Q15:

15.

Proposition 1. *Let $f(x)$ be irreducible in $F[x]$, where F is a field. If $f(x) \mid p(x)q(x)$, then either $f(x) \mid p(x)$ or $f(x) \mid q(x)$.*

Proof. Suppose $f(x) \mid p(x)q(x)$.
Then, as $f(x)$ is irreducible, the ideal $\langle f(x) \rangle \subset F[x]$ is maximal.
More specifically, this gives that $\langle f(x) \rangle$ is prime as all maximal ideals are also prime ideals.
Furthermore, we know that $f(x) \mid p(x)q(x)$ means $p(x)q(x) = f(x)g(x)$ for some $g(x) \in F[x]$.
Thus, by definition $p(x)q(x) \in \langle f(x) \rangle$.
By the definition of prime ideals, then $p(x) \in \langle f(x) \rangle$ or $q(x) \in \langle f(x) \rangle$.
Thus $p(x) = f(x)g(x)$ or $q(x) = f(x)g'(x)$ for some $g(x), g'(x) \in F[x]$.
Hence, we have that $f(x) \mid p(x)$ or $f(x) \mid q(x)$.

□

15. Let f(x) be irreducible in a F[x]. Let $f(x)|p(x)q(x)$ and we will show that $f(x)|p(x)$ or $f(x)|q(x)$. By Theorem 17.2 we know that F[x] is a PID. Since it's a PID, we know that it's also a UFD. And by definition of a UFD, we know there is only one way to factor any element f(x) into unique factors: p(x)q(x)=f(x)c for some c$\in F(x)$. Therefore f(x) must be an irreducible factor for p(x) or q(x). Equivalently, this means that $f(x)|p(x)$ or $f(x)|q(x)$.

Q20:

20.

Proposition 2. *The polynomial*

$$\Phi_n(x) = \frac{x^n - 1}{x - 1} = x^{n-1} + x^{n-2} + ... + x + 1$$

is called the ***cyclotomic polynomial****, and* $\Phi_p(x)$ *is irreducible over* $\mathbb{Q}$ *for any prime* p*.*

Proof. Suppose for contradiction $\Phi_p(x)$ is reducible over $\mathbb{Q}$ for prime p.
Then, we can decompose $\Phi_p(x) = f(x)g(x)$ with $f(x), g(x) \in \mathbb{Z}[x]$ by Gauss's Lemma and $\deg f(x), \deg g(x) < p - 1$.
However, this gives us that $\Phi_p(x+1) = f(x+1)g(x+1)$.
Let $f'(x) = f(x+1)$ and $g'(x) = g(x+1)$, and observe $f'(x), g'(x) \in \mathbb{Z}[x]$.
Note that this gives us that $\Phi_p(x+1)$ is reducible over $\mathbb{Q}$.
However, expanding $\Phi_p(x+1)$, we get

$$\begin{aligned}
\Phi_p(x+1) &= \frac{(x+1)^p - 1}{x + 1 - 1} \\
&= \frac{(x+1)^p - 1}{x} \\
&= \frac{\sum_{k=0}^{p} \binom{p}{k} x^{p-k} - 1}{x} \\
&= \frac{\sum_{k=0}^{p-1} \binom{p}{k} x^{p-k}}{x} \\
&= \sum_{k=0}^{p-1} \binom{p}{k} x^{p-k-1}
\end{aligned}$$

Now, we may observe that the highest-power term is $\binom{p}{0} x^{p-1} = x^{p-1}$.
Noticeably, the coefficient of this term is 1 and $p \nmid 1$.
Every other coefficient $1 \leq k \leq p-1$, however, is given by $\binom{p}{k}$.
Furthermore, by the below lemma, we know that $p \mid \binom{p}{k}$.
Now, the a_0 term is $\binom{p}{p-1} = p$, and $p^2 \nmid p$.
Thus, by Eisenstein's Criterion, we have that $\Phi_p(x+1)$ is irreducible.
This provides a contradiction, and thus $\Phi_p(x)$ is irreducible. □

Q16:

16.

Proposition 8. *$\mathbb{Z}[\sqrt{5}i]$ is not a UFD.*

Proof. Suppose for contradiction that $\mathbb{Z}[\sqrt{5}i]$ is a UFD.
Take $6 \in \mathbb{Z}[\sqrt{5}i]$.
Obviously 6 is not a unit as $\mathbb{Z}[\sqrt{5}i] \subset \mathbb{Q}$ and the inverse of 6 in $\mathbb{Q}$ is $\frac{1}{6}$, which is not in $\mathbb{Z}[\sqrt{5}i]$.
Hence 6 must have a unique factorization into irreducible elements.
However, we may observe that $6 = 2 \cdot 3$ and $6 = (1 - \sqrt{5}i)(1 + \sqrt{5}i)$.
We will show that $2, 3, 1 - \sqrt{5}i$, and $1 + \sqrt{5}i$ are irreducible.
First, as $\mathbb{Z}[\sqrt{5}i]$ is a subring of the Gaussian Integers, the units must be from ± 1 and $\pm i$.
However $\pm i \notin \mathbb{Z}[\sqrt{5}i]$ and thus the units are ± 1.
Namely, none of the above elements are units.
Take the function $\phi : \mathbb{Z}[\sqrt{5}i] \to \mathbb{Z}_{\geq 0}$ given by $\phi(a + b\sqrt{5}i) = a^2 + 5b^2$.
This is equivalent to multiplication by the complex conjugate, and thus preserves multiplication.
Evidently $\phi(\pm 1) = 1$ and if $\phi(a+b\sqrt{5}i) = 1$, then $a = \pm 1$ as if b is nonzero then $\phi(a + b\sqrt{5}i)$ would be strictly greater than 5.
Therefore, we have an if and only if relationship.
Now, if 2 were not irreducible then $2 = cd$ for some $c, d \in \phi(a + b\sqrt{5}i)$ such that c, d are not units.
Therefore, applying ϕ to both sides, $4 = \phi(c)\phi(d)$ and $\phi(c)$ and $\phi(d)$ are strictly greater than 1.
However, this implies that $\phi(c) = \phi(d) = 2$.
The equation $a^2+5b^2 = 2$ has no integer solutions so 2 must be irreducible.
Similarly $a^2 + 5b^2 = 3$ has no integer solutions so 3 must be irreducible.
Now, take $1 + \sqrt{5}i$.
By the same logic, we know that if this were not irreducible, there would be some $c, d \in \mathbb{Z}[\sqrt{5}i]$ such that $1 + \sqrt{5}i = cd$ and c, d are not units.
Again, applying ϕ, this gives us that $2 = \phi(c)\phi(d)$ with $\phi(c)$ and $\phi(d)$ strictly greater than 1.
This has no integer solutions, so $1 + \sqrt{5}i$ is irreducible.
Considering that $\phi(1-\sqrt{5}i) = 2$, the exact same logic gives us that $1-\sqrt{5}i$ is irreducible.
We may notice that neither 2 nor 3 is a unit multiple of $1 \pm \sqrt{5}i$ as the only units are ± 1.
Hence, we have shown that 6 has two distinct factorizations into irreducible elements in $\mathbb{Z}[\sqrt{5}i]$ and therefore $\mathbb{Z}[\sqrt{5}i]$ is not a UFD. $\square$