Modern Algebra I HW 4 Solutions

Theo Coyne

Problem 1.

In general, given a group G and an element $g \in G$ of (finite) order n, the order of g^i is $n/\gcd(n,i)$ for every integer i.

(a) Since g generates C_{10} it must have full order 10. With the above fact in mind, we immediately have:

g^2 has order $10/2 = 5$.

g^5 has order $10/5 = 2$.

g^4 has order $10/2 = 5$.

g^3 has order 10.

All cyclic groups are abelian so C_{10} is in particular. We saw above that g^3 has order 10, so it is a generator too.

(b) We use the theorem that in a finite cyclic group of order n, there is exactly one subgroup of each order dividing n and these are all the subgroups.

Order 1 subgroup: the trivial subgroup $\{1\}$.

Order 2 subgroup: $\langle g^5 \rangle = \{1, g^5\}$.

Order 5 subgroup: $\langle g^2 \rangle = \{1, g^2, g^4, g^6, g^8\}$.

Order 10 subgroup: The full group C_{10}.

Problem 2.

Since a has order 40, the order of a^i is $40/\gcd(40,i)$ for each i. Using this:

- a^2 has order $40/2 = 20$.
- a^{12} has order $40/4 = 10$.
- a^{-5} has order $40/5 = 8$.
- a^{11} has order 40.

There is a subgroup of order 8 because 8 divides 40- take the subgroup generated by a^5. There is no subgroup of order 12 because 12 doesn't divide 40.

Problem 3.

Recall that a subset H of a group G is a subgroup if it is closed under the group operation, contains the identity element of G, and all of its elements' inverses are also in H.

(a) $\{1, -1\}$ is closed under multiplication, contains 1, and is closed under inversion because $(-1)^{-1} = -1$. It is a subgroup of $\mathbb{C}^*$.

(b) $\{i, -i\}$ is not a subgroup of $\mathbb{C}$ because it does not contain the identity element 1. Closure also fails as, for example, $i^2 = -1 \notin \{i, -i\}$.

(c) $\{z \in \mathbb{C} : |z| = 1\}$ is closed under multiplication because if $|z| = |z'| = 1$, then $|zz'| = |z| \cdot |z'| = 1$ too. Since $|1| = 1$, it contains the identity element. For every $z \in \mathbb{C}^*$ with $|z| = 1$, we have $|z^{-1}| = |z|^{-1} = 1$, so H is closed under inversion.

(d) $\mathbb{R}^*$ is clearly closed under multiplication, 1 is a nonzero real, and $1/z$ exists and is a nonzero real whenever z is. So $\mathbb{R}^*$ is a subgroup of $\mathbb{C}^*$.

(e) $\mathbb{R}^* \cup i\mathbb{R}^*$ contains 1 because $1 \in \mathbb{R}^*$. Inverses: let $z \in \mathbb{R}^* \cup i\mathbb{R}^*$. If $z \in \mathbb{R}^*$, then $1/z \in \mathbb{R}^*$, as in the above part. If instead $z = ix \in i\mathbb{R}^*$ for $x \in \mathbb{R}^*$, then $1/z = 1/(ix) = -i/x \in i\mathbb{R}^*$. Finally, the product of two elements of $\mathbb{R}^*$ is in $\mathbb{R}^*$, the product of two elements in $i\mathbb{R}^*$ is in $\mathbb{R}^*$, and the product of an element of $\mathbb{R}^*$ with an element of $i\mathbb{R}^*$ is in $i\mathbb{R}^*$. This exhausts all possible cases of products of elements of $\mathbb{R}^* \cup i\mathbb{R}^*$ and we see that our set is closed under multiplication and is a subgroup of $\mathbb{C}^*$.

Problem 4.

In general, $\mathbb{Z}_n^*$ consists of the elements in $\{0, \ldots, n-1\}$ that are coprime to n. So,

1. $\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\}$ has 6 elements. The cyclic subgroups generated by its elements are as follows:

   $$\langle 1 \rangle = \{1\}$$
   $$\langle 2 \rangle = \{1, 2, 4, 8, 7, 5\}$$
   $$\langle 4 \rangle = \{4, 7, 1\}$$
   $$\langle 5 \rangle = \{1, 5, 7, 8, 4, 2\}$$
   $$\langle 7 \rangle = \{1, 7, 4\}$$
   $$\langle 8 \rangle = \{1, 8\}$$

   So, $1, 2, 4, 5, 7, 8$ have orders $1, 6, 3, 6, 3, 2$ respectively.

