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

1. **[12 Points]**

   (a) Assume that G is a set that is closed under a binary operation $*$. What properties are needed to make G a group with the binary operation $*$?

   ▶ **Solution.**

   Associativity $(a * b) * c = a * (b * c)$ for all a, b, $c \in G$.
   Identity There is an element $1 \in G$ with $1 * a = a * 1 = a$ for all $a \in G$.
   Inverses For each $a \in G$ there is a $b \in G$ with $a * b = b * a = 1$.

   ◀

   (b) The set $S = \{a \in \mathbb{Q} \mid a \neq 0\}$ is closed under the commutative binary operation $*$ defined by

   $$a * b = \frac{ab}{3}.$$

   Prove that the set S with the binary operation is an abelian group.

   ▶ **Solution.** $*$ is associative:

   $$(a * b) * c = \left(\frac{ab}{3}\right) * c = \frac{\left(\frac{ab}{3}\right) c}{3} = \frac{abc}{9}$$

   and

   $$a * (b * c) = a * \left(\frac{bc}{3}\right) = \frac{a\left(\frac{bc}{3}\right)}{3} = \frac{abc}{9}$$

   Thus, $(a * b) * c = a * (b * c)$ for all a, b, $c \in S$ and associativity holds.
   Since $a * b = \frac{ab}{3} = \frac{ba}{3} = b * a$ the operation $*$ on S is commutatative. Thus, to check the identity and inverse properties, it is only necessary to check one side.
   Thus, $a * 3 = \frac{a \cdot 3}{3} = a$ for all $a \in S$, so $3 = 1_S$ for this operation.

   Also, given $a \in S$, $a * \frac{9}{a} = \frac{a \cdot \frac{9}{a}}{3} = \frac{9}{3} = 3$. Thus, each $a \in S$ has an inverse with respect to $*$, namely, $\frac{9}{a}$.
   Therefore, the set S under $*$ satisfies the 3 properties in part (a), and hence is a group under $*$. Since the operation is commutative, the group S is abelian. ◀

2. **[14 Points]** Circle True (T) or False (F).

   T F (a) If G is a group with $|G| = 13$, then G and $\{1\}$ are the only subgroups. **T**
   T F (b) If G is a group with $|G| = 12$, then the order of every element of G is 12. **F**
   T F (c) If H is a subgroup of a group G with $|G| = 15$ and $|H| = 3$, then every coset of H has 5 elements. **F**
   T F (d) $o(\sigma) \leq 5$ for every σ in the permutation group S_5. **F**
   T F (e) The ring $\mathbb{Z}_3[x]/\langle x^2 \rangle$ has nine elements, namely $a + bx + \langle x^2 \rangle$, a, $b \in \mathbb{Z}_3$. **T**
   T F (f) The ring $\mathbb{Q}[x]/\langle x^2 - 2 \rangle$ is an integral domain. **T**
   T F (g) The ring $\mathbb{R}[x]/\langle x^2 - 2 \rangle$ is a field. **F**

3. **[15 Points]**

   (a) What properties must a subset S of a ring R satisfy in order to be a subring?

   ▶ **Solution.** $1 \in S$, and $a, b \in S \implies a + b \in S$ and $ab \in S$. ◀

   (b) Prove that $T = \{a + bi \mid a, b \in \mathbb{Q}\}$ is a subring of the ring $\mathbb{C}$ of complex numbers. (Recall $\mathbb{Q}$ denotes the rational numbers and $i = \sqrt{-1}$.)

   ▶ **Solution.** $1 = 1 + 0i \in T$. If $a + bi$ and $c + di \in T$, then $(a + bi) + (c + di) = (a + c) + (b + d)i \in T$ since $a + c \in \mathbb{Q}$ and $b + d \in \mathbb{Q}$ when $a, b, c, d \in \mathbb{Q}$. Also,

   $$(a + bi)(c + di) = (ac - bd) + (bc + ac)i \in T$$

   since $ac - bd \in \mathbb{Q}$ and $bc + ac \in \mathbb{Q}$ whenever $a, b, c, d \in \mathbb{Q}$. Thus T is a subring of $\mathbb{C}$. ◀

   (c) Is T a field? Why or why not?

   ▶ **Solution.** T is a field, since if $a + bi \in T$ and $a + bi \neq 0$, then $(a + bi)(a - bi) = a^2 + b^2 \neq 0$ so

   $$(a + bi)\left(\frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}i\right) = 1,$$

   and therefore,

   $$(a + bi)^{-1} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}i \in T.$$

   ◀

4. **[12 Points]**

   (a) Suppose that G is a finite group and H is a subgroup of G. Then Lagrange's theorem states that: $\boxed{|H| \text{ divides } |G|.}$

   (b) Assume that G is a finite group with subgroups H of order 12 and K of order 30. If the order of G is less than 200, what are the possible values for the order of G.

