Math 212, Assignment 3

Solutions

All questions are equally weighted. They will be marked for correctness and clarity of explanation.

1. Let
$$H = \{(a, b, c) : a, b, c \in \mathbb{Z}, a + b + c = 0\}.$$
Prove that H is a subgroup of $\mathbb{Z}^3$.

Solution. We will use the two-step test.

As $0 + 0 + 0 = 0$, we see that $(0, 0, 0)$ is in H.

Now suppose that (a, b, c) and (d, e, f) are in H. This means that $a+b+c = 0$ and $d + e + f = 0$. Then we have $-(a, b, c) + (d, e, f) = (-a + d, -b + e, -c + f)$ (using additive notation in stead of $a^{-1}b$). Now if we want to see this is in H, we must add the entries and see we get 0:

$$(-a + d) + (-b + e) + (-c + f) = -(a + b + c) + (d + e + f) = -0 + 0 = 0$$

and so this element is in H.

2. Exercise 3.7.16, Part 1.

Solution. We use Theorem 3.7.5. First, since the identity ε of G has order 1, clearly ε is in $Tor(G)$. To see that $Tor(G)$ is closed under the operation of G, let a and b be two elements of $Tor(G)$; let $o(a) = k$ and $o(b) = \ell$. Since G is abelian,

$$(ab)^{k\ell} = a^{k\ell}b^{k\ell} = (a^k)^\ell(b^\ell)^k = \varepsilon^\ell\varepsilon^k = \varepsilon.$$

Therefore the order of ab is at most $k\ell$, which is finite because k and ℓ are finite. Finally, to see that a^{-1} is in $Tor(G)$, note that

$$(a^{-1})^k = (a^k)^{-1} = \varepsilon^{-1} = \varepsilon,$$

so the order of a^{-1} is at most k (in fact with a little more work we could show that it equals k), so it is finite.

Therefore by Theorem 3.7.5, $Tor(G)$ is a subgroup of G.

3. Let G be a group and let H_1 and H_2 be subgroups of G.

   (a) Prove that $H_1 \cap H_2$ is a subgroup of G.

   (b) Suppose that G is finite and H_1 and H_2 have orders p and q, respectively, where p and q are distinct primes. Prove that $H_1 \cap H_2 = \{e\}$.

   Solution.

   (a) To see that $H_1 \cap H_2$ is a subgroup, we will use Theorem 3.7.6. Since H_1 and H_2 both contain the identity element e of G, we have $e \in H_1 \cap H_2$, so $H_1 \cap H_2$ is nonempty. Now suppose g and h are both in $H_1 \cap H_2$. Then g and h are both in H_1, and since H_1 is a group, $g^{-1}h$ is in H_1. Similarly, g and h are in H_2, so $g^{-1}h$ is in H_2. Therefore $g^{-1}h$ is in $H_1 \cap H_2$. Then by Theorem 3.7.6, $H_1 \cap H_2$ is a subgroup of G.

   (b) We know $H_1 \cap H_2$ is a group, since it is a subgroup of G. Then, since it is a subset of both H_1 and H_2, it is a subgroup of both of these groups. By a corollary of Lagrange's Theorem, the order of $H_1 \cap H_2$ is a divisor of both p and q. But p and q are distinct primes, so their only common divisor is 1. It follows that $H_1 \cap H_2$ has order 1, and consequently $H_1 \cap H_2$ is the trivial subgroup $\{e\}$.

4. Exercise 3.8.10

   Solution. Let $S_1 = \left\{ \begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix} : a \in \mathbb{R}, a \neq 0 \right\}$ and $S_2 = \left\{ \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} : b \in \mathbb{R}, b \neq 0 \right\}$.

   We will use Theorem 3.7.5 to show that S_1 and S_2 are subgroups of the $ax + b$ group. First, note that S_1 and S_2 are both subsets of the $ax + b$ group, and clearly the identity matrix $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is in both sets.

   To see that S_1 is closed under matrix multiplication, let $A = \begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix}$ and $C = \begin{bmatrix} c & 0 \\ 0 & 1 \end{bmatrix}$ be in S_1, so $a, c \in \mathbb{R}$ and $a, c \neq 0$. Then $AC = \begin{bmatrix} ac & 0 \\ 0 & 1 \end{bmatrix}$. Since $a, c \in \mathbb{R}$, $ac \in \mathbb{R}$, and since $a, c \neq 0$, $ac \neq 0$. Therefore $AC \in S_1$. The

inverse of A is $\begin{bmatrix} \frac{1}{a} & 0 \\ 0 & 1 \end{bmatrix}$. Since $a \in \mathbb{R} - \{0\}$, we have $\frac{1}{a} \in \mathbb{R} - \{0\}$, so A^{-1} is in S_1. We have shown that S_1 is a subgroup of the $ax + b$ group.

