

1. (15 pts) Define $f : \mathbf{Z}_8 \rightarrow \mathbf{Z}_{12}$ by $f([x]_8) = [3x]_{12}$, for all $[x]_8 \in \mathbf{Z}_8$.
(a) (7 pts) Show that f is a well-defined function. *Show that if $x_1 \equiv x_2 \pmod{8}$, then $3x_1 \equiv 3x_2 \pmod{12}$.*

If $[x_1]_8 = [x_2]_8$, then $8 \mid (x_1 - x_2)$, so multiplying by 3 gives $24 \mid (3x_1 - 3x_2)$, and therefore $12 \mid (3x_1 - 3x_2)$, showing that $f([x_1]_8) = f([x_2]_8)$.

- (b) (8 pts) Find the image $f(\mathbf{Z}_8)$ and the set of equivalence classes \mathbf{Z}_8/f defined by f , and exhibit the one-to-one correspondence between these sets.

We have $f([0]_8) = [0]_{12}$, $f([1]_8) = [3]_{12}$, $f([2]_8) = [6]_{12}$, $f([3]_8) = [9]_{12}$, $f([4]_8) = [12]_{12} = [0]_{12}$, $f([5]_8) = [15]_{12} = [3]_{12}$, $f([6]_8) = [18]_{12} = [6]_{12}$, and $f([7]_8) = [21]_{12} = [9]_{12}$.

The image of f is the subset $\{[0]_{12}, [3]_{12}, [6]_{12}, [9]_{12}\}$. The corresponding preimages, in order, are the sets $\{[0]_8, [4]_8\}$, $\{[1]_8, [5]_8\}$, $\{[2]_8, [6]_8\}$, $\{[3]_8, [7]_8\}$, and these make up the factor set \mathbf{Z}_8/f .

2. (25 pts) Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 5 & 1 & 8 & 3 & 6 & 4 & 7 & 9 \end{pmatrix}$ and $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 5 & 4 & 7 & 2 & 6 & 8 & 9 & 3 \end{pmatrix}$.

We have $\sigma = (1, 2, 5, 3)(4, 8, 7)$, which has order 12 and is odd; $\tau = (2, 5)(3, 4, 7, 8, 9)$, which has order 10 and is odd; $\sigma\tau = (1, 2, 3, 8, 9)$, which order 5 and is even; $\tau\sigma = (1, 5, 4, 9, 3)$, which has order 5 and is even; $\sigma\tau\sigma^{-1} = (5, 3)(1, 8, 4, 7, 9)$, which has order 10 and is odd.

3. (20 pts) Let $f : S \rightarrow T$ and $g : T \rightarrow U$ be functions.
(a) (10 pts) State these definitions: f is **one-to-one**; f is **onto**.
(b) (5 pts) Prove that if gf is a one-to-one function, then so is f .

Suppose that $f(x_1) = f(x_2)$ for $x_1, x_2 \in S$. Then $g(f(x_1)) = g(f(x_2))$ since g is a function, and this implies that $x_1 = x_2$, since gf is one-to-one.

- (c) (5 pts) Prove that if gf is an onto function, then so is g .

Let $u \in U$. Then there exists $s \in S$ with $gf(s) = u$, since gf is onto, and thus $g(t) = u$ for $t = f(x) \in T$, showing that g is onto.

4. (20 pts) For integers m, n, b with $n > 1$, define $f : \mathbf{Z}_n \rightarrow \mathbf{Z}_n$ by $f([x]_n) = [mx + b]_n$. *You may assume that f is a well-defined function.*

Prove that f is a one-to-one correspondence if and only if $\gcd(m, n) = 1$. Then find the inverse function f^{-1} , assuming that $\gcd(m, n) = 1$.

(6 pts) First assume that f is a one-to-one correspondence. Then f is onto, and so $f([x]_n) = [1 + b]_n$ has a solution. But then $mx + b \equiv 1 + b \pmod{n}$, so $mx \equiv 1 \pmod{n}$, which implies that $(m, n) = 1$.

