True/False. (2 points each) You did not need to justify your answers, but here we include the answers and the reasons.

(a) The cycles $(7, 6, 5)$ and $(3, 58, 28)$ are conjugate in S_{100}.

[✓ TRUE] FALSE

If we let $\tau = (7, 3)(6, 58)(5, 28)$, then $\tau(7, 6, 5)\tau^{-1} = (\tau(7), \tau(6), \tau(5)) = (3, 58, 28)$. There are other choices of τ that work as well.

(b) The subgroup $\langle(1, 2, 3)\rangle$ is a normal subgroup of S_4.

TRUE [✓ FALSE]

For example, $(1, 4)(1, 2, 3)(1, 4)^{-1} = (4, 2, 3) \notin \langle(1, 2, 3)\rangle$.

(c) The set of all positive real numbers with operation multiplication is a group.

[✓ TRUE] FALSE

We have seen that $\mathbb{R} \setminus \{0\}$ is a group with operation multiplication, with identity element 1. The set of all positive real numbers is a subset of $\mathbb{R} \setminus \{0\}$, it contains the identity 1, the product of any two positive numbers is positive, and the inverse of a positive number r is $\frac{1}{r}$, which is still positive. Thus, the set of all positive real numbers is a subgroup of $\mathbb{R} \setminus \{0\}$, and in particular is a group itself.

(d) The function $f : S_3 \to \mathbb{I}_3$ sending each element to its order $f(\alpha) = \mathrm{ord}(\alpha)$ is a homomorphism.

TRUE [✓ FALSE]

The order of a product is not the sum of the orders, so this is false. For a specific counterexample, note that $(1, 2) \cdot \mathbb{1} = (1, 2)$, but $\mathrm{ord}((1, 2)) = 2$, $\mathrm{ord}(\mathbb{1}) = 1$, but

$$\mathrm{ord}((1, 2) \cdot \mathbb{1}) = 2 \not\equiv 0 \mod 3.$$

(e) The function $Sq : (\mathbb{R}, +) \to (\mathbb{R}, +)$ defined by $Sq(x) = x^2$ is a homomorphism.

TRUE [✓ FALSE]

In general, $(x + y)^2 = x^2 + 2xy + y^2$. This is equal to $x^2 + y^2$ if and only if x or y is zero or both are zero. For example, $(1 + 1)^2 = 2^2 = 4 \neq 2 = 1^2 + 1^2$. Thus, the map Sq is not a homomorphism.

Question 1. Equivalence relations. $(3+6+6$ points per part)

(a) Give the definition of an **equivalence relation** on a set X.

An **equivalence relation** is a relation $\sim$ on a set X (thought of as pairs that are "equivalent": we write $x \sim y$ for pairs of elements that are equivalent) which satisfies

1. $\sim$ **is reflexive**: for every $x \in X$, $x \sim x$;
2. $\sim$ **is symmetric**: whenever $x \sim y$, we also have $y \sim x$; and
3. $\sim$ **is transitive**: whenever $x \sim y$ and $y \sim z$, we also have $x \sim z$.

- Some of you said (correctly) that a relation is a subset of $X \times X$. In that case, you needed to prove the following parts in terms of those subsets.

(b) Let $\sigma : X \to X$ be a bijection. Define a relation on X by $x \sim y$ if $\sigma^n(x) = y$ for some $n \in \mathbb{Z}$. Show that $\sim$ defines an equivalence relation.

We must check properties (1)–(3) above.

For (1), σ^0 is the identity function, so $\sigma^0(x) = x$, and so $x \sim x$.

For (2), if $x \sim y$, that means there is an integer n so that $\sigma^n(x) = y$. Note that $\sigma^{-n} = (\sigma^n)^{-1}$, so we also have $\sigma^{-n}(y) = x$, and so $y \sim x$.

Finally, for (3), note that if $x \sim y$, then $\sigma^n(x) = y$ for some $n \in \mathbb{Z}$, and if $y \sim z$, then $\sigma^m(y) = z$ for some $m \in \mathbb{Z}$, THEN $\sigma^{m+n}(x) = \sigma^m(\sigma^n(x)) = \sigma^m(y) = z$, and so $x \sim z$.

(c) For the bijection $\sigma : \mathbb{Z} \to \mathbb{Z}$ given by $\sigma(m) = m + 5$, determine the equivalence classes of $\sim$.

