Instructions. Answer each of the questions on your own paper. Be sure to show your work so that partial credit can be adequately assessed. Put your name on each page of your paper.

1. [**10 Points**] All of the following are commutative rings with identity: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_4$, $\mathbb{Z}_5$, and $\mathbb{Z}_6$. Which of these rings are integral domains? Which are fields? You do not need to justify your answers to this question.

   ▶ **Solution.** Integral domains are: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_5$

   Fields are: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_5$ ◀

2. [**20 Points**] Suppose that R is a commutative ring with identity.

   (a) What properties must a subset I of R satisfy in order to be an ideal?

   ▶ **Solution.** If $a, b \in I$, $r \in R$, then $a \pm b \in I$ and $ra \in I$. ◀

   (b) Define what it means for an ideal to be *prime*.

   ▶ **Solution.** An ideal I is prime if $I \neq R$ and if $ab \in I$ then $a \in I$ or $b \in I$. ◀

   (c) Define what it means for an ideal to be *maximal*.

   ▶ **Solution.** An ideal I is maximal if $I \neq R$ and for any ideal J with $I \subseteq J \subseteq R$, either $J = I$ or $J = R$ ◀

   (d) Prove that the ideal $I = \{f(x) \in \mathbb{Z}[x] \mid f(0) = 0\}$ of $\mathbb{Z}[x]$ is prime, but not maximal.

   ▶ **Solution.** The map $\phi : \mathbb{Z}[x] \to \mathbb{Z}$ given by $\phi(f(x)) = f(0)$ is a ring homomorphism. The homomorphism ϕ is surjective since, for the constant polynomial n, $\phi(n) = n$, and $\operatorname{Ker}(\phi) = I$ so by the first isomorphism theorem for ring homomorphisms, $\mathbb{Z}[x]/I \cong \mathbb{Z}$. Since $\mathbb{Z}$ is an integral domain I is a prime ideal. Since $\mathbb{Z}$ is not a field, I is not a maximal ideal. ◀

   (e) Give an example to show that a factor ring of an integral domain may have zero-divisors. (Recall that a nonzero element a in a ring R is a zero-divisor if there is a nonzero $b \in R$ with $ab = 0$.)

   ▶ **Solution.** $\mathbb{Z}_4 = \mathbb{Z}/4\mathbb{Z}$ is a factor ring of the integral domain $\mathbb{Z}$, but $2 \in \mathbb{Z}_4$ is a zero-divisor since $2 \neq 0$ and $2^2 = 0 \in \mathbb{Z}_4$. ◀

3. [**12 Points**] For the permutation

$$\sigma = \begin{pmatrix}1 & 3 & 5 & 7\end{pmatrix}\begin{pmatrix}2 & 3 & 4 & 7\end{pmatrix}\begin{pmatrix}6 & 1\end{pmatrix}\begin{pmatrix}1 & 7 & 5 & 3\end{pmatrix} \in S_7:$$

(a) Write σ as a product of disjoint cycles.

▶ **Solution.** $\sigma = \begin{pmatrix} 1 & 2 & 5 & 4 \end{pmatrix} \begin{pmatrix} 3 & 6 \end{pmatrix}$ ◀

(b) Compute the order of σ in the group S_7.

▶ **Solution.** $|\sigma| = \operatorname{lcm}(4, 2) = 4$ ◀

(c) Determine whether σ is even or odd.

▶ **Solution.** A 4-cycle is odd and a 2-cycle is odd, so σ is the product of two odd permutations, and hence is even. ◀

(d) Compute σ^{-1}. You may express your answer in whatever form you wish.

▶ **Solution.** $\sigma^{-1} = \begin{pmatrix} 1 & 4 & 5 & 2 \end{pmatrix} \begin{pmatrix} 3 & 6 \end{pmatrix}$ ◀

4. **[12 Points]** The alternating group A_4 consists of the 12 elements in S_4 which are even permutations. Let

$$H = \left\{(1), \begin{pmatrix} 1 & 2 \end{pmatrix} \begin{pmatrix} 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 3 \end{pmatrix} \begin{pmatrix} 2 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 4 \end{pmatrix} \begin{pmatrix} 2 & 3 \end{pmatrix}\right\}.$$

You may assume without proof that H is a subgroup of A_4. The remaining elements of A_4 are the 8 3-cycles in S_4.

