

Justify all your steps. You may use any results that you know unless the question says otherwise, but don't invoke a result that is essentially equivalent to what you are asked to prove or is a standard corollary of it.

1. (10 pts) Let $U(n) = (\mathbf{Z}/n\mathbf{Z})^\times$ be the multiplicative group of units modulo n .
 - (a) (6 pts) For relatively prime $m \geq 2$ and $n \geq 2$, show $U(mn)$ and $U(m) \times U(n)$ are isomorphic groups by writing down a map and proving it is an isomorphism.
 - (b) (4 pts) Use the prime factorization $2024 = 8 \cdot 11 \cdot 23$ to compute the order of 3 in $U(2024)$. Part (a) might be helpful.

2. (10 pts)

We want to define an action of the group $\mathrm{GL}_2(\mathbf{R})$ on the set $\mathbf{C} - \mathbf{R}$ by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \frac{az + b}{cz + d},$$

where $z \in \mathbf{C} - \mathbf{R}$. For example, $\begin{pmatrix} 2 & 3 \\ 0 & 1 \end{pmatrix} z = 2z + 3$ and $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} z = \frac{1}{z}$.

 - (a) (5 pts) Prove the above formula defines an action of $\mathrm{GL}_2(\mathbf{R})$ on $\mathbf{C} - \mathbf{R}$. (This includes checking its values are in $\mathbf{C} - \mathbf{R}$.)
 - (b) (3 pts) Prove the stabilizer of i for this action is $\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in \mathbf{R} \text{ and } (a, b) \neq (0, 0) \}$.
 - (c) (2 pts) Prove this group action has a single orbit.

3. (10 pts)
 - (a) (3 pts) Define what it means for a nonzero element of an integral domain to be irreducible.
 - (b) (7 pts) Prove the reduction mod p test in $\mathbf{Z}[x]$: if $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ is monic and nonconstant and there is a prime p such that $f(x) \bmod p$ is irreducible in $(\mathbf{Z}/p\mathbf{Z})[x]$, then $f(x)$ is irreducible in $\mathbf{Z}[x]$.

4. (10 pts)
 - (a) (5 pts) Prove $\mathbf{Z}[i]$ is Euclidean with respect to the norm on $\mathbf{Z}[i]$: if α and β are in $\mathbf{Z}[i]$ and $\beta \neq 0$, then there are γ and ρ in $\mathbf{Z}[i]$ such that (i) $\alpha = \beta\gamma + \rho$ and (ii) $N(\rho) < N(\beta)$.
 - (b) (5 pts) Prove each ideal in a Euclidean domain is principal. (This does not use (a).)

5. (10 pts) Let V be a real vector space with an inner product $\langle \cdot, \cdot \rangle$ and finite dimension $n \geq 1$.
 - (a) (4 pts) Show every (nonempty) orthogonal set of nonzero vectors in V is a linearly independent set in V .
 - (b) (3 pts) When $w \neq 0$ in V , show $V = \mathbf{R}w \oplus U$ where $U = \{v \in V : \langle v, w \rangle = 0\}$.
 - (c) (3 pts) Use (b) to prove every nonzero finite-dimensional inner product space has an orthogonal basis. Part (a) might be helpful here too.

6. (10 pts) Give examples as requested, with justification.
 - (a) (2.5 pts) A permutation $\sigma \in S_7$ such that $\sigma(123)(4567)\sigma^{-1} = (354)(1762)$.
 - (b) (2.5 pts) An odd prime number p such that the ideal (p) in $\mathbf{Z}[i]$ is not a prime ideal.
 - (c) (2.5 pts) A UFD that is not a PID.
 - (d) (2.5 pts) For $V = \mathbf{R}^2$, a linear map $L: V \rightarrow V$ that is self-adjoint with respect to the usual inner product on V and is not multiplication by a scalar.