1. The order of $\alpha$ must divide $2^9 - 1 = 511$. Hence it is either 7, 73, or 511. Clearly $o(\alpha) \neq 7$, since otherwise $\alpha$ is a root of $x^2 + 1$ which contradicts the fact that its minimal polynomial has degree 9. On the other hand $\alpha^9 = \alpha + 1$, so that $\alpha^{72} = (\alpha + 1)^8 = \alpha^8 + 1$, and thus $\alpha^{73} = \alpha^9 + \alpha = 1$. Hence $o(\alpha) = 73$.

2. (a) If $f(x) = x^3 + x^2 + 2$ is not irreducible, it must have at least one linear factor. But, since $f(0), f(1),$ and $f(2)$ are all nonzero, none of $x, x-1,$ and $x-2$ is a factor of $f(x)$. Hence $f(x)$ is irreducible over $GF(3)$. Note, however, that this approach does not apply to polynomials of degree greater than three.

(b) $(2\alpha + 1)(\alpha^2 + 2) = 2\alpha^3 + \alpha^2 + \alpha + 2 = \alpha^3 + \alpha = 2\alpha^2 + \alpha + 1$.

(c) The possible multiplicative orders are all the divisors of 26, namely 1, 2, 13, and 26.

(d) Since clearly $\alpha^2 \neq 1$, the order of $\alpha$ must be either 13 or 26. Since $\alpha^3 + \alpha^2 + 2 = 0$ in the field, we deduce that $\alpha^3 = 2\alpha^2 + 1$ and $\alpha^4 = 2\alpha^3 + \alpha = 2(2\alpha^2 + 1) + \alpha = \alpha^2 + 2 + \alpha$. Also, since $\alpha(\alpha^2 + \alpha) = \alpha^3 + \alpha^2 = 1$, we conclude that $(\alpha^2 + \alpha) = \alpha^{-1}$. Now
\[
\alpha^{12} = (\alpha^4)^3 = (\alpha^2 + \alpha + 2)^3 = \alpha^6 + \alpha^3 + 2 = (2\alpha^2 + 1)^2 + (2\alpha^2 + 1) + 2 = \alpha^4 + \alpha^2 + 1 + 2\alpha^2 = \alpha^4 + 1 = \alpha^2 + \alpha + 2 + 1 = \alpha^2 + \alpha = \alpha^{-1}.
\]
It follows that $\alpha^{13} = \alpha^{12} = \alpha\alpha^{-1} = 1$, and therefore $o(\alpha) = 13$.

3. (a) If $\gamma^p = \beta$ then $\gamma$ and $\beta$ must have the same minimal polynomial. In other words, $\gamma$ must be a conjugate of $\beta$ which implies that $\gamma$ belongs to \{ $\beta, \beta^p, \beta^{p^2}, \ldots, \beta^{p^{r-1}}$ \}, where $r$ is the smallest integer such that $\beta^{p^r} = \beta$ (such an integer necessarily exists since $\beta^{p^m} = \beta$ for all $\beta$ in the field). The only element $\gamma$ in the above set which satisfies $\gamma^p = \beta$ is $\gamma = \beta^{p^{r-1}}$.

(b) Clearly 1 and $-1$ are the square roots of 1 in any field. In a field of characteristic two, we have $-1 = 1$. Furthermore, by part (a), square roots are unique in such a field and hence 1 is the only square root of 1. Now let $\alpha$ be a primitive element in $GF(p^m)$, where the characteristic $p$ is odd. Then $\alpha^{(p^m - 1)/2}$ is well-defined and is the second square root of 1. This implies, in particular, that in a field of odd characteristic $-1 = \alpha^{(p^m - 1)/2}$.

(c) Let $q = p^m$ be the order of the field, where $p$ is odd. From part (b), we have
\[
(\alpha\beta)^{(q-1)/2} = \alpha^{(q-1)/2} \beta^{(q-1)/2} = (-1)(-1) = 1
\]
Hence the order of $\alpha\beta$ is a divisor of $(q-1)/2$, and thus $\alpha\beta$ cannot be primitive in $GF(q)$.

(d) Take for instance $\beta = \alpha$ in $GF(2^m)$. Then $\alpha\beta = \alpha^2$ is a conjugate of $\alpha$ and is therefore primitive. Another option is to consider a field $GF(2^m)$ such that $2^m - 1$ is prime (for instance $2^3, 2^5,$ or $2^7$) in which every element, except 0 and 1, is primitive.

