1. (3 points) Let G be a cyclic group of prime order q and generator g, i.e. $G = \langle g \rangle$. Let $h \in G$ be another generator of G such that the discrete logarithm of h with respect to g is not known. In multiplicative notation, a Pedersen commitment to a value $\beta \in \mathbb{Z}_q$ with randomizer $\alpha \in \mathbb{Z}_q$ is given by $u = g^\alpha h^\beta$. The pair $(\alpha, \beta) \in \mathbb{Z}_q^2$ is called the *representation* of the group element u with respect to generators g and h. Suppose a prover wants to convince a verifier that it knows the representation of $u \in G$. Prove that the following protocol is **honest-verifier zero-knowledge** and a **proof of knowledge** for the relation

$$\mathcal{R} = \left\{ (u, (\alpha, \beta)) \in G \times \mathbb{Z}_q^2 \mid u = g^\alpha h^\beta \right\}.$$

   (i) Prover picks $\alpha_t \xleftarrow{\$} \mathbb{Z}_q, \beta_t \xleftarrow{\$} \mathbb{Z}_q$ and sets $u_t = g^{\alpha_t} h^{\beta_t}$.
   (ii) Prover sends u_t to the verifier.
   (iii) Verifier picks $c \xleftarrow{\$} \mathbb{Z}_q$ and sends c to the prover.
   (iv) Prover computes $\alpha_z = \alpha_t + \alpha c, \beta_z = \beta_t + \beta c$ and sends α_z, β_z to the verifier.
   (v) Verifier checks that $g^{\alpha_z} h^{\beta_z} = u_t u^c$.

2. (3 points) In the zero-knowledge proof of graph 3-coloring given below, the prover uses a commitment scheme `com` which is perfectly binding and computationally hiding, like the El Gamal commitment scheme. What can go wrong if the prover uses a computationally binding and perfectly hiding commitment scheme, like the Pedersen commitment scheme?

   - Common input: A simple 3-colorable graph $G = (V, E)$ where $|V| = n$ and $V = \{1, 2, \ldots, n\}$
   - Prover has a 3-coloring of G given by $\psi : V \to \{1, 2, 3\}$ such that $\psi(u) \neq \psi(v)$ for all $(u, v) \in E$
   - Interactive proof
     1. Prover selects a random permutation $\pi : \{1, 2, 3\} \to \{1, 2, 3\}$ and sets $\phi(v) = \pi(\psi(v))$
     2. Prover computes commitments $c_v = \texttt{com}(\phi(v))$ for all $v \in V$ and sends $c_1, c_2, \ldots, c_n$ to verifier
     3. Verifier selects an edge $(u, v) \in E$ and sends it to prover
     4. Prover opens the commitments of the colors $\phi(u)$ and $\phi(v)$
     5. Verifier checks commitment openings and if $\phi(u) \neq \phi(v)$

3. (4 points) Let G be a cyclic group of prime order p with a non-degenerate bilinear pairing $e : G \times G \mapsto G_T$ and $G = \langle g \rangle$. Suppose the q-power knowledge of exponent assumption holds in G.

   - Bob chooses s randomly from $\mathbb{F}_p^*$ and sends $g, g^s, g^{s^2}, \ldots, g^{s^q}$ to Alice.
   - For a polynomial $f(x) = \sum_{i=0}^d f_i x^i$ with $f_i \in \mathbb{F}_p$ known only to Alice, she computes

$$u = g^{f(s)} = \prod_{i=0}^{d} \left(g^{s^i} \right)^{f_i}$$

     and sends u to Bob. Assume $d \leq q$.
   - Alice wants to convince Bob that u is of the form $g^{f(s)}$ where $f(x)$ is a polynomial which has remainder $r(x)$ when divided by a polynomial $t(x)$. The polynomials $r(x)$ and $t(x)$ are public while Alice wants to keep $f(x)$ secret.

   Describe a procedure using pairings that Alice can use to convince Bob. Specify what further information does Alice need from Bob to execute the procedure.