1) Prove that if \( f \in \mathbb{Z}[x] \) is primitive and \( g \in \mathbb{Z}[x] \) divides \( f \) in \( \mathbb{Z}[x] \), then either \( g \) or \( -g \) is also primitive.

Proof. Let \( f = g \cdot q \), where \( q \in \mathbb{Q}[x] \). Write, \( g = c \cdot g_0, \ q = d \cdot q_0 \), where \( c, d \in \mathbb{Q} \) and \( g_0, q_0 \) are primitive. [So, \( c \) and \( d \) are the content of \( g \) and \( q \) respectively.] Since, \( g, q \in \mathbb{Z}[x] \), we have that \( c, d \in \mathbb{Z} \).

By Gauss’s Lemma, \( g_0 \cdot q_0 \) is primitive, and then, since \( f = g \cdot q = (cd) \cdot (g_0 \cdot q_0) \), by the unique representation of a polynomial with rational coefficients as a rational number times a primitive polynomial, and since \( f \) is primitive, we have that \( cd = 1 \). So, since \( c, d \in \mathbb{Z} \), we have that \( c = \pm 1 \) [and \( d = c \)]. Hence \( g = g_0 \), and \( g \) is primitive, or \( g = -g_0 \), and \( -g \) is primitive.

\( \square \)
2) Find whether or not the following polynomials are irreducible over \( \mathbb{Q}[x] \).

(a) \( f_1(x) = x^4 + x^3 + x - 6 \)

\textit{Solution.} Look for rational roots. The possibilities are \( \pm 1, \pm 2, \pm 3, \pm 6 \). We have that \( f_1(-2) = 0 \). Hence \( (x + 2) \) divides \( f_1 \), and so \( f_1 \) is \textit{not} irreducible.

(b) \( f_2(x) = x^6 - 2x^5 + 14x^2 - 8x + 34 \)

\textit{Solution.} Applying the Eisenstein’s Criterion with \( p = 2 \), we see that \( f_2 \) is \textit{irreducible}.

(c) \( f_3(x) = 100x^3 - x + 2008 \)

\textit{Solution.} Reducing modulo 3, we get \( \bar{f}_3(x) = x^3 + 2x + 2 \). If this polynomial is reducible in \( \mathbb{F}_3[x] \), it must have a root. But \( \bar{f}_3(0) = \bar{f}_3(1) = \bar{f}_3(2) = 2 \). Hence it has no roots and \( \bar{f}_3 \) is irreducible in \( \mathbb{F}_3[x] \). Therefore \( f_3 \) is \textit{irreducible} in \( \mathbb{Q}[x] \).

(d) \( f_4(x) = x^4 + x^3 + x^2 + x + 1 \)

\textit{Solution.} This is \( \phi_5 \), the \textit{cyclotomic polynomial} for the prime 5. Hence, it is \textit{irreducible}. [You can prove it by applying the Eisenstein’s Criterion to \( f_4(x + 1) \) with \( p = 5 \).]
3) Let $F$ be a field. We say that $\alpha \in F$ is a multiple root of $f(x) \in F[x]$ if $f(x) = (x - \alpha)^2 \cdot g(x)$, for some $g \in F[x]$.

(a) Prove that if $\alpha$ is a multiple root of $f$, then $f(\alpha) = f'(\alpha) = 0$, where $f'(x)$ is the derivative of $f(x)$ [as in calculus]. [Note that all calculus formulas for derivatives hold for polynomials.]

Proof. Since $\alpha$ is a multiple root of $f$, write $f(x) = (x - \alpha)^2 g(x)$. We then have:

$$f'(x) = \frac{d}{dx} (x - \alpha)^2 g(x) = 2(x - \alpha)g(x) + (x - \alpha)^2 g'(x).$$

Hence $f'(\alpha) = 2(\alpha - \alpha)g(\alpha) + (\alpha - \alpha)^2 g(\alpha) = 0$.  

(b) Prove that if $f(x) \in F[x]$ is irreducible, then $f(x)$ has no multiple roots in any extension of $F$, as long as $f'(x) \neq 0$. [Hint: What’s the greatest common divisor of $f(x)$ and $f'(x)$?]

Proof. Since $f(x)$ is irreducible, we have that if $g(x)$ divides $f(x)$, then $g$ is a [non-zero] constant or it is associated to $f$.

Let then $g$ be a common divisor of $f$ and $f'$. If $g$ is an associate of $f$, it has the same degree as $f$, and so $g$ cannot divide $f'$, since $\deg f' < \deg f = \deg g$ and $f'(x) \neq 0$. [If we have that $f' = g \cdot q$, then $\deg f' = \deg g + \deg q$. So, if $f' \neq 0$, then $\deg g \leq \deg f'$, which is a contradiction. But notice that if $f' = 0$, then $f' = 0 \cdot g$, and so $g | f'$]

So, since $g$ cannot be an associate of $f$, it has to be a constant [i.e., a unit] and $\gcd(f, f') = 1$.