4. The polynomial $f(x) = x^2 + x + 1$ is the only irreducible polynomial of degree 2 over $GF(2)$. Using this polynomial to construct $GF(4) = \{0, 1, \alpha, \alpha^2\}$ as a set of 2-tuples over $GF(2)$, we obtain the following table:

<table>
<thead>
<tr>
<th>$x$</th>
<th>$0$</th>
<th>$0$</th>
<th>$00$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\alpha^0$</td>
<td>1</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>$\alpha^1$</td>
<td>$\alpha$</td>
<td>01</td>
<td></td>
</tr>
<tr>
<td>$\alpha^2$</td>
<td>$1 + \alpha$</td>
<td>11</td>
<td></td>
</tr>
</tbody>
</table>

One choice of a polynomial of degree 2 which is irreducible over $GF(4)$ is $p(x) = x^2 + x + \alpha$. There are several other choices. To see that $p(x)$ it is indeed irreducible, note that $p(0) = \alpha$,
\[ p(1) = \alpha, \ p(\alpha) = \alpha^2, \text{ and } p(\alpha^2) = \alpha^2. \] Hence \( p(x) \) has no roots in \( \text{GF}(4) \), and thus no linear factors. Using this polynomial to construct \( \text{GF}(16) \) as a set of 2-tuples over \( \text{GF}(4) \), we obtain:

\[
\begin{array}{ccc}
0 & 0 & 0 \\
\beta^0 & 1 & 0 \\
\beta^1 & \beta & 0 \\
\beta^2 & \beta + \alpha & \alpha \\
\beta^3 & \alpha^2 \beta + \alpha & \alpha^2 \\
\beta^4 & \beta + 1 & 1 \\
\beta^5 & \alpha & 0 \\
\beta^6 & \alpha \beta & 0 \\
\beta^7 & \alpha \beta + \alpha^2 & \alpha^2 \\
\beta^8 & \beta + \alpha^2 & \alpha^2 \\
\beta^9 & \alpha \beta + \alpha & \alpha \\
\beta^{10} & \alpha^2 & \alpha^2 \\
\beta^{11} & \alpha^2 \beta & 0 \\
\beta^{12} & \alpha^2 \beta + 1 & 1 \\
\beta^{13} & \alpha \beta + 1 & 1 \\
\beta^{14} & \alpha^2 \beta + \alpha^2 & \alpha^2 \\
\end{array}
\]

where \( \beta \) is the root of \( p(x) \), and \( \beta^{15} = \beta(\alpha^2 + \alpha^2 \beta) = \alpha^2 \beta + \alpha^2(\beta + \alpha) = \alpha^3 = 1 \).

5. (a) We have \( x^5 - 1 = (x - 1)f(x) \). Hence if \( \alpha \) is a root of \( f(x) \) it is also a root of \( x^5 - 1 \), and therefore \( o(\alpha) = 5 \). Thus \( \alpha \) cannot be primitive in \( \text{GF}(16) \).
(b) The order of any element in \( \text{GF}(16) \), except 0 and 1, is either 3, 5 or 15. It is clear that \( (\alpha + 1)^3 - 1 \neq 0 \), since the minimal polynomial of \( \alpha \) is of degree 4. Furthermore,

\[
(\alpha + 1)^5 - 1 = (\alpha + 1)(\alpha + 1)^4 - 1 = (\alpha + 1)(\alpha^4 + 1) - 1
\]

\[
= \alpha^5 + \alpha^4 + \alpha = \alpha(\alpha^4 + \alpha^3 + 1) = \alpha(\alpha^2 + \alpha) = \alpha^3 + \alpha^2 \neq 0
\]

in the field at hand. Hence \( o(\alpha + 1) \neq 5 \) and \( o(\alpha + 1) \neq 5 \), which implies \( o(\alpha + 1) = 15 \).
(c) Since \( (\alpha + 1) \) is a primitive element of \( \text{GF}(16) \) its minimal polynomial \( g(x) \) has to be an irreducible primitive polynomial of degree 4. Furthermore, we have \( g(\alpha + 1) = 0 = f(\alpha) \). Thus \( g(\alpha + 1) = \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1 = 0 \). Let \( \beta = \alpha + 1 \), so that \( \alpha = \beta + 1 \). Then,

\[
g(\beta) = (\beta + 1)^4 + (\beta + 1)^3 + (\beta + 1)^2 + (\beta + 1) + 1
\]

\[
= \beta^4 + 1 + (\beta + 1)(\beta^2 + 1) + \beta^2 + 1 + \beta + 1 + 1
\]

\[
= \beta^4 + \beta^3 + 1
\]

Hence \( g(x) = x^4 + x^3 + 1 \). This is an example of a general method which can be used to obtain a primitive irreducible polynomial from a non-primitive irreducible polynomial.
(d) A typical element of \( \text{GF}(2)[x]/f(x) \) is given by \( a_3 \alpha^3 + a_2 \alpha^2 + a_1 \alpha + a_0 \) while a typical element of \( \text{GF}(2)[x]/g(x) \) is given by \( b_3 \beta^3 + b_2 \beta^2 + b_1 \beta + b_0 \), where \( a_i, b_i \in \text{GF}(2) \) and \( \beta = \alpha + 1 \). Using the latter relation, we find that \( \gamma = (b_0, b_1, b_2, b_3) \in \text{GF}(2)[x]/g(x) \) may be expressed as

\[
\gamma = b_3(\alpha + 1)^3 + b_2(\alpha + 1)^2 + b_1(\alpha + 1) + b_0
\]

\[
= b_3(\alpha^3 + \alpha^2 + \alpha + 1) + b_2(\alpha^2 + 1) + b_1(\alpha + 1) + b_0
\]

\[
= b_3 \alpha^3 + (b_3 + b_2) \alpha^2 + (b_3 + b_1) \alpha + (b_3 + b_2 + b_1 + b_0)
\]