   ▶ **Solution.** By Lagrange's Theorem $|H| = 12$ and $|K| = 30$ divide $|G|$. Thus, $|G|$ is a common multiple of 12 and 30, and hence is a multiple of the least common multiple of 12 and 30, that is 60. Therefore, $|G|$ must be a multiple of 60 that is less that 200, that is $|G| \in \{60, 120, 180\}$. ◀

5. **[15 Points]** Suppose that R is a commutative ring.

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

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

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

   ▶ **Solution.** An ideal I is prime if $i \neq R$ and $ab \in I \implies a \in I$ 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 such that $I \subseteq J \subseteq R$ it follows that $J = I$ or $J = R$. ◀

(d) Show that $I_1 = 2\mathbb{Z} \times 3\mathbb{Z}$ is an ideal of the ring $\mathbb{Z} \times \mathbb{Z}$.

▶ **Solution.** $I_1 = \{(2k, 3m) \mid k, m \in \mathbb{Z}\}$. Thus, if $a = (2k_1, 3m_1)$ and $b = (2k_2, 3m_2)$ are in I_1, then

$$a \pm b = (2k_1, 3m_1) \pm (2k_2, 3m_2) = (2(k_1 \pm k_2), 3(m_1 \pm m_2) \in I_1$$

and if $r = (s, t) \in \mathbb{Z} \times \mathbb{Z}$ then

$$ra = (s, t)(2k_1, 3m_1) = (2k_1 r, 3m_1 s) \in I_1.$$

Thus, I_1 is an ideal of $\mathbb{Z} \times \mathbb{Z}$. ◀

(e) Show that $I_1 = 2\mathbb{Z} \times 3\mathbb{Z}$ is not a prime ideal of the ring $\mathbb{Z} \times \mathbb{Z}$.

▶ **Solution.** $(2, 1)(1, 3) = (2, 3) \in I_1$ but $(2, 1) \notin I_1$ and $(1, 3) \notin I_1$ so I_1 is not a prime ideal. ◀

6. **[14 Points]** For the permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 8 & 7 & 2 & 4 & 9 & 1 & 5 & 6 \end{pmatrix}$:

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

▶ **Solution.** $\sigma = \begin{pmatrix} 1 & 3 & 7 \end{pmatrix} \begin{pmatrix} 2 & 8 & 5 & 4 \end{pmatrix} \begin{pmatrix} 6 & 9 \end{pmatrix}$ ◀

(b) Write σ as a product of transpositions.

▶ **Solution.** $\sigma = (1\,3)(3\,7)(2\,8)(8\,5)(5\,4)(6\,9)$ or $\sigma = (1\,7)(1\,3)(2\,4)(2\,5)(2\,8)(6\,9)$. ◀

(c) Is σ even, odd, neither or both? **Even**

(d) What is the order of σ?

▶ **Solution.** $o(\sigma) = \operatorname{lcm}\{3, 4, 2\} = 12$. ◀

7. **[12 Points]**

(a) If $G = \langle a \rangle$ is a cyclic group of order 100 then what is the order of a^{24}?

▶ **Solution.** $o(a^{24}) = 100/\gcd(24, 100) = 100/4 = 25$. ◀

(b) What is the order of the group $\mathbb{Z}_{40} \times \mathbb{Z}_{60}$?

(c) $|\mathbb{Z}_{40} \times \mathbb{Z}_{60}| = 40 \cdot 60 = 2400$.

(d) What is the order of $(4, 4)$ in $\mathbb{Z}_{40} \times \mathbb{Z}_{60}$?

▶ **Solution.** The order of 4 in $\mathbb{Z}_{40}$ is $40/4 = 10$ and the order of 4 in $\mathbb{Z}_{60}$ is $60/4 = 15$. Thus, the order of $(4, 4) \in \mathbb{Z}_{40} \times \mathbb{Z}_{60}$ is $\text{lcm}(10, 15) = 30$. ◀

8. **[12 Points]** Suppose that F is a field.

   (a) Suppose that $f(x)$, $g(x)$ are nonzero polynomials in $F[x]$. What does the division algorithm in $F[x]$ say?

   ▶ **Solution.** $g(x) = q(x)f(x) + r(x)$ where $r(x) = 0$ or $\deg r(x) < \deg f(x)$. ◀

   (b) Find the quotient $q(x)$ and remainder $r(x)$ when $g(x) = 3x^3 + x^2 + 2x + 3$ is divided by $f(x) = 2x^2 + 3$ in $\mathbb{Z}_5[x]$.
   Answer: $q(x) = 4x + 3$, $r(x) = 4$.

9. **[12 Points]**

   (a) Compute the greatest common divisor d of the integers 803 and 154.