To see that the set S_2 is closed under matrix multiplication, let $B = \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}$ and $D = \begin{bmatrix} 1 & d \\ 0 & 1 \end{bmatrix}$ be elements of S_2. Then $BD = \begin{bmatrix} 1 & b+d \\ 0 & 1 \end{bmatrix}$. Since $b, d \in \mathbb{R}$, $b + d \in \mathbb{R}$, so BD is in S_2. Now, to see that S_2 is closed under taking inverses, note that the inverse of B is the matrix $\begin{bmatrix} 1 & -b \\ 0 & 1 \end{bmatrix}$, where $-b$ is in $\mathbb{R}$ because b is in $\mathbb{R}$. Therefore B^{-1} is in S_2.

Therefore by Theorem 3.7.5, both S_1 and S_2 are subgroups of the $ax + b$ group.

For the second part of the question, we will show that every element of the $ax + b$ group is a product of an element of S_1 and an element of S_2.

Let $M = \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}$, so $a, b \in \mathbb{R}$ and $a \neq 0$. Then $M = AB$, where $A = \begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix}$ is in S_1 and $B = \begin{bmatrix} 1 & \frac{b}{a} \\ 0 & 1 \end{bmatrix}$ is in S_2.

The subgroups S_1 and S_2 are both abelian, while the $ax + b$ group is not.

5. Let θ be a real number and consider

$$A = \begin{bmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{bmatrix}$$

(a) Verify that A is in $O_2(\mathbb{R})$.

(b) Using induction, prove that

$$A^n = \begin{bmatrix} \cos(n\theta) & \sin(n\theta) \\ -\sin(n\theta) & \cos(n\theta) \end{bmatrix}$$

for all $n = 1, 2, 3, \ldots$.

(c) For which values of θ does A have finite order in $O_2(\mathbb{R})$?

Solution.

(a) We verify that A is in $O_2(\mathbb{R})$ by checking conditions 1 and 3 of Theorem 3.8.7.

First we compute:

$$\begin{aligned} A^TA &= \begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix} \begin{bmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{bmatrix} \\ &= \begin{bmatrix} \cos^2(\theta)+\sin^2(\theta) & \cos(\theta)\sin(\theta)-\cos(\theta)\sin(\theta) \\ \cos(\theta)\sin(\theta)-\cos(\theta)\sin(\theta) & \cos^2(\theta)+\sin^2(\theta) \end{bmatrix} \\ &= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \end{aligned}$$

The calculation for AA^T is similar.
We take the dot product of the first and second rows:

$$(\cos(\theta),\sin(\theta))\cdot(-\sin(\theta),\cos(\theta)) = -\cos(\theta)\sin(\theta)+\cos(\theta)\sin(\theta) = 0.$$

We do the first row with itself:

$$(\cos(\theta),\sin(\theta))\cdot(\cos(\theta),\sin(\theta)) = \cos^2(\theta)+\sin^2(\theta) = 1,$$

and finally the second row with itself

$$(-\sin(\theta),\cos(\theta))\cdot(-\sin(\theta),\cos(\theta)) = \sin^2(\theta)+\cos^2(\theta) = 1.$$

(b) Using induction, prove that

$$A^n = \begin{bmatrix} \cos(n\theta) & \sin(n\theta) \\ -\sin(n\theta) & \cos(n\theta) \end{bmatrix}$$

for all $n = 1, 2, 3, \ldots$.

The statement is obviously true when $n = 1$. Now assume it is true for some $n \geq 1$ and we will show it for $n+1$:

$$\begin{aligned} A^{n+1} &= A^nA \\ &= \begin{bmatrix} \cos(n\theta) & \sin(n\theta) \\ -\sin(n\theta) & \cos(n\theta) \end{bmatrix} \begin{bmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{bmatrix} \\ &= \begin{bmatrix} \cos(n\theta)\cos(\theta)+\sin(n\theta)(-\sin(\theta)) & \cos(n\theta)\sin(\theta)+\sin(n\theta)\cos(\theta) \\ -\sin(n\theta)\cos(\theta)+\cos(n\theta)(-\sin(\theta)) & -\sin(n\theta)\sin(\theta)+\cos(n\theta)\cos(\theta) \end{bmatrix} \\ &= \begin{bmatrix} \cos(n\theta+\theta) & \sin(n\theta+\theta) \\ -\sin(n\theta+\theta) & \cos(n\theta+\theta) \end{bmatrix} \\ &= \begin{bmatrix} \cos((n+1)\theta) & \sin((n+1)\theta) \\ -\sin((n+1)\theta) & \cos((n+1)\theta) \end{bmatrix} \end{aligned}$$

(c) For which values of θ does A have finite order in $O_2(\mathbb{R})$?