Using the equivalence relation from (b), we see that $x \sim y$ if $\sigma^n(x) = y$ for some $n \in \mathbb{Z}$. But $\sigma^n(x) = x + n \cdot 5$. This means that the integers equivalent to x are those other integers which differ from x by a multiple of 5. Thus, the equivalence classes are

- $[0] = \{x \mid x \equiv 0 \mod 5\}$
- $[1] = \{x \mid x \equiv 1 \mod 5\}$
- $[2] = \{x \mid x \equiv 2 \mod 5\}$
- $[3] = \{x \mid x \equiv 3 \mod 5\}$
- $[4] = \{x \mid x \equiv 4 \mod 5\}$

We note that these are precisely the equivalence classes of $\mathbb{I}_5$.

Question 2. Permutations. ($6 + 4 + 5$ points per part) Consider the permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 4 & 9 & 6 & 5 & 2 & 3 & 1 & 7 \end{pmatrix} \in S_9.$$

(a) Factor σ into disjoint cycles. Write σ as a product of transpositions. Compute $\mathrm{ord}(\sigma)$ and $\mathrm{sgn}(\sigma)$.

- $\sigma = (1,8)(2,4,6)(3,9,7)(5)$. You don't need to include the (5)!
- $\sigma = (1,8)(2,6)(2,4)(3,7)(3,9)$. You shouldn't need to include (5)! There are multiple ways to write this, but you have to be a little careful.
- $\mathrm{ord}(\sigma) = \mathrm{lcm}(2,3,3,1) = 6$.
- $\mathrm{sgn}(\sigma) = -1$ because σ is a product of an **odd** number of transpositions.

(b) Determine σ^{-1} (in two-line notation) and factor it into disjoint cycles.

- $\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 6 & 7 & 2 & 5 & 4 & 9 & 1 & 3 \end{pmatrix}$.
- $\sigma^{-1} = (1,8)(2,6,4)(3,7,9)$. This has different possible forms.

(c) Is $\sigma^{-1} = \tau\sigma\tau^{-1}$ for some $\tau \in S_9$? Please justify your answer.

Two permutations are conjugate if and only if they have the same cycle type. We saw in (a) and (b) that σ and σ^{-1} do have the same cycle type. (In fact, they always do: you can find the inverse by inverting each of the cycles, which you invert by reversing the order of the numbers in the cycle.) It is easy to check that for $\tau = (4,6)(7,9)$, $\tau\sigma\tau^{-1} = \sigma^{-1}$.
There are other choices of τ that work.

Question 3. Order of an element. ($3+6+6$ points per part)

(a) Give the definition of the **order** of an element g in a group G.

We say that g has **order** $k \in \mathbb{N}$ if k is the smallest positive integer satisfying $g^k = \mathbb{1}$. If there is no such k, we say g has **infinite** order.

A number of you forgot about the infinite order case – careful!!

(b) Show that every non-identity element in the group $G = \left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \middle| \; a, b, c \in \mathbb{I}_3 \right\}$ (with matrix multiplication) has order 3.

We check

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}^2 = \begin{bmatrix} 1 & 2a & 2b+ac \\ 0 & 1 & 2c \\ 0 & 0 & 1 \end{bmatrix}.$$

If the matrix is not the identity to begin with, then at least one of a, b, c is non-zero (mod 3). If a or c is non-zero mod 3, then $2a$ or $2c$ is non-zero mod 3 (respectively). If a and c are zero mod 3, then b must be non-zero, and so $2b + ac \equiv 2b$ is also non-zero mod 3, so this matrix squared is still not the identity matrix.

Next we calculate

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}^3 = \begin{bmatrix} 1 & 3a & 3b+3ac \\ 0 & 1 & 3c \\ 0 & 0 & 1 \end{bmatrix}.$$

Now all the potentially non-zero entries are multiples of 3, so this cubed matrix is the identity, and so the original matrix

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$$

has order 3, as desired.

Checking that $g^2 \neq \mathbb{1}$ is an important step. No one solved it this way, but once you know $g \neq \mathbb{1}$ and $g^3 = \mathbb{1}$, you can deduce that the order isn't 2 because if $g^3 = \mathbb{1}$, the order must be a divisor of 3.

(c) Show that if G is an abelian group, then the subset $H = \{a \in G \mid a^2 = \mathbb{1}\}$ is a subgroup of G.

We simply check:

- $\mathbb{1} \in H$ because $\mathbb{1}^2 = \mathbb{1}$.
- If $a, b \in H$, and because $ab = ba$ by the abelian property,

  $$(ab)^2 = abab = aabb = a^2b^2 = \mathbb{1}\mathbb{1} = \mathbb{1},$$

  so $ab \in H$.
- If $a \in H$, then $a^2 = \mathbb{1}$, so $a = a^{-1}$ and we automatically have $a^{-1} \in H$.

This guarantees that H is a subgroup of the abelian group G.