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

$$\begin{bmatrix} 1 & 0 & 154 \\ 0 & 1 & 803 \end{bmatrix} \longrightarrow \begin{bmatrix} 1 & 0 & 154 \\ -5 & 1 & 33 \end{bmatrix} \longrightarrow \begin{bmatrix} 21 & -4 & 22 \\ -5 & 1 & 33 \end{bmatrix} \longrightarrow \begin{bmatrix} 11 & -4 & 23 \\ -26 & 5 & 11 \end{bmatrix}.$$

   Since 11 divides 22, we conclude that $11 = \gcd(803, 154)$ and that

$$11 = -26 \cdot 154 + 5 \cdot 803.$$

   ◀

   (b) Write d as a linear combination $d = 803 \cdot s + 154 \cdot t$. (Done in part (a))

   (c) Compute the least common multiple m of the integers 803 and 154.

   ▶ **Solution.**

$$m = \text{lcm}(803, 154) = \frac{803 \times 154}{11} = \frac{123662}{11} = 11242.$$

   ◀

10. **[10 Points]** Solve the equation $5x = 12$ in the ring $\mathbb{Z}_{44}$.

   ▶ **Solution.** In $\mathbb{Z}_{44}$ $5^{-1} = 9$ since $5 \cdot 9 = 45 \equiv 1 \pmod{44}$. Thus,

$$x = 5^{-1} \cdot 12 = 9 \cdot 12 = 108 \equiv 20 \pmod{44}.$$

   Hence $x = 20 \in \mathbb{Z}_{44}$. ◀

11. **[12 Points]**

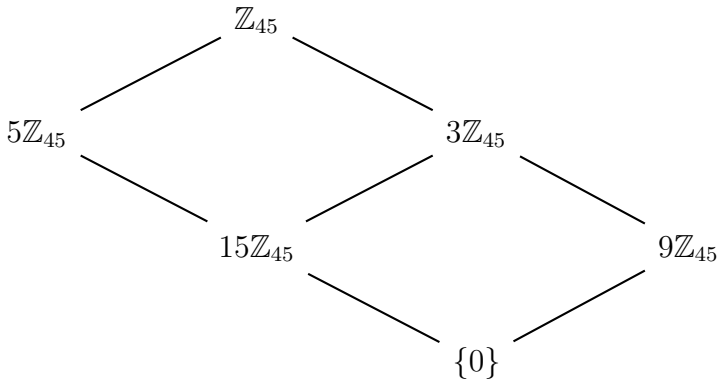
(a) List all of the subgroups of the cyclic group $\mathbb{Z}_{45}$ and give the order of each subgroup.

► **Solution.** The subgroups are $m\mathbb{Z}_{45}$ for all divisors m of 45 and the order of $m\mathbb{Z}_{45}$ is $45/m$. The divisors of 45 are 1, 3, 5, 9, 15, 45 so the subgroups and their orders are:

Subgroup	Order
Z_{45}	45
$3\mathbb{Z}_{45}$	15
$5\mathbb{Z}_{45}$	9
$9\mathbb{Z}_{45}$	5
$15\mathbb{Z}_{45}$	3
$45\mathbb{Z}_{45} = \{0\}$	1

◄

(b) Draw the subgroup diagram for $\mathbb{Z}_{45}$.



12. **[16 Points]** Let $G = \mathbb{Z}_{21}^* = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$ and let $H = \langle 4 \rangle = \{1, 4, 16\}$.

(a) Explain why H is a normal subgroup of G.

► **Solution.** G is an abelian group and in an abelian group all subgroups are normal. ◄

(b) List all of the cosets of H in G. Label each coset as Hg where g is as small as possible. For example, the coset $\{1, 4, 16\}$ (which $= H1 = H4 = H16$) would be labeled $H1$. This is just for convenient labeling. How many cosets are there?

► **Solution.** There are 4 distinct cosets:

$$H1 = \{1, 4, 16\}$$
$$H2 = \{2, 8, 11\}$$
$$H5 = \{5, 20, 17\}$$
$$H10 = \{10, 19, 13\}$$

◀

(c) Write the multiplication table for G/H. List the elements of G/H as in part (b).

▶ **Solution.**

$\times$	$H1$	$H2$	$H5$	$H10$
$H1$	$H1$	$H2$	$H5$	$H10$
$H2$	$H2$	$H1$	$H10$	$H5$
$H5$	$H5$	$H10$	$H1$	$H2$
$H10$	$H10$	$H5$	$H2$	$H1$

◀

(d) Every group of order 4 is isomorphic to $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$. You may assume this fact. Which of these two groups is G/H isomorphic to, and why?

▶ **Solution.** From the table, $x^2 = H1 = 1_{G/H}$ for every $x \in G/H$. Thus every nonidentity element has order 2. This is true for $\mathbb{Z}2 \times \mathbb{Z}_2$ but not for $\mathbb{Z}_4$. Therefore, $G/H \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. ◀