JOSEPH OKONOBOH
Mathematics
Cal State Long Beach

1. Consider the veracity or falsehood of each of the following statements. For bonus, argue for those that you believe are true while providing a counterexample for those that you believe are false. Throughout G is a group.

   (1) If $g \in G$ is the only element of order 2, then $g \in Z(G)$, the center.

   (2) The intersection of two subgroups of G is also a subgroup.

   (3) The union of two subgroups of G is also a subgroup.

   (4) The largest order of an element in S_{12} is 60.

   (5) If an Abelian group has an element of order 10 and an element of order 12, then it has an element of order 30.

   Solution.

   (1) True.
   Proof. Assume that $g \in G$ is the only element of order 2. Let h be an arbitrary element in G. It suffices to show that $gh = hg$. We claim that $|hgh^{-1}| = 2$. So we have that $(hgh^{-1})^2 = hgh^{-1}hgh^{-1} = hg^2h^{-1} = hh^{-1} = e$. Now suppose that $hgh^{-1} = e$. Then it must be the case that $g = h^{-1}h = e$, a contradiction since $|g| = 2$. Thus we have that $|hgh^{-1}| = 2$. But since g is the only element of order 2, it follows that $hgh^{-1} = g$, so that $hg = gh$; since the choice of h was arbitrary, we can conclude that $g \in Z(G)$. $\square$

   (2) True.
   Proof. Let $H_1 \leq G$, $H_2 \leq G$, and $H' = H_1 \cap H_2$. Since e is in both H_1 and H_2, it follows that $e \in H'$. The set H' is also associative because it is a subset of G. Now let $a, b \in H'$. Thus we must have that $a, b \in H_1$ and $a, b \in H_2$. Since H_1 and H_2 are groups, it follows that they both contain ab and a^{-1} so that $ab, a^{-1} \in H'$. That is, H is closed under the operation of G and also closed under taking inverses. Thus $H' \leq G$. $\square$

   (3) False.
   Counterexample: Consider $2\mathbb{Z}, 3\mathbb{Z} \leq \mathbb{Z}$. We have that $2 \in 2\mathbb{Z}$ and $3 \in 3\mathbb{Z}$, but $2 + 3 = 5 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$.

   (4) True. The permutation

   $$\sigma = (1\ 2\ 3\ 4\ 5)(6\ 7\ 8\ 9)(10\ 11\ 12)$$

   has order 60. Let Suppose $\alpha \in S_{12}$ has order greater than 60. Now write α as a product of disjoint cycles

   $$\alpha = \alpha_1 \alpha_2 \cdots \alpha_n.$$

   Let $j \in \{1, 2, \ldots, n\}$. Then α_j cannot be a 12-cycle since that would imply that $|\alpha| = 12$. For the same reason α_j can neither be an 11-cycle or a 10-cycle. If α_j is a 9-cycle, then $|\alpha|$ is either 9 (9+3)or 18 (9+2+1). Now if α_j is a 8-cycle, then $|\alpha|$ is either 8 (8+4, 8+2+2, 8+2+1+1) or 24(8+3+1).

(5) True.

Proof. Let g and h have orders 10 and 12 in some abelian group. The element g^2 has order 5 and the element h^2 has order 6. Since $\gcd(5,6)=1$, it follows that $|g^2h^2| = 5 \cdot 6 = 30$. □

2. We have beads of four different colors.

(1) How many distinct four-bead necklaces can we make?

(2) How many distinct five-bead necklaces can we make?

(3) How many distinct six-bead necklaces can we make?

BONUS: Answer the same questions if we now have beads of five colors.

Solution.

(1) a

3. Consider the following two sets of matrices

$$S_1 = \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} : a, b \in \mathbb{Z} \right\} \text{ and } S_2 = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in \mathbb{Z} \right\}.$$

Do the following for both:

(1) Decide if they are rings or not—and give reasons.

(2) Decide if they are integral domains or not—and give reasons.

(3) Can you find a root for the polynomial x^2+1 in either place? If so find all the roots or give reasons.

Solution.

(1) a

4. Let R be a ring. An additive subgroup I is called an ideal if whenever $r \in R$ and $a \in I$, then $ra, ar \in I$.

(1) Find two ideals of $\mathbb{Z}$ that are neither 0 nor $\mathbb{Z}$.

(2) Let I be an ideal. Prove the following are true: if $I+x$ and $I+y$ are the same coset and $I+m$ and $I+n$ are the same coset, then $I+(x+m)$ and $I+(y+n)$ are the same coset, and so are $I+xm$ and $I+yn$.