(a) Show that H is isomorphic to the group $\mathbb{Z}_2 \times \mathbb{Z}_2$.

▶ **Solution.** Every abelian group of order 4 is isomorphic to $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$. Since any product of disjoint 2-cycles has order 2, it follows that all non-identity elements of H have order 2, and hence there is no element of order 4. Thus, it must be isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$. ◀

(b) List the left and right cosets of H in A_4.

▶ **Solution.** Left cosets:

$$\begin{aligned}
(1)H &= \left\{(1), \begin{pmatrix} 1 & 2 \end{pmatrix} \begin{pmatrix} 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 3 \end{pmatrix} \begin{pmatrix} 2 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 4 \end{pmatrix} \begin{pmatrix} 2 & 3 \end{pmatrix}\right\} \\
\begin{pmatrix} 1 & 2 & 3 \end{pmatrix} H &= \left\{\begin{pmatrix} 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 2 & 4 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 4 & 2 \end{pmatrix}\right\} \\
\begin{pmatrix} 1 & 2 & 4 \end{pmatrix} H &= \left\{\begin{pmatrix} 1 & 2 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 4 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 3 & 4 \end{pmatrix}\right\}
\end{aligned}$$

Right cosets:

$$\begin{aligned}
H(1) &= \left\{(1), \begin{pmatrix} 1 & 2 \end{pmatrix} \begin{pmatrix} 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 3 \end{pmatrix} \begin{pmatrix} 2 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 4 \end{pmatrix} \begin{pmatrix} 2 & 3 \end{pmatrix}\right\} \\
H \begin{pmatrix} 1 & 2 & 3 \end{pmatrix} &= \left\{\begin{pmatrix} 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 2 & 4 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 4 & 2 \end{pmatrix}\right\} \\
H \begin{pmatrix} 1 & 2 & 4 \end{pmatrix} &= \left\{\begin{pmatrix} 1 & 2 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 4 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 3 & 4 \end{pmatrix}\right\}
\end{aligned}$$

◀

(c) Is H a normal subgroup of A_4?

▶ **Solution.** Since each left coset is a right coset in part (b), H is a normal subgroup of A_4. ◀

5. [**10 Points**]

(a) If $G = \langle a \rangle = \{1, a, a^2, \ldots, a^{11}\}$ is a cyclic group of order 12, then list all of the generators of G.

▶ **Solution.** The element a^k is a generator of G if and only if $\gcd(k, 12) = 1$. Thus the generators of G are a, a^5, a^7, and a^{11} ◀

(b) The group $U(13)$ of integers modulo 13 with a multiplicative inverse is a cyclic group (under multiplication modulo 13) of order 12. List all of the generators. (*Hint:* $U(13)$ is generated by 2.)

▶ **Solution.** The powers of 2 in $U(13)$ are

k	1	2	3	4	5	6	7	8	9	10	11	12
2^k	2	4	8	3	6	12	11	9	5	10	7	1

By part (a), the generators of $U(13)$ are $2^1 = 2$, $2^5 = 6$, $2^7 = 11$, and $2^{11} = 7$. ◀

6. [**15 Points**] If G is a group, let $H = \{a \in G \mid a^2 = 1\}$.

(a) If G is abelian, prove that H is a subgroup of G.

▶ **Solution.** Use the subgroup test. $1^2 = 1$ so $1 \in H$. If $a \in H$, then $a^2 = 1$ so $a = a^{-1}$ and $a^{-1} \in H$. Now suppose $a, b \in H$. Then $a^2 = 1$ and $b^2 = 1$, and since G is abelian, $(ab)^2 = abab = aabb = a^2b^2 = 1 \cdot 1 = 1$ so $ab \in H$. Thus, H is a subgroup. ◀

(b) Give an example of a nonabelian group G such that H is not a subgroup.