This happens exactly when $n\theta$ is a multiple of 2π, for some $n \geq 1$: that is, $\theta = \frac{2\pi k}{n}$, for some integers k, l. (θ is a rational multiple of 2π.)

6. Let a, b be non-zero integers. Prove that a and b are relatively prime if and only if they are the first row of a matrix in $GL_2(\mathbb{Z})$: that is, there is a matrix

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

in $GL_2(\mathbb{Z})$.

First suppose that a, b are relatively prime. Then we can find integers c, d such that $ac + bd = 1$. Then

$$A = \begin{bmatrix} a & b \\ -d & c \end{bmatrix}$$

is in $GL_2(\mathbb{Z})$ since its determinant is $ac - b(-d) = 1$.

Conversely, if

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

is in $GL_2(\mathbb{Z})$, then the determinant is 1 or -1 so $ad - bc = \pm 1$. If $ad + b(-c) = 1$, then 1 must be the greatest common divisor of a and b, so a and b are relatively prime. On the other hand, if $ad - bc = -1$, we also have $a(-d) + bc = 1$ and again then 1 must be the greatest common divisor of a and b, so a and b are relatively prime.

7. Let $G = D_6$ and $H =< r^2 >= \{e, r^2, r^4\}$ (which is a subgroup – you should be able to prove this, but you do not need to include the proof on your assignment). List all of the left cosets of H in G. Find $[G : H]$.

Solution. It is easiest to list them in a table:

g	gH	gH
e	$\{e \cdot e, e \cdot r^2, e \cdot r^4\}$	$\{e, r^2, r^4\}$
r	$\{r \cdot e, r \cdot r^2, r \cdot r^4\}$	$\{r, r^3, r^5\}$
r^2	$\{r^2 \cdot e, r^2 \cdot r^2, r^2 \cdot r^4\}$	$\{e, r^2, r^4\}$
r^3	$\{r^3 \cdot e, r^3 \cdot r^2, r^3 \cdot r^4\}$	$\{r, r^3, r^5\}$
r^4	$\{r^4 \cdot e, r^4 \cdot r^2, r^4 \cdot r^4\}$	$\{e, r^2, r^4\}$
r^5	$\{r^5 \cdot e, r^5 \cdot r^2, r^5 \cdot r^4\}$	$\{r, r^3, r^5\}$
j	$\{j \cdot e, j \cdot r^2, j \cdot r^4\}$	$\{j, r^4 j, r^2 j\}$
rj	$\{rj \cdot e, rj \cdot r^2, rj \cdot r^4\}$	$\{rj, r^5 j, r^3 j\}$
$r^2 j$	$\{r^2 j \cdot e, r^2 j \cdot r^2, r^2 j \cdot r^4\}$	$\{r^2 j, j, r^4 j\}$
$r^3 j$	$\{r^3 j \cdot e, r^3 j \cdot r^2, r^3 j \cdot r^4\}$	$\{r^3 j, rj, r^5 j\}$
$r^4 j$	$\{r^4 j \cdot e, r^4 j \cdot r^2, r^4 j \cdot r^4\}$	$\{r^4 j, r^2 j, j\}$
$r^5 j$	$\{r^5 j \cdot e, r^5 j \cdot r^2, r^5 j \cdot r^4\}$	$\{r^5 j, r^3 j, rj\}$

There are four distinct left cosets. Thus, $[G : H] = 4$.

8. Let $G = GL_2(\mathbb{R})$ and $H = SL_2(\mathbb{R})$. Prove that, for any a, b in G, the cosets aH and bH are equal if and only if $det(a) = det(b)$.

Solution.

First, suppose that $aH = bH$. We will actually give two proofs that $\det(a) = \det(b)$.

We know that a is in the coset aH. The fact that this is equal to bH means that there is some h in H such that $a = bh$. Then we have

$$\det(a) = \det(bh) = \det(b)\det(h) = \det(b)1 = \det(b),$$

since h is in H, it has determinant 1.

