Solutions to Assignment 4

1. Given that f and g are endomorphisms of an abelian group M. Define $h(a) = f(a)+g(a)$ for every a in M. Check that h is an endomorphism of the abelian group M.

Solution: We check that

$$h(a+b) = f(a+b) + g(a+b) = (f(a) + f(b)) + (g(a) + g(b))$$

We now use commutativity and associativity of the operation to get

$$h(a+b) = (f(a) + g(a)) + (f(b) + g(b)) = h(a) + h(b)$$

This shows that h is an endomorphism. (We can easily check that $h(0) = 0$ and $h(-a) = -h(a)$ by the same method.)

2. Given that f and g are endomorphisms of an abelian group M. Define $h(a) = f(g(a))$ for every a in M. Check that h is an endomorphism of the abelian group M.

Solution: We check that

$$h(a+b) = f(g(a+b)) = f(g(a) + g(b)) = f(g(a)) + f(g(b)) = h(a) + h(b)$$

We similarly check that $h(0) = 0$ and $h(-a) = -h(a)$.

3. The $\underline{0}$ endomorphism of an abelian group M sends every element of M to 0. The $\underline{1}$ endomorphism of M is the identity map of M to itself. With the above definitions of addition and multiplications, check that $\mathrm{End}(M)$ is a ring.

Solution: The associativity of addition and multiplication is easily checked. Let us check the distributive law.

$$\begin{aligned}(f \circ (g+h))(a) = f((g+h)(a)) = f(g(a) + h(a)) = f(g(a)) + f(h(a)) = \\ (f \circ g)(a) + (f \circ h)(a) = (f \circ g + f \circ h)(a)\end{aligned}$$

The additive and multiplicative identities are similarly checked.

4. Consider the natural ring homomorphism $\eta : \mathbb{Z} \to \mathrm{End}(M)$ given that the latter is a ring. Describe the element $\eta(3)$ and $\eta(-2)$. How do you prove that this description is correct?

Solution: The element $\eta(3)$ maps every element a of M to the element $a + a + a$. This is because $\eta(1)$ is the identity endomorphism of M, and $\eta(3) = \eta(1)+\eta(1)+\eta(1)$.

The element $\eta(-2)$ maps every element a of M to the element $(-a) + (-a)$. This is because $\eta(-1)$ sends each element of M to its additive inverse, so that $\eta(0) = \eta(1) + \eta(-1)$ sends each element of M to the 0 element of M. It follows that $\eta(-2) = \eta(-1) + \eta(-1)$ is as described.

5. Use the (left) distributive law in a ring R to show that $x \mapsto a \cdot x$ is an endomorphism of $(R, +)$.

Solution: The left distributive law for R says that if a, x and y are elements of R, then

$$a \cdot (x + y) = a \cdot x + a \cdot y$$

Moreover, $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$, so by adding $-(a \cdot 0)$ to both sides we see that $a \cdot 0 = 0$. Next,

$$a \cdot x + a \cdot (-x) = a \cdot (x + (-x)) = a \cdot 0 = 0$$

shows that $a \cdot (-x) == (a \cdot x)$, so that a preserves additive inverses.

6. Call the map in the previous exercise ℓ_a. Use associativity of multiplication in R to show that $\ell_a \circ \ell_b = \ell_{a \cdot b}$.

Solution: We use associativity at the third step to get

$$(\ell_a \circ \ell_b)(x) = \ell_a(\ell_b(x)) = a \cdot (b \cdot x) = (a \cdot b) \cdot x = (\ell_{a \cdot b})(x)$$

7. Use the right distributive law in R to show that $\ell_{a+b} = \ell_a + \ell_b$ where the right-hand side is addition of endomorphisms of $(R, +)$.

Solution: We use associativity at the third step to get

$$(\ell_{a+b})(x) = (a + b) \cdot x = a \cdot x + b \cdot x = \ell_a(x) + \ell + b(x) = (\ell_a + \ell_b)(x)$$

8. Use the multiplicative identity law to show that ℓ_1 is the identity endomorphism of $(R, +)$. Similarly, show that ℓ_0 is the constant endomorphism that sends every element to 0.

Solution:

$$(\ell_1)(a) = 1 \cdot a = a$$

Secondly, we have

$$(\ell_0)(a) = 0 \cdot a = 0$$

9. If p is any integer and a an element of an abelian group M, then show that the order of $p \cdot a$ divides the order m of a.

Solution: If the order of a is n, then the subgroup of M which consists of integer multiples of a (i. e. the sub-group generated by a) is isomorphic to the cyclic group $\mathbb{Z}/n$ via the map that sends p to $p \cdot a$.

The order of every element $p \cdot a$ of this subgroup divides the order n if this subgroup.

10. In the above situation, if p and m have no common factor, then show that the order of $p \cdot a$ is m.

Solution: If p and n have no common factor, then there are integers A and B so that $pA + nB = 1$. As a has order n, we see that $A \cdot (p \cdot a) + B \cdot (n \cdot a) = 1 \cdot a = a$. It follows that $A \cdot (p \cdot a) = a$.

This means that the order of a divides the order of $p \cdot a$ and the order $p \cdot a$ divides the order of a. Hence these are both of the same order.