▶ **Solution.** Let $G = S_3$. In this case H consists of the identity (1) and all 2-cycles, so

$$H = \{(1), (1, 2), (1, 3), (2, 3)\}.$$

Since $(1, 2)(1, 3) = (1, 3, 2) \notin H$, H is not closed under multiplication, and hence is not a subgroup of S_3. ◀

7. [**10 Points**] Let $G = \mathbb{Z}_4 \times \mathbb{Z}_2$, let $H = \langle (2, 1) \rangle$ and $K = \langle (2, 0) \rangle$. Show that H is isomorphic to K, but G/H is not isomorphic to G/K.

▶ **Solution.** Since $2(2,\,1) = (0,\,0) \in G$ and $2(2,\,0) = (0,\,0) \in G$, both H and K are cyclic subgroups of G or order 2 and hence are isomorphic. Since $2((1,\,0) + H) = (2,\,0) + H \neq (0,\,0) + H$ because $(2,\,0) \notin H$ it follows that $(1, 0) + H$ has order greater than 2, and hence it must have order 4 since $|G/H| = |G| / |H| = 8/2 = 4$. Thus G/H is cyclic of order 4. The distinct elements of G/K are $(0, 0) + K$, $(1, 0) + K$, $(0, 1) + K$, and $(1, 1) + K$. Since $2(1, 0) = (2, 0 \in K$, $2(0, 1) = (0, 0) \in K$, $2(1, 1) = (2, 0) \in K$, it follows that every element of G/K has order 2 or 1, and hence is not cyclic. Thus, G/H is not isomorphic to G/K. ◀

8. [**10 Points**]

(a) Compute the greatest common divisor d of the integers 1769 and 2378.

▶ **Solution.** Use the Euclidean algorithm:

$$\begin{aligned} 2378 &= 1769 + 609 \\ 1769 &= 2 \cdot 609 + 551 \\ 609 &= 551 + 58 \\ 551 &= 9 \cdot 58 + 29 \\ 58 &= 2 \cdot 29 + 0 \end{aligned}$$

Thus, $\gcd(2378,\,1769) = 29$. ◀

(b) Write d as a linear combination $d = 1769 \cdot s + 2378 \cdot t$.

▶ **Solution.** Reverse the above steps:

$$\begin{aligned} 29 &= 551 - 9 \cdot 58 \\ &= 551 - 9(609 - 551) = 10 \cdot 551 - 9 \cdot 609 \\ &= 10(1769 - 2 \cdot 609) - 9 \cdot 609 = 10 \cdot 1769 - 29 \cdot 609 \\ &= 10 \cdot 1769 - 29(2378 - 1769) \\ &= 39 \cdot 1769 - 29 \cdot 2378. \end{aligned}$$

◀

9. [**12 Points**]

(a) Give of list of the distinct isomorphism classes of abelian groups of order 72.

▶ **Solution.** Since $72 = 2^3 \cdot 3^2$ the distinct isomorphism class of abelian groups of order 72 are:

i. $\mathbb{Z}_8 \times \mathbb{Z}_9$
ii. $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_9$
iii. $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9$

iv. $\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3$

v. $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$

vi. $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$

◀

(b) Which of the groups in your list satisfy the condition $a^{12} = 1$ for all $a \in G$. This condition is written multiplicatively. If the group operation is addition, the condition would be $12a = 0$.

▶ **Solution.** The condition $12a = 0$ (these groups are written additively) means that the order of every element is divisible by 12. Thus, the possible orders of elements are 1, 2, 3, 4, 6, 12. Groups i.-iv. all have elements of order 9 or 8, which are not divisible by 12. Since in a direct product of groups, the order of an element is the least common multiple of the orders of its component elements, the groups v. and vi. have orders of all elements divisible by 12. ◀

(c) Which group on your list is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}_6$.

▶ **Solution.** Since if m and n are relatively prime, $\mathbb{Z}_n \times \mathbb{Z}_n \cong \mathbb{Z}_{nm}$ it follows that

$$\mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_3$$

which is isomorphic to the group vi. in the above list. ◀