Question 1

Let $F[x]$ be a polynomial ring over a field F and let $f(x) \in F[x]$. Show that the ideal generated by $f(x)$ is maximal if and only if $f(x)$ is irreducible.

Solution:
($\Longrightarrow$):

If $(f(x))$ is a maximal ideal, then it is also a prime ideal, which means $f(x)$ is prime. Therefore, $f(x)$ is irreducible.

($\Longleftarrow$):

Because F is a field, $F[x]$ is a PID, so if $f(x)$ is irreducible, then $f(x)$ is prime. This means that $(f(x))$ is a prime ideal. But as $F[x]$ is a PID, a prime ideal is a maximal ideal.

Question 2

Prove that $(x^n - 1)/(x - 1)$ is irreducible in $\mathbb{Z}[x]$ if and only if n is a prime integer.

Solution: Firstly, notice that

$$\frac{x^n - 1}{x - 1} = x^{n-1} + x^{n-2} + x^{n-3} + \cdots + 1$$

and that $(\mathbb{Z}[x])^\times = \{\pm 1\}$
($\Longrightarrow$):

The proof use contraposition. For $n = 1$, $(x^n - 1)/(x - 1) = 1$ is a unit. Thus, it is not irreducible.

If $n \neq 1$ is not a prime integer, then let $ab = n$ for some integer a, b which is not 1. Then

$$(x^{a-1} + x^{a-2} + \cdots + 1)(x^{(b-1)a} + x^{(b-2)a} + \cdots + 1) = (x^{n-1} + \cdots + 1)$$

Since both are not a unit, then the polynomial is not irreducible.

($\Longleftarrow$):

Let n be prime. Since

$$\begin{aligned}\frac{x^n - 1}{x - 1} &= \frac{((x-1)+1)^n - 1}{x - 1} \\ &= \frac{(x-1)^n + \binom{n}{n-1}(x-1)^{n-1} + \cdots + \binom{n}{0}1 - 1}{x - 1} \\ &= (x-1)^{n-1} + \binom{n}{n-1}(x-1)^{n-1} + \cdots + \binom{n}{1}\end{aligned}$$

Then, as $n \mid \binom{n}{i}$ for all $1 \leq i \leq n-1$ and $n^2 \nmid \binom{n}{1}$, the eisenstein criterion applies. So, $\frac{x^n-1}{x-1}$ is irreducible in $\mathbb{Q}[x-1]$, thus it is irreducible in $\mathbb{Q}[x]$. Moreover, as $\frac{x^n-1}{x-1} = x^{n-1} + x^{n-2} + \cdots + 1$, then it is monic, thus primitive. So, $\frac{x^n-1}{x-1}$ is irreducible in $\mathbb{Z}[x]$.

Question 3

Let R be a UFD and let $f \in R[x]$ be a primitive polynomial. Show that if a non-constant polynomial g divides f, then g is also primitive.

Solution: If $g \mid f$, then there is some polynomial h such that $gh = f$. So, as f is primitive, then $C(g)C(h) = R$. Now, assume that g is not primitive, then $C(g) = aR$ for some $a \notin R^\times$. But $aRC(h) = R$ is not possible as $1 \notin aRC(h)$ no matter what polynomial is h. Thus, by contradiction, g must be primitive.

Question 4

Show that $x^4 + yx + 5y + 2y^2x^2 \in \mathbb{C}[x, y]$ is irreducible.

Solution: Notice that y is irreducible in the field $\mathbb{C}[y]$ because if $y = ab$ for some $a, b \in \mathbb{C}[y]$. It must be the case that $\deg y = \deg a + \deg b$. But since degree is non-negative, $\deg a = 0$ without loss of generality. Then, $a \neq 0$, otherwise $y = ab = 0$. So $a \in \mathbb{C} - \{0\} = \mathbb{C}^\times$.

Rewriting the polynomial gives $f = x^4 + (2y^2)x^2 + (y)x + (5y) \in \mathbb{C}[y][x]$. Then, $y \in \mathbb{C}[y]$ is irreducible such that $y \mid 5y$, $y \mid y$, $y \mid 2y^2$, $y \nmid 1$, and $y^2 \nmid 5y$. Therefore, by the eisenstein criterion, f is irreducible over $(\mathbb{C}[x,y] - \{0\})^{-1}\mathbb{C}[x,y]$, which is the quotient field of $\mathbb{C}[x,y]$. However, as f is monic, it is primitive. Therefore, f is also irreducible in $\mathbb{C}[x,y]$ since it is primitive and irreducible in the quotient field.