So, by Bezout’s Theorem, there are $r, s \in F[x]$ such that

$$r(x)f(x) + s(x)f'(x) = 1.$$ 

If $\alpha$ is a multiple root of $f(x)$, by (a) it is also a root of $f'(x)$. Then, plugging $x = \alpha$ in the equation above would give us $0 = 1$, a contradiction. Hence, $f$ has no multiple roots.

[Note: Let $f \overset{\text{def}}{=} x^2 + t^2 \in \mathbb{F}_2(t^2)[x]$. Then, $f$ has no roots in $\mathbb{F}_2(t^2)$, since $f = (x + t)^2$ [we are in characteristic 2], and so the only root is $t \notin \mathbb{F}_2(t^2)$. Since $f$ has degree 2 and no roots in $\mathbb{F}_2(t^2)$, it is irreducible in $\mathbb{F}_2(t^2)[x]$.

But, in the extension $\mathbb{F}_2(t)$, $f$ does have multiple roots, namely, $t$ is a double root. But, as you can expect from the statement, we have $f' = 2x = 0$.]
4) Let $R$ be a UFD and let $P$ be a non-zero *prime* ideal of $R$ such that if $P'$ is another prime ideal, with $(0) \subseteq P' \subseteq P$, then $P' = P$. Prove that $P$ is principal.

**Proof.** Since $P \neq (0)$, there is $a \in P$, with $a \neq 0$. If $a$ is a unit, then $P = R$, and $P$ would not be prime. [$R = (1)$ is not prime by definition.] Since $R$ is a UFD, we can write $a = p_1 \cdots p_k$, where the $p_i$ are primes [and irreducible]. Since $P$ is a prime ideal, and $a = p_1 \cdots p_k \in P$, we have $p_i \in P$ for some $i \in \{1, \ldots, k\}$.

So, $(0) \subseteq (p_i) \subseteq P$. Since $p_i$ is prime, the ideal $(p_i)$ is also prime. [We have seen that in class, but it is easy to see: $ab \in (p_i)$ iff $p_i \mid ab$ iff $p_i \mid a$ or $p_i \mid b$ [definition of prime element] iff $a \in (p_i)$ or $b \in (p_i)$.]

Hence, by hypothesis, $(p_i) = P$, and $P$ is principal. 

\[\square\]
5) Maximal ideals of polynomial rings with complex coefficients.

(a) Prove that if \( I \) is an ideal of \( \mathbb{C}[x, y] \) and \( M \) is a maximal ideal containing \( I \), then there is a point \((a, b)\) such that for all \( f(x, y) \in I \), we have \( f(a, b) = 0 \).

[Observation: This statement is also true for \( n \) variables (with an analogous solution).]

**Proof.** By the Nullstellensatz, \( M = (x - a, y - b) \) for some \( a, b \in \mathbb{C} \). Since \( I \subseteq M \), for all \( f \in I \), there are \( f_1, f_2 \in \mathbb{C}[x, y] \) such that

\[
  f(x, y) = (x - a)f_1(x, y) + (y - b)f_2(x, y).
\]

But then, \( f(a, b) = 0 \).

(b) Let \( I = (3x - y - 2, y - x^2) \) be an ideal of \( \mathbb{C}[x, y] \). Find all maximal ideals of \( \mathbb{C}[x, y] \) that contain \( I \).

**Solution.** By (a), if \( I \subseteq M = (x - a, y - b) \), then every polynomial in \( I \) must vanish at \((a, b)\), in particular, \((a, b)\) must be a common zero of \( 3x - y - 2 \) and \( y - x^2 \). So, we just need to solve the system:

\[
\begin{align*}
  3x - y - 2 &= 0 \\
  y - x^2 &= 0
\end{align*}
\]

Solving we find only two points: \((1, 1)\) and \((2, 4)\).

So, there are only two possible maximal ideals that *might* contain \( I \): \((x - 1, y - 1)\) and \((x - 2, y - 4)\). Now, if \( f(x, y) \in I \), we have that

\[
  f(x, y) = (3x - y - 2)f_1(x, y) + (y - x^2)f_2(x, y),
\]

and thus \( f(1, 1) = f(2, 4) = 0 \). Hence, indeed \( I \) is indeed contained in those maximal ideals. [Remember that \( f(x, y) \in (x - x_0, y - y_0) \) iff \( f(x_0, y_0) = 0 \). We used Taylor expansions around \((x_0, y_0)\) to prove that.]