above to show that h has order n. Conclude that G is cyclic, conclusion (a) of the lemma.

Question 25. (*Roots of polynomials*)
Suppose K is a field, and suppose

$$P \in K[X], \quad P(X) = X^m + a_{m-1}X^{m-1} + \cdots + a_0$$

is a monic polynomial of degree m with coefficients in K.
25.1 Suppose $b \in K$. Show that the Euclidean division of the polynomial P by the polynomial $(X - b)$ gives an expression of the form

$$P(X) = (X - b) \cdot Q(X) + R$$

where $Q(X) = X^{m-1} + c_{m-2}X^{m-2} + \ldots + c_0$ is a monic polynomial of degree $m - 1$, and $R \in K$. Can you write out explicitly some of the coefficients of c_j of Q?
25.2 In the above expression, show by plugging in the value $X = b$, that $R = P(b)$.
25.3 Conclude the following fact: if $r \in K$ is a root of the polynomial, that is to say $P(r) = 0$, then P factors as

$$P(X) = (X - r) \cdot Q(X).$$

25.4 Use the above to prove by induction on the degree m of the polynomial P, that the number of distinct roots $r_1, \ldots, r_d$ of P is $\leq m$.

Question 26. (*Finite Fields — II: Fermat's Little Theorem*)
Suppose K is a finite field. Let q be the number of elements of k. We have seen in Question 21 that $q = p^k$ for a prime number p called the *characteristic* of F. Let $K^\times$ denote the set of nonzero elements of K, with the group operation $\times$. This is called the *multiplicative group* of K. Note that it has order $q - 1$ because the element 0 was removed. Here we are going to prove: **Fermat's Little Theorem:** *The multiplicative group is cyclic:* $K^\times \cong \mathbb{Z}/(q-1)\mathbb{Z}$.

We should just be careful that the group operation of $K^\times$ is $\times$, hence written multiplicatively. In particular, iterating the operation on an element itself is written as a power:

$$a^k := a \cdot a \cdots a \quad (k \text{ times }).$$

This is the same as the power in the field K.
26.1 State the general property of orders of elements in a finite group, that tells us that for any element $a \in K^*$ we have

$$a^{(q-1)} = 1.$$