(1) Classify all groups of order 75 up to isomorphism.

Proof. Let G be a group of order $75 = 3 \cdot 5^2$. By Sylow's theorems, G has a normal Sylow 5-subgroup P of order 25.

(a) Assume $P \cong \mathbb{Z}/25\mathbb{Z}$. Because $\mathrm{Aut}(P)$ has order 20, any morphism $\mathbb{Z}/3 \to \mathrm{Aut}(P)$ is trivial. Thus, $G \cong P \times \mathbb{Z}/3$.

(b) Assume $P \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$. Then $\mathrm{Aut}(P) \cong GL_2(\mathbb{Z}/5\mathbb{Z})$ has order $24 \times 20 = 3 \times 160$. By Sylow's theorem, the Sylow 3-subgroups of $\mathrm{Aut}(P)$ are conjugate to each other and isomorphic to $\mathbb{Z}/3$. Therefore, any injection $\mathbb{Z}/3 \to \mathrm{Aut}(P)$ give the same group structure on G. Thus, so $G \cong \mathbb{Z}/5 \times \mathbb{Z}/5 \times \mathbb{Z}/3$ or $(\mathbb{Z}/5 \times \mathbb{Z}/5) \rtimes \mathbb{Z}/3$.

□

(2) Let G be a group acting transitively on a set X of size $n > 1$.

(a) If G is finite, show that there exists $g \in G$ so that $gx \neq x$ for all $x \in X$ (hint: count the number of g such that $gx = x$ for some $x \in X$).

Proof. By Burnside's lemma, we have

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|.$$

Since G acts transitively on X, $|X/G| = 1$. Also, we have $X^1 = X$ has size $n > 1$. Therefore there must exist an element g such that $|X^g| = 0$; otherwise, the right-hand side would be greater than 1. □

(b) Give an example to show this can fail for G infinite (Hint: consider $GL_n(\mathbb{C})$ with X the set of 1-dimensional subspaces of the space of column vectors).

Proof. Let $X = \mathbb{P}^1(\mathbb{C}^n)$ and $G = \mathrm{GL}_n(\mathbb{C})$. Then G acts transitively on $\mathbb{C}^n$; hence G acts transitively on X. Because $\mathbb{C}$ is algebraically closed, every matrix $A \in \mathrm{GL}_n(\mathbb{C})$ has all eigenvalues in $\mathbb{C}$. Therefore, the matrix A is at least an eigenvector $v \in \mathbb{C}^n$ and $\mathbb{C} \cdot v \in X$ is a fixed point of G. □

(3) Let R be an integral domain with quotient field F.

(a) If M is a maximal ideal of R, show that the localization R_M of R at M naturally embeds in F.

Proof. This follows from the universal property of localization. □

(b) Show that $R = \cap_M R_M$ where the intersection is over all maximal ideals (hint: If $s \in \cap R_M$ let $I = \{r \in R | rs \in R\}$. show that I is an ideal and is not contained in any maximal ideal M).

Proof. By (a), we can view R_M as a subring of F and take the intersection inside F. It suffices to show that $\frac{\cap_M R_M}{R} = 0$. By the gluing property of modules, it is enough to show that for any maximal ideal $\mathfrak{m}$, $(\frac{\cap_M R_M}{R})_\mathfrak{m} = 0$. Because localization by M and by $\mathfrak{m}$ are commutative and localization is exact,

$$(\frac{\cap_M R_M}{R})_\mathfrak{m} \cong \frac{\cap_M (R_M)_\mathfrak{m}}{R_\mathfrak{m}} = \frac{\cap_M (R_\mathfrak{m})_M}{R_\mathfrak{m}} \subseteq \frac{R_\mathfrak{m}}{R_\mathfrak{m}} = 0.$$

□

(4) Let K be a field of characteristic 0 containing all m-th roots of unity. Let L/K be a field extension and $a \in L$ such that $a^m \in K$. Prove that $K(a)/K$ is Galois with a Galois group that is cyclic of order dividing m.

Proof. Assume ζ is a primitive m-th root of unity. Because $a^m \in K$ and K contains all m-th root of unity, $f(x) = x^m - a^m = (x-a)(x-a\zeta)\cdots(x-a\zeta^{m-1}) \in K[x]$ is separable and splits completely in $K(a)$. Hence, $K(a)/K$ is Galois.

