition of the form $(k(k+1))$ can be written as a product of (12) and $(12 \dots n)$. Note first that $(12 \dots n)^{-1} = (12 \dots n)^{n-1}$, so it is enough to show that every transposition of the form $(k(k+1))$ can be written as a product of (12) , $(12 \dots n)$, and $(12 \dots n)^{-1}$. Now, I claim that

$$(12 \dots n)^{k-1}(12)(12 \dots n)^{-(k-1)} = (k(k+1))$$

for all $k \in \{1, \dots, n-1\}$. Let's check this directly; let σ be the left-hand side of this expression. Given $\ell \in \{1, \dots, n\}$, we have that $\sigma(\ell)$ is

$$(12 \dots n)^{k-1}(12)(12 \dots n)^{-(k-1)}(\ell) \equiv (12 \dots n)^{k-1}(12)(\ell - k + 1).$$

(Of course, this is only really true mod n , but being careful we'll see that everything works out). Applying (12) to $\ell - k + 1$ yields $\ell - k + 1$ unless $\ell - k + 1 = 1$ or 2 , i.e. unless $\ell = k$ or $k + 1$. So, if ℓ is not k or $k + 1$, we get

$$(12 \dots n)^{k-1}(12)(\ell - k + 1) = (12 \dots n)^{k-1}(\ell - k + 1) = \ell,$$

so $\sigma(\ell) = \ell = (k(k+1))(\ell)$. On the other hand, we calculate:

$$\sigma(k) = (12 \dots n)^{k-1}(12)(1) = k + 1 = (k(k+1))(k)$$

and

$$\sigma(k+1) = (12 \dots n)^{k-1}(12)(2) = k = (k(k+1))(k+1),$$

so $\sigma = (k(k+1))$ as desired.

3. CREATIVE PROBLEMS

Problem 3.1. (Other groups of symmetries) We've now seen groups of "symmetries of a set" (the symmetric group S_n), "symmetries of the n -gon" (the dihedral group D_n), and a few other groups of symmetries (for example, the symmetries of a rectangle don't fall into either class above). Now consider the following:

- (1) The "group of symmetries of the integers": Let G be the set of functions $f : \mathbb{R} \rightarrow \mathbb{R}$ of the form $f(x) = ax + b$, where $a, b \in \mathbb{R}$, such that f induces a bijection from \mathbb{Z} to \mathbb{Z} (for example, $f(x) = x + 1$ is such a function, but $f(x) = 2x + 1$ is not). Describe all possible a and b . Show that G is a group under composition. Try to find as many interesting properties of G as you can.
- (2) Now come up with TWO other interesting examples of "groups arising from symmetries"; you might look at symmetries of your favorite shape, or symmetries of the tile pattern on your bathroom wall. Try to say as much as you can about the groups you discover.

Solution to first part of (1): Let $f(x) = ax + b$. Since we want f to give a bijection from \mathbb{Z} to \mathbb{Z} , there must in particular be some integer solution to the equation $ax + b = b + 1$, which reduces to $ax = 1$. The only integers a for which this has a solution are $a = \pm 1$. I claim that for $a = \pm 1$ and $b \in \mathbb{Z}$ arbitrary, $f(x) = ax + b$ induces a bijection from \mathbb{Z} to \mathbb{Z} .

For injectivity, notice that $a^2 = 1$. Suppose that $f(c) = f(d)$. Then $ac + b = ad + b$, hence $ac = ad$. Multiplying by a yields $c = a^2c = a^2d = d$, so f is injective.

For surjectivity, let $c \in \mathbb{Z}$ be arbitrary. Then $f(a(c - b)) = a^2(c - b) + b = c - b + b = c$. Hence f is surjective.

Checking that G is a group is now easy; I leave this to you.

Solution to second part of (1): I'm sure there are a bunch of neat things to observe about this group. Here's my favorite: consider the elements f and g defined by $f(x) = -x$ and $g(x) = -x + 1$. Then $f^2 = f \circ f = \text{id}$ and likewise, since $g^2(x) = g(g(x)) = g(-x + 1) = -(-x + 1) + 1 = x$, we have $g^2 = \text{id}$. But now notice that

$$g \circ f(x) = g(-x) = x + 1.$$

Let $h = g \circ f$, and let k be an arbitrary element of G ; write $k(x) = ax + b$ where $a = \pm 1$ and $b \in \mathbb{Z}$. If $a = 1$ then $k = h^b$, whereas if $a = -1$ then $k = h^b \circ g$. So, we have that every element of G is a product of the elements f and g ; hence G is a group of infinite order, but every element of G is a product of the two elements f and g , each of which has order 2.

Problem 3.2. Let G be a group, let g be an element of G , and let H be a subgroup of G . Do the following:

- (1) Show that $gH = Hg$ if and only if $gHg^{-1} = H$; here $gHg^{-1} = \{ghg^{-1} \mid h \in H\}$.
- (2) Part (1) shows that multiplying subgroups of G by elements of G “behaves like multiplying elements of G ” in some sense. Try to find other examples of this. Try to find cases where this fails (for example, what happens if you replace g here by another subgroup K of G ?). See how general of a statement you can prove.

Solution to (1): Suppose that $gH = Hg$. We want to show that $gHg^{-1} = H$:

$(gHg^{-1} \subseteq H)$: Let $h \in H$ be arbitrary. Then we have that $gh \in gH = Hg$, so there is another element $h' \in H$ such that $gh = h'g$. Hence

$$ghg^{-1} = h' \in H,$$

so $gHg^{-1} \subseteq H$.

$(H \subseteq gHg^{-1})$: Let $h \in H$ be arbitrary. Then we have that $hg \in Hg = gH$, so there is another element $h' \in H$ such that $hg = gh'$. Hence

$$h = gh'g^{-1} \in gHg^{-1},$$

so $H \subseteq gHg^{-1}$, as desired.

Now, suppose on the other hand that $gHg^{-1} = H$. We want to show that $gH = Hg$:

$(gH \subseteq Hg)$: Let $h \in H$ be arbitrary. Let $h' = ghg^{-1}$; by our assumption, $h' \in H$. Multiplying on the right by g , we get

$$gh = h'g \in Hg,$$

hence $gH \subseteq Hg$.

$(Hg \subseteq gH)$: Let $h \in H$ be arbitrary. By our assumption, $h = gh'g^{-1}$ for some $h' \in H$. Multiplying on the right by g , we have that

$$hg = gh' \in gH,$$

hence $Hg \subseteq gH$, as desired.