Question 5

Let $f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Q}[x]$. Let f' denote the derivative of f, i.e., $f' = a_n n x^{n-1} + a_{n-1}(n-1)x^{n-2} + \cdots + a_1$. Show that f is divisible by the square of a non-constant polynomial in $\mathbb{Q}[x]$ if and only if f and f' are not relatively prime.

Solution: Since $\mathbb{Q}$ is a field, then $\mathbb{Q}[x]$ is a PID and UFD.
($\Longrightarrow$):

If f is divisible by a square of non-constant polynomial, g^2. Then $f = g^2 h$ for some h. Now, by the product rule of derivative, $f' = (g^2)'h + g^2 h' = 2gg'h + g^2 h' = g(2g'h + gh')$. Therefore, a non-constant, which means non-unit g divides both f and f'. Thus, f and f' is not-relatively prime.

Note that if g is constant, then g^2 is constant, which is not the case, so g is non-constant.

($\Longleftarrow$):

If f and f' is not relatively prime, then let g be an irreducible, thus non-constant polynomial such that $g \mid f$ and $g \mid f'$. Then, as $g \mid f$, let $f = gh$ for some polynomial h. So, $f' = gh' + g'h$ by the product rule. However, as $g \mid f$ and $g \mid gh'$, it must be the case that $g \mid g'h$. But $g \nmid g'$ since $\deg g > \deg g'$. But since $\mathbb{Q}[x]$ is a PID, then g is prime, which means that $g \mid h$.

Now, since $g \mid h$, then $h = gr$ for some polynomial r. This means that $f = gh = ggr$. Therefore, f is divisible by a square for non-constant polynomial.

Question 6

Let E/F be a field extension and let $a, b \in E$. Show that if $[F(a) : F]$ and $[F(b) : F]$ are relatively prime, then $[F(a,b) : F] = [F(a) : F][F(b) : F]$

Solution: If a or b is transcendental, then $[F(a,b) : F]$ is not finite, and either $[F(a) : F]$ or $[F(b) : F]$ is not finite, thus, $[F(a,b) : F] = [F(a) : F][F(b) : F]$.

Now, consider the case where both a, b are algebraic element over F.

Since $F(a,b) \simeq F[a,b] \simeq F[a][b] \simeq F(a)[b]$, then $F(a,b)$ is a field extension of $F(a)$. This means that

$$[F(a,b) : F] = [F(a,b) : F(a)][F(a) : F] = [F(a,b) : F(b)][F(b) : F]$$

But $[F(b) : F]$ divides $[F(a,b) : F] = [F(a,b) : F(a)][F(a) : F]$ while being relatively prime to $[F(a) : F]$ means that $[F(b) : F] \mid [F(a,b) : F(a)]$.

However, $[F(a,b) : F(a)] \leq [F(b), F]$ as if f is a minimal polynomial of b over F, then the minimal polynomial of b over $F(a)$ would divide f since $f(b) = 0$ over $F(a)$.

Therefore, $[F(a,b) : F(a)] = [F(b), F]$. Which means that $[F(a,b) : F] = [F(a,b), F(a)][F(a), F] = [F(a), F][F(b), F]$.

Question 7

Find the minimal polynomial of $\sqrt{p} + \sqrt{q}$ over $\mathbb{Q}$ where $p \neq q$ are prime integers. Show also that $\mathbb{Q}(\sqrt{p} + \sqrt{q}) = \mathbb{Q}(\sqrt{p}, \sqrt{q})$.

