Algebra 1 Midterm 1 Solutions

Noah Olander, Anton Wu, and Iris Rosenblum-Sellers

April 1, 2020

1) True or False:

a) For any three sets A, B, C,

$$A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$$

True: $x \in A \setminus (B \cap C) \iff x \in A$ and $x \notin B \cap C \iff x \in A$ and $x \notin B$ or $x \notin C \iff x \in A, x \notin B$ or $x \in A, x \notin C \iff x \in (A \setminus B) \cup (A \setminus C)$.

b) If H and J are subgroups of a group G, then so is $H \cup J$.

False: For example, take $H = 2\mathbf{Z}$ and $J = 3\mathbf{Z}$, both subgroups of $\mathbf{Z}$. Then $5 = 2 + 3$ but $2, 3 \in 2\mathbf{Z} \cup 3\mathbf{Z}$ and 5 isn't.

c) $108 \equiv -3 \pmod{37}$

True: $108 + 3 = 3 \cdot 37$.

d) Let A, B, C be sets, and let $f : A \to B$ be injective and $g : B \to C$ surjective. Then $g \circ f : A \to C$ is bijective.

False: Take $A = B = \{1, 2\}, C = \{1\}$, and let f be the identity and g the unique function $B \to C$ (i.e. $g(1) = g(2) = 1$.

e) Let $f : \mathbf{Z}_5 \to \mathbf{Z}_5$ be the function which takes $[n]$ to $[3n]$. Then f is a bijection.

True: It's inverse is the function g which takes $[n]$ to $[2n]$. Compute $fg([n]) = gf([n]) = [6n] = [n]$.

2) a) (i) $41 + 76 \equiv 12 \pmod{35}$

(ii) $1000000000001^2 \equiv 1 \pmod{10}$

b) List the elements of $\mathbf{Z}_6$ that are *not* generators.

These are the $[n]$ such that $(6, n) \neq 1$. That is, $[0], [2], [3], [4]$.

3) Which of the following is an equivalence relation? Justify your answer.

a) On the set X of residents of New York City, we say $a \sim b$ if a and b live on the same street.

This is an equivalence relation. We check reflexivity: it is clear that a person lives on the same street as themself. Transitivity: If two people a and b live on the same street, call that street α; then if b lives on the same street as a person c, person c must live on α, so a and c live on the same street as well. Symmetry: let a and b live on α again; we see that b lives on α, and so does a, so $b \sim a$ if $a \sim b$.

b) Let N be an integer. On the set $\mathbb{N}$ of natural numbers, we say $a \sim b$ if $\gcd(a, N) = \gcd(b, N)$.

This is an equivalence relation. We check reflexivitity: it is clear that $\gcd(a, N) = \gcd(a, N)$. Likewise, symmetry: $a \sim b \Rightarrow \gcd(a, N) = \gcd(b, N) \Rightarrow \gcd(b, N) = \gcd(a, N) \Rightarrow b \sim a$. Finally, transitivity: if $\gcd(a, N) = \gcd(b, N)$, and $\gcd(b, N) = \gcd(c, N)$, then by transitivity of equality, we have $\gcd(a, N) = \gcd(c, N)$.

c) On the set $\mathbb{C}$ of complex numbers, we say $a \sim b$ if $a - b$ is the square of an integer.

This is not an equivalence relation because it's not symmetric; if $a = 2, b = 1$, then we have $a - b = 2 - 1 = 1 = 1^2$, so $a \sim b$. However, $b - a = 1 - 2 = -1$, which is not the square of an integer, so $b \nsim a$.

4) Let G be a group, and let g, h, j be elements of G. Prove carefully that if $jghj = jhgj$, then g and h commute.

Proof. Let the setup be as given. Then $jghj = jhgj := z$. Then since G is a group, let j^{-1} be the inverse of j; the unique element such that $jj^{-1} = j^{-1}j = e$, where e is the identity. $j^{-1}zj^{-1} = j^{-1}zj^{-1}$, since they are equal termwise; i.e. $j^{-1} = j^{-1}, z = z$, so their products are equal since the binary operation given by the product is uniquely valued. Then $z = jghj = jhgj$, so $j^{-1}jghjj^{-1} = j^{-1}jhgjj^{-1}$, by the same principle. Then by definition of j^{-1}, we have $j^{-1}j = jj^{-1} = e$, so $eghe = ehge$. Then by definition of the identity, $e(ghe) = ghe$, and $e(hge) = hge$, so $ghe = hge$. Finally, by definition of the identity, we have $(gh)e = gh, (hg)e = hg$, so $gh = hg$, so they commute. ∎

5)

a) Let $\mathbb{R}^\times$ be the group of non-zero real numbers under multiplication. Find a finite subgroup of $\mathbb{R}^\times$ that contains more than one element.

A finite subgroup of $\mathbb{R}^\times$ containing more than one element is $\langle -1 \rangle = \{1, -1\}$; one easily verifies that $\langle -1 \rangle$ is closed under multiplication, contains 1, and contains inverses.

b) Show that the subgroup found in (a) and the subgroup with one element are the only finite subgroups of $\mathbb{R}^\times$.

Suppose $G \neq \{1\}, \{1, -1\}$ is another finite subgroup of $\mathbb{R}^\times$. Then $1 \in G$ by the properties of subgroups, and thus G must contain at least one other element $x \neq -1$, to distinguish it from $\{1\}$ and $\{1, -1\}$. But then $x^n \neq 1$ for any n (as roots of unity must have absolute value 1), so the cyclic subgroup generated by x is infinite. Since $\langle x \rangle \subseteq G$, we see that G must, too, be infinite, a contradiction.

Hence $\{1\}$ and $\{1, -1\}$ are the only finite subgroups of $\mathbb{R}^\times$.

6) List the sets of cyclic subgroups of $\mathbb{Z}_3 \times \mathbb{Z}_3$ and of $\mathbb{Z}_3 \times \mathbb{Z}_2$.

The cyclic subgroups of $\mathbb{Z}_3 \times \mathbb{Z}_3$ are

$$\langle (0,0) \rangle = \{(0,0)\}$$
$$\langle (0,1) \rangle = \langle (0,2) \rangle = \{(0,0), (0,1), (0,2)\}$$
$$\langle (1,0) \rangle = \langle (2,0) \rangle = \{(0,0), (1,0), (2,0)\}$$
$$\langle (1,1) \rangle = \langle (2,2) \rangle = \{(0,0), (1,1), (2,2)\}$$
$$\langle (1,2) \rangle = \langle (2,1) \rangle = \{(0,0), (1,2), (2,1)\}$$

and the cyclic subgroups of $\mathbb{Z}_3 \times \mathbb{Z}_2$ are

$$\langle (0,0) \rangle = \{(0,0)\}$$
$$\langle (0,1) \rangle = \{(0,0), (0,1)\}$$
$$\langle (1,0) \rangle = \langle (2,0) \rangle = \{(0,0), (1,0), (2,0)\}$$
$$\langle (1,1) \rangle = \langle (2,1) \rangle = \{(0,0), (1,1), (2,0), (0,1), (1,0), (2,1)\}$$

[Observe that $\mathbb{Z}_3 \times \mathbb{Z}_3$ is not cyclic, while $\mathbb{Z}_3 \times \mathbb{Z}_2 = \langle (1,1) \rangle$ is cyclic.]