11. In the situation where k divides the order m of a, show that the element $k \cdot a$ has order *exactly* m/k.

Solution: It is clear that $(m/k) \cdot (k \cdot a) = m \cdot a = 0$. On the other hand, write $m = l \cdot k$ and suppose $p \cdot (k \cdot a) = 0$. Then, m divides $p \cdot k$ or $p \cdot k = q \cdot m$ for some integer q. This gives $p \cdot k = q \cdot l \cdot k$. Cancelling k, we have $p = q \cdot l$; in other words, l divides q. It follows that l is the order of $k \cdot a$.

12. Combine the above two exercises to show that if the order of $p \cdot a$ is m/k where k the greatest common divisor of p and m.

Solution: We write $p = l \cdot k$ where k is as above and l and m have no common factor. Then l and k also have no common factor. It follows that $k \cdot a$ has order m/k as above and that $l \cdot (k \cdot a)$ has the same order as that of $k \cdot a$.

13. Given two elements a and b in an abelian group M with orders m and n respectively. If m and n have no common factor then show that if some multiple $p \cdot a$ equals some multiple $q \cdot b$ then both of these are the 0 element of M. (Hint: The order of $p \cdot a$ is a divisor of m and that of $q \cdot b$ is a divisor of n.)

Solution: The order of $p \cdot a$ is a divisor of m and the order of $q \cdot b$ is a divisor of n. As m and n have greatest common divisor 1, it follows that the order of $p \cdot a = q \cdot b$ is 1. In other words, this is the 0 element.

14. In the above situation, if m and n have no common factor then the order of $a+b$ is $m \cdot n$.

Solution: If $p \cdot (a + b) = 0$, then $p \cdot a = (-p) \cdot b$. It follows that both of these must be 0. In other words, p is divisible by the order n of a and $(-p)$ is divisible by the order m of b. It follows that p is divisible by mn. Conversely, we check that $(mn) \cdot (a + b) = 0$.

15. Given positive integers m and n, show that there is a divisor k of m and a divisor l of n so that:

    1. k and l have no common factor.
    2. The least common multiple of m and n is $k \cdot l$.

    (Hint: Let k be product of those prime powers dividing m that are the same as the prime powers dividing the least common multiple of m and n. Let l be the product of the remaining prime powers dividing the l.c.m. of m and n.)

Solution: Let k as in the hint, be the product of those prime powers dividing m which are the same as those dividing the least common multiple of m and n. Then m/k divides $l = L/k$ where L is the least common multiple of m and n. Then k and l have no common factor and $k \cdot l = L$.

16. With a, b in M as above and m, n, k and l positive integers as above, show that $(m/k) \cdot a + (n/l) \cdot b$ has order equal to the least common multiple of the m and n.

Solution: As seen above, $(m/k) \cdot a$ has order k and $(n/l) \cdot b$ has order l. Since l and k are co-prime, we see that $(m/k) \cdot a + (n/l) \cdot b$ has order $l \cdot k = L$, the least common multiple of m and n.

17. (Starred) Given a and b in M of order m and n respectively, show that the order of any element of the form $p \cdot a + q \cdot b$ divides the least common multiple of m and n.

18. Check that the order of every non-zero element of $\mathbb{Z}/3 \times \mathbb{Z}/3$ is 3.

> **Solution:** On the one hand, if $(a, b) \neq (0, 0)$ then its order is *bigger* than 1. On the other hand $3 \cdot (a, b) = (0, 0)$ so that its order divides 3. Hence, this order is 3.

19. Check that the order of the element $(1, 1)$ of $\mathbb{Z}/4 \times \mathbb{Z}/9$ is 36.

> **Solution:** The element $(1, 0)$ has order 4 and the element $(0, 1)$ has order 9. Hence, by what has been seen above, we see that $(1, 1) = (1, 0) + (0, 1)$ has order $36 = 4 \cdot 9$.

20. Find an element of order 6 in $\mathbb{Z}/4 \times \mathbb{Z}/9$.

> **Solution:** By an earlier exercise, the element $6 \cdot (1, 1) = (2, \cdot 6)$ has order $36/6 = 6$.

21. If a is an element of an (abelian) group M, and N is a subgroup of G. Suppose $s \cdot a$ and $t \cdot a$ lie in N. Show that $p \cdot a$ lies in N where p is the greatest common divisor of s and t. (Hint: p can be written as an additive combination of s and u.)

> **Solution:** We have integers S and U so that $p = Ss + Uu$. It follows that $p \cdot a = S \cdot (s \cdot a) + U \cdot (u \cdot a)$. It is clear that the right-hand side lies in N, hence the left-hand-side lies in N.

22. Suppose that u divides n and s divides u. Now if k is a divisor of n so that $n/k = u/s$, show that s divides k.

> **Solution:** We write $n = u \cdot v$ and $u = s \cdot t$. We deduce $n = s \cdot t \cdot v$. Now $n = k \cdot (u/s) = k \cdot t$. It follows that $s \cdot t \cdot v = k \cdot t$. Cancelling t, we have $s \cdot v = k$ so that s divides k.