If m is the minimal positive integer such that $a^m \in K$ then $x^m - a^m$ is irreducible over K and the Galois group of $K(a)/K$ is isomorphic to $\mathbb{Z}/m\mathbb{Z}$. If $d < m$ and $a^d \in K$, then $a^{\gcd(d,m)} \in K$ and $x^{\gcd(d,m)} - a^{\gcd(d,m)}$ is irreducible over K; hence $\mathrm{Gal}(K(a)/K) \cong \mathbb{Z}/\gcd(d,m)\mathbb{Z}$. □

(5) Let k be field with $f, g \in k[x_1, ..., x_n]$. Show that $f(a_1, ..., a_n) = 0$ if and only if $g(a_1, ..., a_n) = 0$ is equivalent to f and g having exactly the same (monic) irreducible factors.

Proof. Note that $V(f) = V(g)$ iff Rad(f) = Rad(g), where $V(f)$ is the vanishing locus of the ideal generated by f and Rad(f) is the radical of the ideal generated by f. It suffices to show that f and g have the same irreducible factors if and only if Rad(f) = Rad(g).

Suppose Rad(f) = Rad(g). Then $f \in$ Rad(g), i.e. $f^n \in (g)$. Since $k[x_1, ..., x_n]$ is a UFD, irreducible elements are prime. If $p \mid g$ is irreducible, then $g \mid f^n$ implies $p \mid f^n$ implies $p \mid f$. Thus, any irreducible factor of g is an irreducible factor of f. Therefore, f and g have same irreducible factors.

Conversely, if f and g have the same irreducible factors $p_1, \cdots, p_n$, then $f = a_f p_1^{e_1} \cdots p_n^{e_n}$ and $g = a_g p_1^{d_1} \cdots p_n^{d_n}$ for some $a_f, a_g \in k$ and $e_i, d_i \in \mathbb{Z}_{>0}$. Then there exists some large M such that $e_i M > d_i$ for all i; hence, $g \mid f^M$, i.e. $f \in$ Rad(g) and Rad$(f) \subseteq$ Rad(g). Similarly, one can show that $g \in$ Rad(f), and the conclusion follows. □

(6) Assume that R is a semisimple ring which is a finite-dimensional algebra over a field k, such that for every $r \in R$, there exists a positive integer $n = n(r)$ such that $r^n \in Z(R)$ the center of R. Prove that R is commutative in the following two cases:
  (a) k is finite;
  (b) $k = \mathbb{R}$. (hint: first show that there exists $x \in \mathbb{C}$ such that $x^n \notin \mathbb{R}$, for all positive n)

Proof. Let R be as above. Then R is Artinian since it is finite dimension over k. By Wedderburn-Artin theorem, we have a k-algebra isomorphism

$$R \cong \mathrm{Mat}_{n_1}(D_1) \times \cdots \mathrm{Mat}_{n_k}(D_k).$$

where $n_i \in \mathbb{Z}_{>0}$ and D_i are division algebra over k.

  (a) Assume k is finite. Because k is finite and $\dim_k R < \infty$ implies R is finite; hence, D_i's are finite division rings. Since any finite division ring is a field, D_i's are fields. Note that if $n_i > 1$, then the matrix $E_{11}^k = E_{11}$ and $E_{11} \notin D_i = Z(\mathrm{Mat}_{n_i}(D_i))$ as $E_{11}E_{12} = E_{12} \neq 0 = E_{12}E_{11}$. Hence, $n_i = 1$ for all i and $R \cong D_1 \times \cdots D_k$ is commutative.
  (b) Assume $k = \mathbb{R}$. Then every D_i is one of $\mathbb{R}, \mathbb{C}, \mathbb{H}$(the quaternions). The same argument as in (a) shows that n_i must be 1. It remains to show that $D_i \ncong \mathbb{H}$. Note that the center of $\mathbb{H}$ is $\mathbb{R}$. Consider the element $x = \cos 1 + i \sin 1 \in \mathbb{H}$. Then $x^k = \cos k + i \sin k$ is never in $\mathbb{R}$ for any positive integer k because $\mathbb{Z}\pi \cap \mathbb{Z} = \varnothing$. Therefore, $D_i \ncong \mathbb{H}$ for all i. Thus, R is a product of $\mathbb{R}$'s or $\mathbb{C}$'s; hence R is commutative.

□