   Since 5 and 2 are generators, the group $\mathbb{Z}_9^*$ is cyclic.

2. $\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$ has 4 elements. The cyclic subgroups generated by its elements are as follows:

   $\langle 1 \rangle = \{1\}$

   $\langle 5 \rangle = \{1, 5\}$

   $\langle 7 \rangle = \{1, 7\}$

   $\langle 11 \rangle = \{1, 11\}$

   All of the non-identity elements have order 2 and so none are generators of $\mathbb{Z}_{12}^*$, hence $\mathbb{Z}_{12}^*$ is not cyclic. It is isomorphic to the Klein four-group $C_2 \times C_2$.

3. $\mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ has 10 elements. As this group is somewhat larger, I'll only write down a couple of its cyclic subgroups. The first several powers of 2 mod 11 are $1, 2, 4, 8, 5, 10, 9, 7, 3, 6$, which is all of $\mathbb{Z}_{11}^*$, so $\langle 2 \rangle = \mathbb{Z}_{11}^*$. The element 5 generates a subgroup with elements $\{1, 5, 3, 4, 9\}$.

   So, $\mathbb{Z}_{11}^*$ is cyclic and 2 is a generator.

   Remark 1. *For any prime p, it's the case that $\mathbb{Z}_p^*$ is cyclic.*

Problem 5.

(a) We must check associativity, the existence of an identity element, and the existence of inverses for all elements.

Associativity: Let (g_i, h_i) for $i = 1, 2, 3$ be three arbitrary elements of $G \times H$. We have

$$((g_1, h_1) \circ (g_2, h_2)) \circ (g_3, h_3) = (g_1 g_2, h_1 h_2) \circ (g_3, h_3) = ((g_1 g_2) g_3, (h_1 h_2) h_3)$$
$$= (g_1 (g_2 g_3), h_1 (h_2 h_3)) = (g_1, h_1) \circ (g_2 g_3, h_2 h_3) = (g_1, h_1) \circ ((g_2, h_2) \circ (g_3, h_3)) .$$

To go from the first to the second line, we used the associativity of the group operations in G and H.

Identity: Let e_G be the identity element of G and e_H the identity element of H. Then for any element $(g, h) \in G \times H$, we have

$$(e_G, e_H) \circ (g, h) = (e_G g, e_H h) = (g, h)$$

and

$$(g, h) \circ (e_G, e_H) = (g e_G, h e_H) = (g, h).$$

Hence (e_G, e_H) is an identity element for $G \times H$.

Inverses: Let (g, h) be an arbitrary element of $G \times H$. We check that (g^{-1}, h^{-1}) is an inverse element. We have
$(g, h) \circ (g^{-1}, h^{-1}) = (g g^{-1}, h h^{-1}) = (e_G, e_H)$ and
$(g^{-1}, h^{-1}) \circ (g, h) = (g^{-1} g, h^{-1} h) = (e_G, e_H)$, as required.

(b) If G and H are both abelian, then for all $(g_1, h_1) \in G \times H$ and $(g_2, h_2) \in G \times H$, we have

$$(g_1, h_1) \circ (g_2, h_2) = (g_1 g_2, h_1 h_2) = (g_2 g_1, h_2 h_1) = (g_2, h_2) \circ (g_1, h_2).$$

Hence, $G \times H$ is abelian.

Remark 2. *The "if" in the problem statement can be strengthened to an "if and only if". If $G \times H$ is an abelian group under $\circ$, then for all $g, g' \in G$ and $h, h' \in H$, we have*

$$(gg', hh') = (g, h) \circ (g', h') = (g', h') \circ (g, h) = (g'g, h'h),$$

from which the equalities $gg' = g'g$ and $hh' = h'h$ follow. This implies that G and H are both abelian.