Solution: Let $x = \sqrt{p} + \sqrt{q}$, then $x^2 = p + 2\sqrt{pq} + q$. Now, $x^2 - (p+q) = 2\sqrt{pq}$, so

$$x^4 - 2(p+q)x^2 + (p+q)^2 = 4pq$$
$$x^4 - 2(p+q)x^2 + (p-q)^2 = 0$$

So, let $f = x^4 - 2(p+q)x^2 + (p-q)^2$, then $m_{\sqrt{p}+\sqrt{q},\mathbb{Q}} \mid f$. However, $x^4 - 2(p+q)x^2 + (p-q)^2$ does not factor in $\mathbb{Q}$ because it is factored as

$$(x^2 - (p+q) + 2\sqrt{pq})(x^2 - (p+q) - 2\sqrt{pq})$$

which is then factored as

$$(x - \sqrt{p+q-2\sqrt{pq}})(x + \sqrt{p+q-2\sqrt{pq}})(x - \sqrt{p+q+2\sqrt{pq}})(x + \sqrt{p+q+2\sqrt{pq}}) \in \mathbb{R}$$

But as $\mathbb{R}$ is an extension over $\mathbb{Q}$, and any combination of the factors resulting in a polynomial in $\mathbb{R}[x]$ but not in $\mathbb{Q}[x]$. The combination of the factors is in $\mathbb{Q}[x]$ only when all the factors are multiplied. This means that f is not a product of polynomial in $\mathbb{Q}[x]$, thus it is irreducible, thus, $m_{\sqrt{p}+\sqrt{q},\mathbb{Q}} = f$.

Now, consider that $\mathbb{Q}(\sqrt{p}+\sqrt{q}) \subset \mathbb{Q}(\sqrt{p},\sqrt{q})$ obviously because $r + s(\sqrt{p}+\sqrt{q})$ for any $r, s \in \mathbb{Q}$ is $r + s\sqrt{p} + s\sqrt{q}$, which is an element of $\mathbb{Q}(\sqrt{p},\sqrt{q})$.

Next, consider that $\sqrt{p}+\sqrt{q} \in \mathbb{Q}(\sqrt{p}+\sqrt{q})$. Since $(\sqrt{p}-\sqrt{q})(\sqrt{p}+\sqrt{q}) = p+q$. Then, $\sqrt{p}-\sqrt{q} = \frac{p+q}{\sqrt{p}+\sqrt{q}} \in \mathbb{Q}(\sqrt{p}+\sqrt{q})$ because it is a field (by closure of field). Therefore, $\sqrt{p} = 1/2((\sqrt{p}-\sqrt{q}) + (\sqrt{p}+\sqrt{q})) \in \mathbb{Q}(\sqrt{p}+\sqrt{q})$. Then, $\sqrt{p}$ and $\sqrt{q}$ is a member of $\mathbb{Q}(\sqrt{p}+\sqrt{q})$. Therefore, $\mathbb{Q}(\sqrt{p},\sqrt{q}) = \mathbb{Q}(\sqrt{p}+\sqrt{q})$

Question 8

Let m, n be natural numbers. Determine when two fields $\mathbb{Q}(\sqrt{n})$ and $\mathbb{Q}(\sqrt{m})$ are isomorphic.

Solution: Notice that if n and m are a square of integers, including zero and one, then $\sqrt{n}$ and $\sqrt{m}$ are integer, thus, $\sqrt{n}, \sqrt{m} \in \mathbb{Q}$. Therefore, $\mathbb{Q}(\sqrt{n}) \simeq \mathbb{Q}(\sqrt{m}) \simeq \mathbb{Q}$.

Otherwise $\sqrt{n}$ is algebraic in $\mathbb{R}/\mathbb{Q}$ as it is a root of polynomial $x^2 - n = 0$, which has degree 2. Since $\sqrt{n} \notin \mathbb{Q}$, then $x^2 - n$ is the minimal polynomial of $\sqrt{n}$. And $\mathbb{Q}(\sqrt{n})/\mathbb{Q}$ is a vector space of dimension 2, which means that $\{1, \sqrt{n}\}$ is a basis of the vector space as it is a linearly independent set.

If there is an isomorphism $\phi : \mathbb{Q}(\sqrt{n}) \simeq \mathbb{Q}(\sqrt{m})$, then $\phi(1) = 1$ as it is the mutiplicative identity in each field, but then $\phi(r) = r$ for every $r \in \mathbb{Q}$ as $\phi(r) = \phi(a/b) = \phi(a)\phi(b)^{-1}$ for $a, b \in \mathbb{Z}$ and $\phi(a) = \phi(1) + \cdots + \phi(1) = 1 + \cdots + 1 = a$ for any positive integer a. Moreover, $\phi(-a) = -\phi(a) = -a$ since $0 = \phi(0) = \phi(a-a) = \phi(a) + \phi(-a)$. Now, $\phi(\sqrt{n})\phi(\sqrt{n}) = \phi(n) = n$, thus, $\phi(\sqrt{n}) = \sqrt{n}$ or $\phi(\sqrt{n}) = -\sqrt{n}$ only.

