1. Let $U_{12}$ be the group of units in the ring $\mathbb{Z}_{12}$. Is the group $U_{12}$ cyclic? Justify your answer.

**Solution.** The group $U_{12}$ has four elements: 1, 5, 7, 11. By direct computation the square of each element is 1. But a cyclic group of order 4 must have an element of order 4. Hence the group is not cyclic.

2. a) Show that the group $\mathbb{Z}_{12}$ is not isomorphic to the group $\mathbb{Z}_2 \times \mathbb{Z}_6$.
   b) Show that the group $\mathbb{Z}_{12}$ is isomorphic to the group $\mathbb{Z}_3 \times \mathbb{Z}_4$.

**Solution.**
   a) The element 1 $\in \mathbb{Z}_{12}$ has order 12. Every element $(a, b) \in \mathbb{Z}_2 \times \mathbb{Z}_6$ satisfies the equation $6 (a, b) = (0, 0)$. Hence the order of any element in $\mathbb{Z}_2 \times \mathbb{Z}_6$ is at most 6, and the groups can not be isomorphic.
   b) It is sufficient to show that $\mathbb{Z}_3 \times \mathbb{Z}_4$ is cyclic. Indeed $(1, 1) \in \mathbb{Z}_3 \times \mathbb{Z}_4$ has order 12, because $n (1, 1) = (n, n) = (0, 0)$ implies $4 \big| n$, $3 \big| n$ and therefore $12 \big| n$.

   In fact, the more general statement is true. $\mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$ if and only if $(p, q) = 1$ (that was proven in class).

3. Let $R = \mathbb{Z}_5 [x] / (x^2)$. Let $U (R)$ denote the group of units of $R$.
   a) Find the order of $U (R)$.
   b) List all ideals in $R$.
   c) (extra credit) Is $U (R)$ cyclic?

**Solution.**
   a) An element of $R$ can be written uniquely as $[ax + b]$ with $a, b \in \mathbb{Z}_5$. Furthermore, $[ax + b]$ is a unit if and only if $(ax + b, x^2) = 1$. That implies $x$ does not divide $ax + b$, hence $b \neq 0$. Thus, $[ax + b]$ is a unit if and only if $b \neq 0$. There are 5 choices for $a$ and 4 choices for $b$. Therefore $|U (R)| = 20$.
   b) Every ideal in $R$ is principal, since $R$ is a quotient of the polynomial ring. If $r \in R$ is a unit, the ideal generated by $r$ coincides with $R$. All non-zero non-units of $R$ are of the form $[ax]$ with $a \neq 0$. Clearly they generate the same ideal ($[x]$). Thus, $R$ has 3 ideals: $\{0\}, ([x])$ and $R$.
   c) Yes, $U (R)$ is cyclic. To show this, it is sufficient to find an element of order 20. Note that $[2]$ has order 4, and $[x + 1]$ has order 5. As we have shown in class, the order of the product $[2] [x + 1] = [2x + 2]$ is 20.

4. Determine which of the following quotient rings are fields. Explain your answer.
   a) $\mathbb{Z}_3 [x] / (x^3 + x + 1)$;
   b) $\mathbb{Z}_2 [x] / (x^3 + x + 1)$;
   c) $\mathbb{R} [x] / (x^3 + x + 1)$.
Solution. We have to figure out when the polynomial is irreducible. Note that $x^3 + x + 1$ is reducible over $\mathbb{Z}_3$, because 1 is a root, and over $\mathbb{R}$ as any polynomial of degree $\geq 2$. Hence in (a) and (c) the quotient ring is not a field. On the other hand, $x^3 + x + 1$ is irreducible over $\mathbb{Z}_2$, since it does not have roots in $\mathbb{Z}_2$. Therefore in (b) the quotient ring is a field.