You can also give a proof using the fact that f is one-to-one, but it takes more work since we don't have any result that states that being able to cancel m for all possible integers guarantees that $(m, n) = 1$.

(6 pts) Conversely, suppose that $(m, n) = 1$. Then $f([x_1]_n) = f([x_2]_n)$ implies $[mx_1 + b]_n = [mx_2 + b]_n$, so $[mx_1]_n = [mx_2]_n$. Since $(m, n) = 1$, $[m]_n$ has a multiplicative inverse $[m]_n^{-1}$, and multiplying by it gives $[x_1]_n = [x_2]_n$. Because \mathbf{Z}_n is a finite set and f maps \mathbf{Z}_n into \mathbf{Z}_n , it follows that f is also onto.

(8 pts) You can use the calculus algorithm to find the inverse: $[y]_n = [m]_n[x]_n + [b]_n$ so interchange x and y and solve. We get $[x]_n = [m]_n[y]_n + [b]_n$, so $[m]_n[y]_n = [x]_n - [b]_n$, and then we can multiply by $[m]_n^{-1}$, which exists since $(m, n) = 1$. We get $[y]_n = [m]_n^{-1}[x]_n - [m]_n^{-1}[b]_n$ as the formula for the inverse.

Alternatively you could just give the formula and then check that it works as the inverse of f .

5. (10 pts) Let S be the set of all $n \times n$ matrices with real entries. For $A, B \in S$, define $A \sim B$ if there exists an invertible matrix P such that $B = PAP^{-1}$. Prove that \sim is an equivalence relation.

Let A be any $n \times n$ matrix. Since $A = IAI^{-1}$ for the identity matrix I , it follows that $A \sim A$. (You could use $P = A$ instead of $P = I$.)

Let A, B be $n \times n$ matrices with $A \sim B$. Then there exists an invertible matrix P with $B = PAP^{-1}$. To solve for A , multiply on the left by P^{-1} and on the right by P . (Be careful not to mix up the sides, because matrices don't necessarily satisfy the commutative law. If they did, similarity would be the same as equality, and all eigenvalues would be 1. Review Math 240 if you need to.) So we get $P^{-1}BP = A$. To put this in the right form, note that $P = (P^{-1})^{-1}$. Then we have $P^{-1}B(P^{-1})^{-1} = A$ and so $B \sim A$.

Suppose that A, B, C are $n \times n$ matrices with $A \sim B$ and $B \sim C$. Then there exist invertible matrices P and Q with $B = PAP^{-1}$ and $C = QBQ^{-1}$. (Don't make the mistake of assuming that you can use P in both places.) Substituting for B in the second equation, $C = Q(PAP^{-1})Q^{-1} = (QP)A(QP)^{-1}$, and thus $A \sim C$.

We have verified that reflexive, symmetric, and transitive properties, so \sim is an equivalence relation.

6. (10 pts) Let $\sigma \in S_n$ have order m . Prove that if k is any integer, then $\sigma^k = (1)$ if and only if $m \mid k$.

The rules: You must give a direct proof that does not use Proposition 2.3.7 from the text, which states that $\sigma^i = \sigma^j$ if and only if $i \equiv j \pmod{m}$.

(4 pts) First, suppose that $m \mid k$, say $k = mq$. Then $\sigma^k = \sigma^{mq} = (\sigma^m)^q = (1)^q = (1)$.

(6 pts) Conversely, suppose that $\sigma^k = (1)$. Using the division algorithm we can write $k = mq + r$, with $0 \leq r < m$. Then $(1) = \sigma^k = \sigma^{mq+r} = \sigma^{mq}\sigma^r = (1)\sigma^r$. But m is the smallest positive integer with $\sigma^m = (1)$, so we can't have $0 < r$, and therefore $m \mid k$.

Note: This is very similar to the exercise 10 in Section 1.4, about the multiplicative order of elements in \mathbf{Z}_n^\times .

Grades: A 79–97 (6); B 67–74 (7); C 49–60 (8); D 38–45 (4)