Therefore, if $n = r^2 m$ for some $0 \neq r \in \mathbb{Q}$,

$$\mathbb{Q}(\sqrt{n}) = \{\, x + y\sqrt{n} \mid x, y \in \mathbb{Q} \,\} = \{\, x + ry\sqrt{n} \mid x, y \in \mathbb{Q} \,\} = \{\, x + y\sqrt{m} \mid x, y \in \mathbb{Q} \,\} = \mathbb{Q}(\sqrt{m})$$

Together with identity map, $\mathbb{Q}(\sqrt{n}) \simeq \mathbb{Q}(\sqrt{m})$

And if $n \neq r^2 m$ for any $0 \neq r \in \mathbb{Q}$, then $\sqrt{n} \in \mathbb{Q}(\sqrt{n})$ but $\sqrt{n} \notin \mathbb{Q}(\sqrt{m})$ since $\sqrt{n} \neq r\sqrt{m}$ for any r. So $-\sqrt{n} \notin \mathbb{Q}(\sqrt{m})$. Thus, there cannot be any isomorphism between $\mathbb{Q}(\sqrt{n})$ and $\mathbb{Q}(\sqrt{m})$.

To conclude, for $n \neq 0, m \neq 0$, $\mathbb{Q}(\sqrt{n}) \simeq \mathbb{Q}(\sqrt{m})$ if and only if $n = r^2 m$ for some $r \in \mathbb{Q}$, and $\mathbb{Q}(\sqrt{n}) \simeq \mathbb{Q}(\sqrt{0})$ if and only if $\mathbb{Q}(\sqrt{n}) \simeq \mathbb{Q}(\sqrt{1})$

Question 9

Let E/F be a field extension and let $a \in E$. Prove that if $f(a)$ is algebraic over F for a non-constant polynomial $f \in F[x]$, then a is algebraic over F as well.

Solution: If $f(a)$ is algebraic, then there exists $0 \neq g \in F[x]$ such that $f(a)$ is the root of g. This means that $g(f(a)) = 0$.

As g is non-zero, let $g(x) = g_n x^n + \cdots + g_0$ where $g_n \neq 0$ and as f is non-constant, then let $f(x) = f_m x^m + \cdots + f_0$ where $f_m \neq 0$

Then,

$$\begin{aligned} g \circ f(x) &= g_n f(x)^n + \cdots + g_0 \\ &= g_n(f_m x^m + \cdots + f_0)^n + \cdots + g_1(f_m x^m + \cdots + f_0) + g_0 \\ &= g_n f_m^n x^{mn} + \cdots + g_n f_0^n + \cdots + g_1 f_m x^m + \cdots + g_1 f_0 + g_0 \end{aligned}$$

which asserts that $g \circ f$ is non-constant as $g_n f_m \neq 0$, thus it is non-zero.

Moreover, as $g, f \in F[x]$, then $g \circ f \in F[x]$ as shown in the above equations. Since $g \circ f \in F[x]$ is non-zero but $g \circ f(a) = 0$, then a is algebraic.

Question 10

Let $F(x)$ be the quotient field of the polynomial ring $F[x]$ over a field F. Find the degree $[F(x) : F(\frac{x^2}{x-1})$

Solution: Let p be the polynomial $y^2 - \frac{x^2}{x-1}y - 1$ in $F(\frac{x^2}{x-1})[y]$. Now, by eisenstein criterion, $\frac{x^2}{x-1}$ is irreducible in $F[\frac{x^2}{x-1}]$ and satisfies the condition of einsenstein. Thus, p is irreducible in $F(\frac{x^2}{x-1})[y]$. Moreover it is not hard to see that $y = x$ is a root of p, because $x^2 - \frac{x^2}{x-1}(x-1) = 0$.

Therefore, the minimal polynomial of x in $F(\frac{x^2}{x-1})$ is p, and since $\deg(p) = 2$, the degree $[F(x) : F(\frac{x^2}{x-1})]$ is 2.