

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 p be a prime number.
 - (a) (5 pts) Show every group of order p^n where $n \geq 1$ has a nontrivial center.
 - (b) (5 pts) Use part (a) to show every group whose order is p^2 is abelian.
2. (10 pts) For $a \in \mathbf{Z}$ and $\mathbf{u} = (u_1, u_2, u_3) \in \mathbf{R}^3$, define

$$a * \mathbf{u} = (u_1, au_1 + u_2, a^2u_1 + 2au_2 + u_3).$$
 - (a) (7 pts) Prove the above formula defines an action of the *additive* group $(\mathbf{Z}, +)$ on \mathbf{R}^3 .
 - (b) (3 pts) Show a vector $\mathbf{u} = (u_1, u_2, u_3)$ in \mathbf{R}^3 has a finite \mathbf{Z} -orbit for this action if and only if $u_1 = u_2 = 0$.
3. (10 pts) The goal of this problem is to classify all groups of order 35 up to isomorphism.
 - (a) (4 pts) Determine all *abelian* groups of order 35 up to isomorphism.
 - (b) (6 pts) Show that every group of order 35 is abelian.
4. (10 pts) Let I be the ideal $(7, 1 + \sqrt{-13})$ in $\mathbf{Z}[\sqrt{-13}]$.
 - (a) (5 pts) Show the ring homomorphism $\mathbf{Z}/7\mathbf{Z} \rightarrow \mathbf{Z}[\sqrt{-13}]/I$ given by $a \bmod 7\mathbf{Z} \mapsto a \bmod I$ is an isomorphism.
 - (b) (5 pts) Show I is *not* principal.
5. (10 pts) Let p be a prime number.
 - (a) (3 pts) Prove $\mathbf{Z}[x]/p\mathbf{Z}[x] \cong (\mathbf{Z}/p\mathbf{Z})[x]$ as rings.
 - (b) (7 pts) Prove that a maximal ideal in $\mathbf{Z}[x]$ that contains p must have the form $(p, f(x))$ where $f(x)$ is monic in $\mathbf{Z}[x]$ and $f(x) \bmod p$ is irreducible in $(\mathbf{Z}/p\mathbf{Z})[x]$.
6. (10 pts) Give examples as requested, with justification.
 - (a) (2.5 pts) A nonabelian group of order 21.
 - (b) (2.5 pts) An expression of (12345) as a product of transpositions.
 - (c) (2.5 pts) Gaussian integers γ and ρ such that $7 + 2i = (2 + 3i)\gamma + \rho$ and $N(\rho) < N(2 + 3i)$.
 - (d) (2.5 pts) A homomorphism of commutative rings $f: R \rightarrow S$ and an ideal I in R such that $f(I)$ is not an ideal in S .