Homework 3 Solutions

Enrique Treviño

February 13, 2016

1 Chapter 4

Problem 1. (Exercise 1)
Prove or disprove each of the following statements.

(a) \( \mathbb{Z}_8 \) is cyclic.

(b) All of the generators of \( \mathbb{Z}_{60} \) are prime.

(c) \( \mathbb{Q} \) is cyclic.

(d) If every proper subgroup of a group \( G \) is cyclic, then \( G \) is a cyclic group.

(e) A group with a finite number of subgroups is finite.

Solution 1.

(a) To turn in.

(b) To turn in.

(c) Suppose that \( \mathbb{Q} \) is cyclic. Suppose that it has \( a \) as its generator. Since \( a \in \mathbb{Q} \), then there exist \( p \) and \( q \) relatively prime integers such that \( a = \frac{p}{q} \). Since \( a \) is a generator, then any rational number \( x \) can be written in the form \( ka \) for some integer \( k \). Therefore \( x = kp/q \). Therefore \( qx \) is an integer, for any rational number \( x \). The rational number \( r = \frac{1}{q+1} \) doesn’t satisfy that \( qr \in \mathbb{Z} \). This contradicts our assumption that \( \mathbb{Q} \) is cyclic, so it is not cyclic.

(d) To turn in.

(e) True. This one is hard to prove. Let \( G \) be a group with finitely many subgroups. Then in particular, there are finitely many cyclic subgroups of the form \( < g > \). Now define the following equivalence relation on the set \( G \): \( g \sim h \) if \( < g > = < h > \). The set of equivalence classes partitions \( G \). Since each equivalence class creates a subgroup of \( G \) and \( G \) has finitely many subgroups, the set of equivalence classes is finite. For the sake of contradiction assume that \( G \) is infinite. Then, by the Pigeonhole principle, at least one of the equivalence classes has infinitely many elements. Suppose the equivalence class with infinitely many elements is \( [g] \). Let \( g, h \in [g] \) such that \( g \neq h \), and \( h \neq g^{-1} \). Since \( < g > = < h > \), then there exist \( k, j \in \mathbb{Z} \) such that \( g = h^k \) and \( h = g^j \). Therefore \( g = h^k = (g^j)^k = g^{jk} \). Therefore \( g^{jk-1} = e \) (the identity). Now, note that since \( g \) and \( h \) are not the identity, inverses of each other or equal to each other, then \( jk \neq 1 \), so \( jk - 1 \neq 0 \). So then \( | < g > | \leq |jk - 1| \). But if \( r \in [g] \), then \( r \in < g > \) because \( < r > = < g > \) implies \( r \in < g > \). Since \( [g] \) is infinite, \( < g > \) should have infinitely many elements, yet \( < g > \) has finitely many. This contradicts our assumption that \( G \) is infinite, proving that \( G \) is finite.

Problem 2. (Exercise 2)
Find the order of each of the following elements.

(a) \( 5 \in \mathbb{Z}_{12} \)
(b) $\sqrt{3} \in \mathbb{R}$
(c) $\sqrt{3} \in \mathbb{R}^*$
(d) $-i \in \mathbb{C}^*$
(e) $72 \in \mathbb{Z}_{240}$.
(f) $312 \in \mathbb{Z}_{471}$.

Solution 2.
(a) To turn in.
(b) To turn in.
(c) To turn in.
(d) $<-i> = \{1, -i, -1, i\}$, so $|<-i>| = 4$.
(e) To turn in.
(f) The gcd of 312 and 471 is 3. Therefore $3 \in (312)$, so the order of 312 is $471/3 = 157$.

Problem 3. (Exercise 3)
List all of the elements in each of the following subgroups.
(a) The subgroup of $\mathbb{Z}$ generated by 7
(b) The subgroup of $\mathbb{Z}_{24}$ generated by 15
(h) The subgroup generated by 5 in $\mathbb{Z}_{18}^*$

Solution 3. To turn in.

Problem 4. (Exercise 6)
Find the order of every element in the symmetry group of the square, $D_4$.

Solution 4. To turn in.

Problem 5. (Exercise 11)
If $a^{24} = e$ in a group $G$, what are the possible orders of $a$?

Solution 5. Consider the subgroup $<a>$. Suppose the order of $<a>$ is $n$. Then $a^k = e$ if and only if $n \mid k$. Therefore $n \mid 24$. So the possibilities for the order of $a$ are: 1, 2, 3, 4, 6, 8, 12, 24.

