

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 $j \in \{1, 2, \dots, n\}$. 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 $|g^2h^2| = 5 \cdot 6 = 30$. \square

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 We claim that S_1 and S_2 are both commutative rings.

Proof. First we want to show that $(S_1, +)$ and $(S_2, +)$ are abelian groups.

Identity. It is clear that S_1 and S_2 both contain the zero matrix, which is the identity under addition.

Associativity, Closure & Commutativity under $+$. Since \mathbb{Z} is associative, closed, and commutative under addition, it follows that S_1 and S_2 are both associative, closed, and commutative under addition.

Inverse. For each matrix A in S_1 (resp. S_2) we have that $-A$ is in S_1 (resp. S_2) so that S_1 and S_2 are both closed under taking inverses.

Thus we have shown that S_1 and S_2 are abelian groups.

Identity under multiplication. It is clear that S_1 and S_2 both contain the 2×2 identity matrix, which serves as the multiplicative identity.

Associativity, Closure & Commutativity under multiplication. Let

$$\begin{pmatrix} a & b \\ b & a \end{pmatrix}, \begin{pmatrix} c & d \\ d & c \end{pmatrix} \in S_1 \text{ and } \begin{pmatrix} e & f \\ -f & e \end{pmatrix}, \begin{pmatrix} g & h \\ -h & g \end{pmatrix} \in S_2.$$

Then it follows that

$$\begin{pmatrix} a & b \\ b & a \end{pmatrix} \begin{pmatrix} c & d \\ d & c \end{pmatrix} = \begin{pmatrix} ac+bd & ad+bc \\ ad+bc & ac+bd \end{pmatrix} = \begin{pmatrix} c & d \\ d & c \end{pmatrix} \begin{pmatrix} a & b \\ b & a \end{pmatrix} \in S_1$$

and

$$\begin{pmatrix} e & f \\ -f & e \end{pmatrix} \begin{pmatrix} g & h \\ -h & g \end{pmatrix} = \begin{pmatrix} eg-fh & eh+fg \\ -eh-fg & eg-fh \end{pmatrix} = \begin{pmatrix} g & h \\ -h & g \end{pmatrix} \begin{pmatrix} e & f \\ -f & e \end{pmatrix} \in S_2$$

so that S_1 and S_2 are both closed and commutative under multiplication. Associativity follows since matrices are associative under multiplication.

Distributivity. For any $n \times n$ matrices A , B , and C , we know that

$$A(B+C) = AB+AC \text{ and that } (B+C)A = BA+CA;$$

thus multiplication distributes over addition in S_1 and S_2 .

From the arguments above, we have thus shown that S_1 and S_2 are rings. \square

- ② S_1 is not an integral domain because we have that

$$A = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \in S_1,$$

with A and B nonzero but $AB = 0$. We now claim that S_2 is an integral domain.

Proof. Suppose to the contrary that S_2 is not an integral domain. Then there exist nonzero matrices $A, B \in S_2$, where

$$A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}, B = \begin{pmatrix} c & d \\ -d & c \end{pmatrix},$$

such that $AB = 0$. Then it follows that $0 = \det(0) = \det(A)\det(B)$. Since $\det(A)$ and $\det(B)$ are integers and since \mathbb{Z} is an integral domain, it follows that $\det(A) = 0$ or $\det(B) = 0$. Assume without loss that $\det(A) = 0$. Then it follows that $a^2 + b^2 = 0$, so that $a = b = 0$, a contradiction since A is nonzero. Thus S_2 is an integral domain. \square

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 $\alpha : R \rightarrow S$ 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 $I + xm = I + yn$. \square

- ③ **Proof.** Let $\alpha : R \rightarrow S$ 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. □