Intro to Modern Algebra I Midterm Practice Solutions

Iris Rosenblum-Sellers, Noah Olander, Anton Wu

1)

a)

False. If $A = \{1, 2\}$ and $B = \{2, 3\}$, then $A \backslash B = \{x \in A : x \notin B\} = \{1\}$ and $A \backslash (A \backslash B) = \{x \in A : x \notin (A \backslash B)\} = \{2\}$, so in general $A \backslash (A \backslash B) \neq B$. [Observe that $A \backslash (A \backslash B) = A \cap B$ is always true.]

b)

True. If $gh = hg$, then $g^3 h = g^2(gh) = g^2(hg) = g(gh)g = g(hg)g = (gh)g^2 = (hg)g^2 = hg^3$.

c)

False. Recall that $a \equiv b \pmod m$ if m divides $a - b$; so $75 \not\equiv -7 \pmod{17}$, as 17 does not divide $75 - (-7) = 82$.

d)

True. For $x, y \in A$ such that $g(f(x)) = g(f(y))$, because g is injective we must have $f(x) = f(y)$, and then because f is injective we must have $x = y$. Hence $(g \circ f)$ is injective.

e)

False. In $G = S_3$, consider $g = (12)$ and $h = (23)$. We have $\imath(g) = (12)$ and $\imath(h) = (23)$. Then

$$\imath(gh) = \imath((12)(23)) = \imath((123)) = (132) \qquad \text{and} \qquad \imath(g)\imath(h) = (12)(23) = (123)$$

so $\imath(gh) \neq \imath(g)\imath(h)$. [Observe that in general, $\imath(gh) = \imath(h)\imath(g)$.]

2)

a)

Recall that $[a] \in \mathbb{Z}_m$ is a generator if $\gcd(a, m) = 1$. This follows from Bézout's lemma, which says that for any $a, m \in \mathbb{Z}$, there exist integers x, y such that $ax + my = \gcd(a, m)$; so if $\gcd(a, m) = 1$, then $ax \equiv 1 \pmod m$, which means $1 \in \langle a \rangle$, and thus $\mathbb{Z}_m = \langle 1 \rangle \subseteq \langle a \rangle \subseteq \mathbb{Z}_m$, so $\langle a \rangle = \mathbb{Z}_m$, which is to say that a is a generator of $\mathbb{Z}_m$. Hence the generators of $\mathbb{Z}_7$ are [1], [2], [3], [4], [5], [6]; and the generators of $\mathbb{Z}_8$ are [1], [3], [5], [7].

b)

We have $[x] = [991^{13}] = [991]^{13} = [1]^{13} = [1]$, so $991^{13} \equiv 1 \pmod 9$.

c)

Recall that a *homomorphism* f from a group $(G, \cdot)$ to a group $(H, \cdot)$ must satisfy $f(g_1 g_2) = f(g_1)f(g_2)$. Thus, since $f([a_1 + a_2]) = [3(a_1 + a_2)] = [3a_1 + 3a_2] = [3a_1] + [3a_2] = f([a_1]) + f([a_2])$, we have shown that f is a homomorphism from $\mathbb{Z}_9$ to $\mathbb{Z}_9$. The kernel of f is $\{[0], [3], [6]\}$, since 9 divides $3a$ if and only if 3 divides a.

3)

a)

The equivalence classes correspond to each state in the United States; everyone who lives in a particular state is equivalent, and are equivalent to no one from other states.

b)

This is not an equivalence relation; we see that the distance from the origin to $(0,1)$ is 1, $(0,0) \sim (0,1)$. Additionally, the distance from the origin to $(0,-1)$ is 1, so $(0,0) \sim (0,-1)$. If this were an equivalence relation, we would have $(0,-1) \sim (0,1)$ by transitivity. However, the distance between these is 2, which is greater than 1, so they are not equivalent.

c)

Two matrices are equivalent under this relation if they have the same eigenvalues, since those are the roots the characteristic polynomial. Then the equivalence classes consist of possibilities for eigenvalues for a 2x2 complex matrix; each can be represented by a distinct diagonal matrix with entries those eigenvalues.

4)

a)

This inclusion is possible; we note that [2] has order 7, so it generates a cyclic subgroup of order 7.

b)

This inclusion is not possible; by Lagrange's theorem, any subgroup has order equal to a factor of the parent group, and 6 is not a factor of 9.

c)

This inclusion is not possible; the Klein 4 group consists of 3 elements of order 2. The only order 2 element in $\mathbb{Z}/32\mathbb{Z}$ is [16]; to see this, if $[n]$ is order 2, then $[2n] = [0]$, so it's a multiple of 32, so n is half a multiple of 32, so it's [16] or [0], and the latter is order 1, so the inclusion isn't possible.

5)

a)

If $\mathbb{R}$ had a non-trivial subgroup of finite order, it would have a nonzero element of finite order. That is, there would exist $x \in \mathbb{R}, x \neq 0$ such that $nx = 0$ for some $n > 0$. However, there are no such elements, e.g. because $\mathbb{R}$ is a field.

b)

$\mathbb{Z}$ is a subgroup of $\mathbb{Q}$ since $0 \in \mathbb{Z}$, the sum of two integers is an integer, and if $n \in \mathbb{Z}$, then so is $-n$. For an example of a subgroup of $\mathbb{Q}$ bigger than $\mathbb{Z}$, we can take $H = \{x \in \mathbb{Q} : 2x \in \mathbb{Z}\}$. This is a subgroup: $2 \cdot 0 = 0 \in \mathbb{Z}$, so $0 \in H$. If $x, y \in H$ then $2(x \pm y) = 2x \pm 2y \in \mathbb{Z}$ so $x \pm y \in H$.

6)

First of all, there is at least one such element, namely e. We must show it is the only one. Suppose for contradiction that there is $x \in G, x \neq e$, with $x^2 = e$. Take some element $y \neq x, y \neq e$ (this is possible since G has 5 elements and $5 > 2$). Then consider the elements e, x, y, xy. We claim they are distinct. We already know e, x, y are distinct, so we must show $xy \notin \{e, x, y\}$. First of all $xy \neq e$ since that would mean $y = x^{-1} = x$ since $x^2 = e$ and inverses are unique. Next $xy \neq x$ because this would imply $y = e$ by cancellation. Finally, $xy \neq y$ since this would imply $x = e$ by cancellation. Therefore we have proven that $\{e, x, y, xy\}$ has four elements. Since G has five elements, there is one element we haven't yet listed. Let z be this fifth element. We claim that $xz \notin \{e, x, y, xy, z\}$. This will be our contradiction, since $xz \in G$ and G has only 5 elements. To prove this, note that $xz \neq e = x^2$ since this would imply $x = z$ by cancellation. Also, $xz \neq x$ since this would imply $z = 1$; $xz \neq xy$ since this would imply $z = y$; and $xz \neq z$ since this would imply $x = 1$. Finally, if $xz = y$, then $z = x^2z = xy$, which is false. Now we are done.