Problem 6. (Exercise 23)
Let $a, b \in G$. Prove the following statements.
(a) The order of $a$ is the same as the order of $a^{-1}$.
(b) For all $g \in G$, $|a| = |g^{-1}ag|$.
(c) The order of $ab$ is the same as the order of $ba$.

Solution 6.
(a) To turn in.
Suppose \( |a| = n \) and \( |g^{-1}ag| = m \). Then \( a^n = e \). But

\[
(g^{-1}ag)^n = g^{-1}a^n g = g^{-1}eg = e,
\]

so \( m \mid n \). Similarly \( (g^{-1}ag)^m = e \). But then \( g^{-1}a^m g = e \). So then \( a^m = gg^{-1} = e \). Therefore \( n \mid m \).

Therefore \( |a| = |g^{-1}ag| \).

So the statement is easy to prove when \( G \) is finite. What about when \( G \) is infinite? When \( G \) is infinite but \( <a> \) and \( <g^{-1}ag> \) are finite, one can follow the same proof as above. If \( <a> \) is finite, then \( <g^{-1}ag> \) is also finite because whenever \( a^k = e \), then \( (g^{-1}ag)^k = e \) (as shown above). Similarly, if \( <g^{-1}ag> \) is finite \( <a> \) is also finite. Therefore we’re only left with the problem of what happens when both \( <a> \) and \( <g^{-1}ag> \) are infinite.

To prove that \( a \) has the same order as \( g^{-1}ag \) we need to show that there is a bijection from \( <a> \) to \( <g^{-1}ag> \). Let \( f: <a> \rightarrow <g^{-1}ag> \) be defined by \( f(x) = g^{-1}xg \). Let’s show that \( f \) is a bijection. First we must show that the image of \( f \) is indeed contained in \( <g^{-1}ag> \). Let \( h \in <a> \). Then there exists a \( k \in \mathbb{Z} \) such that \( a^k = h \). Now, \( (g^{-1}ag)^k = g^{-1}a^k g = f(h) \). Therefore \( f(h) \in <g^{-1}ag> \). So \( f \) is indeed a function from \( <a> \) to \( <g^{-1}ag> \).

Now we need to show \( f \) is one-to-one and onto. Suppose \( f(h_1) = f(h_2) \). Then there exist integers \( k_1 \) and \( k_2 \) such that \( f(h_1) = g^{-1}a^{k_1}g \) and \( f(h_2) = g^{-1}a^{k_2}g \). Therefore \( g^{-1}a^{k_1}g = g^{-1}a^{k_2}g \). So \( a^{k_1-k_2} = e \). Since \( <a> \) is infinite, then \( k_1 = k_2 \). Therefore \( f \) is one-to-one.

Now let’s prove that \( f \) is onto. Let \( h \in <g^{-1}ag> \). Then \( h = (g^{-1}ag)^k \) for some \( k \in \mathbb{Z} \). Therefore \( h = g^{-1}a^k g = f(a^k) \). Since \( a^k \in <a> \) and \( f(a^k) = h \), then \( f \) is onto.

Since \( f \) is a bijection, the order of \( <a> \) is equal to the order of \( <g^{-1}ag> \).

**Alternative Solution:** The proof above is not the easiest when \( <a> \) and \( <g^{-1}ag> \) are both infinite. So let’s give another proof for this case: If \( <a> \) is infinite, \( |a| = |\mathbb{N}| \) because \( <a> = \{a^k : k \in \mathbb{Z}\} \) has at most \( \mathbb{Z} \) elements and \( |\mathbb{Z}| = |\mathbb{N}| \). Similarly \( |<g^{-1}ag>| = |\mathbb{N}| \). So the orders are the same.

(c) To turn in.

**Problem 7.** (Exercise 26)
Prove that \( \mathbb{Z}_p \) has no nontrivial proper subgroups if \( p \) is prime.

**Solution 7.** \( \mathbb{Z}_p = \langle 1 \rangle \). Suppose \( H \) is a nontrivial subgroup of \( \mathbb{Z}_p \). Since \( \mathbb{Z}_p \) is cyclic, \( H \) must be cyclic. Suppose \( H = \langle b \rangle \). But \( b = b \cdot 1 \). Therefore the order of \( b \) is \( p \). \( p = \gcd(b,p) = p \). But then \( H = \mathbb{Z}_p \). So the only subgroups of \( \mathbb{Z}_p \) are \( \{0\} \) and \( \mathbb{Z}_p \).

**Problem 8.** (Exercise 31)
Let \( G \) be an abelian group. Show that the elements of finite order in \( G \) form a subgroup. This subgroup is called the **torsion subgroup** of \( G \).

**Solution 8.** To turn in.