Alternately, the fact that $aH = bH$ means that $a^{-1}b$ is in H. So

$$1 = \det(a^{-1}b) = \det(a^{-1})\det(b) = \det(a)^{-1}\det(b),$$

and this implies that $\det(a) = \det(b)$.

Now suppose that $\det(a) = \det(b)$. It follows that

$$\det(a^{-1}b) = \det(a^{-1})\det(b) = \det(a)^{-1}\det(b) = 1.$$

This means that $a^{-1}b$ is in H. This implies that $aH = bH$.

9. (a) Let G be a cyclic group of order n. Prove that G has a subgroup of order k for every positive divisor k of n. (In other words, prove that the converse of Corollary 3.9.12 holds for cyclic groups.)

   (b) What are the possible orders of subgroups of A_4 (the alternating group on n elements). Does there actually exist a subgroup of each of these orders? (You may look up a list of the subgroups of A_4.) What conclusion can you draw about Corollary 3.9.12?

Solution.

(a) Let g be a generator of G and suppose that k is a positive divisor of n, so $n = qk$ for some $q \in \mathbb{Z}^+$. Then $\langle g^q \rangle$ is a subgroup of G, and

$$\begin{aligned}\langle g^q \rangle &= \{g^q, (g^q)^2, (g^q)^3, \ldots, (g^q)^{k-1}, (g^q)^k\} \\ &= \{g^q, g^{2q}, g^{3q}, \ldots, g^{(k-1)q}, g^{kq}\} \\ &= \{g^q, g^{2q}, g^{3q}, \ldots, g^{(k-1)q}, e\},\end{aligned}$$

since $g^k q = g^n = e$. To see that $o(\langle g^q \rangle) = k$, we need to show that the k elements listed are all distinct. For this, suppose $g^{iq} = g^{jq}$ for some $i, j \in \{0, 1, \ldots, k-1\}$. Multiplying both sides by $(g^{jq})^{-1}$ and simplifying gives $g^{(i-j)q} = e$. Let $i - j = k'$. Since i and j are both in the range $0, 1, \ldots k-1$, k' is also in this range; in particular $k' < k$, and therefore $k'q < kq = n$. Therefore $k' = 0$, since n is the smallest positive integer such that $g^n = e$. This implies that $i = j$, and so we have established that the only way we can have $g^{iq} = g^{jq}$ is if $i = j$. Therefore the elements of $\langle g^q \rangle$ listed above are all distinct, and so G has a subgroup of order k (namely $\langle g^q \rangle$).

(b) The group A_4 has order 12, since half of the 24 permutations in S_4 are even. By Lagrange's Theorem, any subgroup of A_4 has order 1, 2, 3, 4, 6 or 12, since these are the positive divisors of $o(A_4)$. The subgroups of A_4 are listed below.

- The trivial subgroup: $\{\varepsilon\}$. This has order 1.
- Subgroups generated by an element of the form $(a_1\ a_2)(a_3\ a_4)$: $\{\varepsilon, (12)(34)\}$, $\{\varepsilon, (13)(24)\}$, $\{\varepsilon, (14)(23)\}$. These have order 2.
- Union of the above (unions of subgroups are not always subgroups, but this one happens to be): $\{\varepsilon, (12)(34), (13)(24), (14)(23)\}$. This has order 4.
- Subgroups generated by an element of the form $(a_1\ a_2\ a_3)$: $\{\varepsilon, (123), (132)\}$, $\{\varepsilon, (124), (142)\}$, $\{\varepsilon, (134), (143)\}$, $\{\varepsilon, (234), (243)\}$. These have order 3.

- Whole group:
  $A_4 = \{\varepsilon, (12)(34), (13)(24), (14)(23), (234), (243), (134), (143),$
  $(124), (142), (123), (132)\}$.
  This has order 12.

We see that there is no subgroup of order 6. We conclude that the converse of Lagrange's Theorem is not necessarily true for general groups:

Rules for group assignments. Make sure you follow the universal rules for group assignments (below) and any additional rules/procedures laid out in your Group Contract.

1. Each group member is expected to contribute to the best of their ability, and assignment submissions should only include the names of group members who meet this expectation.

2. Each group member should be able to explain the group's solution to me and answer any questions I may have about it. It is the whole group's responsibility to ensure that this standard is met.

3. The task of composing final solutions and writing them up in good copy must be shared equally among all group members (after a collaborative problem-solving process).

4. After good copy solutions are complete, they should be shared among all group members to be double-checked and proofread. This should be done in advance of the due date, to allow time for any necessary corrections. Corrections should be completed by the person who wrote the original solution.