Q12:

12) a) For $d \in D$, where D is a UFD, to be a greatest common divisor of a and b, $d \mid a$, $d \mid b$, and if $e \mid a$, $e \mid b$, then $e \mid d$ as well. Suppose that d and d' are both greatest common divisors, then $d \mid d'$ and $d' \mid d$, such that $ds = d'$ and $d't = d$. It follows that $d'ts = d'$, or $ts = 1$, where t and s are units within D. Since the two divisors must divide one another, they must differ up to units in D, and are thus associates.

Q12

(a) Proposition: If D is a PID and a and b are both nonzero elements of D, then there exists a unique greatest common divisor of a and b up to associates.

Proof: Since D is a PID, there exists $d \in D$ s.t. $(d) = (a, b)$.

Then since $a \in (d)$, $b \in (d)$, $d \mid a$ and $d \mid b$.

Suppose $c \in D$ s.t. $c \mid a$ and $c \mid b$. Then $a \in (c)$ and $b \in (c)$. So $(a, b) \subseteq (c)$, $(d) \subseteq (c)$. Thus, $c \mid d$ and $d = \gcd(a, b)$.

Suppose d' is also $\gcd(a, b)$. Then $d' \mid a$ and $d' \mid b$. Thus, $d' \mid d$ and $d \mid d'$. Then there exists $e, f \in D$ s.t. $d'e = d$ and $df = d'$. $(df)e = 1 \cdot d$, so $d(fe - 1) = 0$ and $fe = 1$. Therefore, d and d' are associates

Thus, there exists a unique greatest common divisor of a and b up to associates.

b) Let D be a PID and a and b be nonzero elements of D. Prove that there exist elements s and t in D such that $\gcd(a, b) = as + bt$.

Proof: Consider the ideal $(a, b) \subset D$. Since D is a PID, there must exist a $d \in D$ such that $(a, b) = (d)$. Then, there must exist $s, t \in D$ such that $d = as + bt$. Because $(a, b) = (d)$, we can say that $d \mid a$ and $d \mid b$. If there exists another element $c \in D$ such that $c \mid a$ and $c \mid b$, there must exist $m, n \in D$ such that $a = cm$ and $b = cn$. Plugging in these equations into $d = as + bt$, we get $d = cms + cnt = c(ms + nt)$, so c must divide d. Thus, $d = \gcd(a, b)$.

Q17:

Q17. Proposition. Subdomain of a UFD may not be a UFD.

Proof: We can prove by giving a caunter example.

We know that any field is a UFD. Since $\mathbb{C}$ is a field, $\mathbb{C}$ is a UFD.

Then $\mathbb{Z}[\sqrt{-5}] \subseteq \mathbb{C}$ is a subdomain of $\mathbb{C}$.

$\mathbb{Z}[\sqrt{-5}]$ is not UFD because $6 = 2 \times 3 = (1+\sqrt{-5})(1-\sqrt{-5})$.

Thus, subdomain of a UFD may not be a UFD.

17.

Proposition 10. ***Not*** *every subdomain of a UFD is also a UFD.*

Proof. It suffices to provide a counterexample.
By the previous HW, we proved that $\mathbb{Z}[\sqrt{-5}]$ is not a UFD.
However, $\mathbb{Z}[\sqrt{-5}]$ is a subring of $\mathbb{C}$.
Namely, it is a subdomain as all subrings with 1 of an integral domain are integral domains and $1 = 1 + 0\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ and $\mathbb{C}$ is an integral domain as it is a field.
Furthermore, as $\mathbb{C}$ is a field, it is also a PID and therefore a UFD.
Hence $\mathbb{Z}[\sqrt{-5}]$ is a subdomain of a UFD but is not a UFD. $\square$

Q2:

2. Find a basis for each of the following field extensions + what is the degree of extension?

a) $\mathbb{Q}(\sqrt{3}, \sqrt{6})$ over $\mathbb{Q}$
Elements in $\mathbb{Q}(\sqrt{3}, \sqrt{6})$ look like $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ where $a, b, c, d \in \mathbb{Q}$. A basis for this field extension is $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$, and the degree of extension is 4.

c) $\mathbb{Q}(\sqrt{2}, i)$ over $\mathbb{Q}$
Elements in $\mathbb{Q}(\sqrt{2}, i)$ look like $a + b\sqrt{2} + ci + d\sqrt{2}i$ where $a, b, c, d \in \mathbb{Q}$. A basis for this field extension is $\{1, \sqrt{2}, i, \sqrt{2}i\}$, and the degree of extension is 4.

f) $\mathbb{Q}(\sqrt{8})$ over $\mathbb{Q}(\sqrt{2})$
Since $\sqrt{8} = 2\sqrt{2}$, we can say that $\mathbb{Q}(\sqrt{8}) = \mathbb{Q}(\sqrt{2})$. A basis for this field extension is $\{1\}$, and the degree of extension is 1.

h) $\mathbb{Q}(\sqrt{2} + \sqrt{5})$ over $\mathbb{Q}(\sqrt{5})$
We know that $\mathbb{Q}(\sqrt{2} + \sqrt{5}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{5})$, but also $\frac{1}{\sqrt{2}+\sqrt{5}} = \frac{\sqrt{2}-\sqrt{5}}{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{5})$ so both $\sqrt{2}$ and $\sqrt{5} \in \mathbb{Q}(\sqrt{2} + \sqrt{5})$. So we can say that $\mathbb{Q}(\sqrt{2} + \sqrt{5}) = \mathbb{Q}(\sqrt{2}, \sqrt{5})$. A basis for this field extension is $\{1, \sqrt{2}\}$, and the degree of extension is 2.

i) $\mathbb{Q}(\sqrt{2}, \sqrt{6} + \sqrt{10})$ over $\mathbb{Q}(\sqrt{3} + \sqrt{5})$
Since $\sqrt{2}(\sqrt{3} + \sqrt{5}) = \sqrt{6} + \sqrt{10}$, we can say that $\mathbb{Q}(\sqrt{2}, \sqrt{6} + \sqrt{10}) = \mathbb{Q}(\sqrt{2}(\sqrt{3} + \sqrt{5}))$. A basis for this field extension is $\{1, \sqrt{2}\}$, and the degree of extension is 2.