(3) Let S be a ring, and let $\alpha : R \to S$ be a ring homomorphism—this means with respect to both operations. Show $I = \ker(\alpha) = \{a \in R : \alpha(a) = 0\}$ is an ideal.

Solution.

(1) Consider $n\mathbb{Z} < \mathbb{Z}$, with $n > 1$. Let $x \in n\mathbb{Z}$ and let $z \in \mathbb{Z}$. Then $x = nm$ for some integer m, so that $zx = xz = (nm)z = n(mz) \in n\mathbb{Z}$. Thus $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$, so that $444\mathbb{Z}$ and $410\mathbb{Z}$ are both nontrivial ideals of $\mathbb{Z}$.

(2) **Proof.** Let I be an ideal. Assume that $x, y, m, n \in R$ such that $I + x = I + y$ and $I+m = I+n$. We want to show that $I+(x+m) \subseteq I+(y+n)$ and $I+xm \subseteq I+yn$. So let $r_1 \in I + (x + m)$ and $r_2 \in I + xm$. Thus

$$\begin{aligned} r_1 &= i_1 + (x + m) && [\text{for some } i_1 \in I] \\ &= (i_1 + x) + m \\ &= (i_2 + y) + m && [I + x = I + y; i_2 \in I] \\ &= (i_2 + m) + y && [(R, +) \text{ is abelian}] \\ &= (i_3 + n) + y && [I + m = I + n; i_3 \in I] \\ &= i_3 + (y + n) \in I + (y + n) \end{aligned}$$

and $r_2 = i_4 + xm$ for some $i_4 \in I$. Since $I + x = I + y$ and $I + m = I + n$, it follows that $i_4 + x = i_5 + y$ and $i_4 + m = i_6 + n$ for some $i_5, i_6 \in I$. Thus we have that $x = y + i_5 - i_4$ and $m = n + i_6 - i_4$, so that

$$\begin{aligned} r_2 &= i_4 + xm \\ &= i_4 + (y + i_5 - i_4)(n + i_6 - i_4) \\ &= i_4 + y(i_6 - i_4) + n(i_5 - i_4) + (i_5 - i_4)(i_6 - i_4) + yn. \end{aligned}$$

Since I is an ideal, it must be the case that

$$i_4 + y(i_6 - i_4) + n(i_5 - i_4) + (i_5 - i_4)(i_6 - i_4) \in I.$$

Thus $r_2 \in I + yn$. We have thus shown that $I + (x + m) \subseteq I + (y + n)$ and $I+xm \subseteq I+yn$. The argument that $I+(y+n) \subseteq I+(x+m)$ and $I+yn \subseteq I+xm$ follows by symmetry. Thus $I + (x + m) = I + (y + n)$ and $I + xm = I + yn$. □

(3) **Proof.** Let $\alpha : R \to S$ be a homomorphism of rings. To show that $\ker(\alpha)$ is an ideal of R, we have to first show that $(\ker(\alpha), +) \leq (R, +)$.

Identity. Since α is also a group homomorphism, we know from our discussion in group theory that $\alpha(1) = 1$, so that $1 \in \ker(\alpha)$.

Closure. Let $a, b \in \ker(\alpha)$. Then we have that $\alpha(a+b) = \alpha(a)+\alpha(b) = 0+0 = 0$, so that $a + b \in \ker(\alpha)$; i.e., $\ker(\alpha)$ is closed under addition.

Inverse. Let $a \in \ker(\alpha)$. Then we have that

$$\begin{aligned} \alpha(-a) &= \alpha(-1 \cdot a) \\ &= \alpha(-1) \cdot \alpha(a) \\ &= \alpha(-1) \cdot 0 = 0, \end{aligned}$$

so that $-a \in \ker(\alpha)$, and thus $\ker(\alpha)$ is closed under taking inverses.

It follows from above that $\ker(\alpha)$ is an additive subgroup of R. Now let $a \in \ker(\alpha)$, $r \in R$. To complete the proof, we must show that $ar \in \ker(\alpha)$ and $ra \in \ker(\alpha)$. Thus

$$\begin{aligned}
0 &= 0 \cdot \alpha(r) \\
&= \alpha(a) \cdot \alpha(r) && [\alpha(a) \in \ker(\alpha)] \\
&= \alpha(ar) && [\text{so that } ar \in \ker(\alpha)] \\
&= 0 \\
&= \alpha(r) \cdot \alpha(a) \\
&= \alpha(ra), && [\text{so that } ra \in \ker(\alpha)]
\end{aligned}$$

so that$ra, ar \in \ker(\alpha)$ and $\ker(\alpha)$ is an ideal. □