Thus the isomorphism \( \phi : \text{GF}(2)[x]/g(x) \rightarrow \text{GF}(2)[x]/f(x) \) maps a \( \gamma = (b_0, b_1, b_2, b_3) \) into \( \phi(\gamma) = (b_3 + b_2 + b_1 + b_0, b_3 + b_1, b_3 + b_2, b_3) \in \text{GF}(2)[x]/f(x) \).
6. (a) In $\text{GF}(2)$ we have $x^6 - 1 = (x^3 + 1)^2 = (x + 1)^2(x^2 + x + 1)^2$. Thus the factorization of $x^6 - 1$ contains two irreducible factors, each of multiplicity 2. It follows that any monic divisor of $x^6 - 1$ over $\text{GF}(2)$ has the form $(x + 1)^i(x^2 + x + 1)^j$, where $i, j \in \{0, 1, 2\}$. This gives $3^2 = 9$ monic divisors, including the trivial ones 1 and $x^6 - 1$.

(b) Over $\text{GF}(3)$ we have $x^6 - 1 = (x^2 - 1)^3 = (x + 1)^3(x - 1)^3$, and the number of monic divisors is $4^2 = 16$.

7. Let $l = |C_i|$. Then $l$ is the smallest integer, such that $\beta^p = \beta$, and the cyclotomic conjugates of $\beta = \alpha^l$ are given by

$$C_\beta = \{ \alpha^j : j \in C_i \} = \{ \beta, \beta^p, \beta^{p^2}, \ldots, \beta^{p^{l-1}} \}$$

All these elements are roots of $M_\beta(x)$, and hence $\deg M_\beta(x) \geq l$. Now denote

$$A(x) = \prod_{j \in C_i} (x - \alpha^j) = \prod_{j=0}^{l-1} (x - \beta^j) = \sum_{k=0}^{l} a_k x^k$$

Then clearly $A(\beta) = 0$ and $\deg A(x) = l$. Since $M_\beta(x)$ is the unique polynomial of minimal degree with coefficients in $\text{GF}(p)$ having $\beta$ as a root, it would suffice to show that the coefficients of $A(x)$ are in $\text{GF}(p)$ in order to prove that $M_\beta(x) = A(x)$. The coefficients $a_0, a_1, \ldots, a_l$ of $A(x)$ are elementary symmetric functions of the elements of $C_\beta$, given by

$$a_0 = (-1)^l \beta \beta^p \beta^{p^2} \cdots \beta^{p^{l-1}}$$
$$a_1 = (-1)^{l-1} \left( \beta \beta^p \beta^{p^2} \cdots \beta^{p^{l-1}} + \beta \beta^{p^2} \beta^{p^3} \cdots \beta^{p^{l-1}} + \cdots + \beta \beta^{p^{l-2}} \beta^{p^{l-1}} \right)$$
$$\vdots$$
$$a_{l-2} = \beta \beta^p + \beta \beta^{p^2} + \cdots + \beta \beta^{p^{l-1}} + \beta^p \beta^2 + \beta^p \beta^3 + \cdots + \beta^p \beta^{p^{l-1}} + \cdots + \beta^{p^{l-2}} \beta^{p^{l-1}}$$
$$a_{l-1} = - \left( \beta + \beta^p + \beta^{p^2} + \cdots + \beta^{p^{l-1}} \right)$$
$$a_l = 1$$

We need to show that $a_i \in \text{GF}(p)$, or equivalently $\alpha_i^p = a_i$, for all $i = 0, 1, \ldots, l$. We may as well consider $\tilde{a}_i = a_i / (-1)^{l-1}$, since clearly $a_i = \pm \tilde{a}_i$ and $a_i \in \text{GF}(p)$ if $\tilde{a}_i \in \text{GF}(p)$. In general, $\tilde{a}_i$ is the sum of all the possible products of $l - i$ elements from the set $C_\beta$. Now, since $(x + y)^p = x^p + y^p$ in $\text{GF}(p^m)$, we observe that $\tilde{a}_i^p$ is still a sum of the same number of terms, and these terms are products of $l - i$ elements from $C_\beta$ raised to the $p$-th power. Since $\beta^p = \beta$, the $p$-th power of a product of $l - i$ elements of $C_\beta$ is still a product of $l - i$ elements of $C_\beta$. Furthermore, the set of all such products is clearly invariant under the operation of raising to the $p$-th power (this is equivalent to adding 1 modulo $l$ to the set of integers $\{0, 1, \ldots, l - 1\}$). It follows that $\tilde{a}_i^p = \tilde{a}_i$ and $\tilde{a}_i, a_i \in \text{GF}(p)$ for all $i$. 