In class, we finished proving if a polynomial $p(x) \in F[x]$ with coefficients in a field is prime, then it is irreducible.

We started (and didn't finish) proving that if it is irreducible, then it is also prime.

What we had at the end of class was:

Given $p(x) \in F[x]$ is irreducible
(which means if $p(x) = s(x)t(x)$ where $s(x), t(x) \in F[x]$ then $s(x)$ and $t(x)$ are each either associates of $p(x)$ or they are units (non-zero elements of F).

Suppose $p(x) \mid f(x)g(x)$ (we need to prove that $p(x) \mid f(x)$ or $p(x) \mid g(x)$)

Suppose $p(x) \nmid f(x)$
Let $d(x) = \gcd(p(x), f(x))$ This is the first idea/hint you need to get from irreducible to prime.
Then $d(x) \mid f(x)$ and $d(x) \mid p(x)$ which means $f(x) = d(x)a(x)$ and $p(x) = d(x)b(x)$
$d(x) = u(x)f(x) + v(x)g(x)$
where $a(x), b(x), u(x), v(x) \in F[x]$

Also $p(x) \mid f(x)g(x)$ means $f(x)g(x) = p(x)q(x)$ for some $q(x) \in F[x]$

Now we use the given that $p(x)$ is irreducible with the equation $p(x) = d(x)b(x)$ to say
$d(x)$ is either a unit or an associate of $p(x)$

Case 1: $d(x)$ is a unit, which means $d(x) = n \in F$ and n has an inverse n^{-1}
Substitute this into the equations with d:
$f(x) = n \cdot a(x)$ and $p(x) = n \cdot b(x)$
$n = u(x)f(x) + v(x)p(x)$
In this last equation, we're going to make it more similar to the proof with integers by multiplying through by n^{-1}
$n^{-1} \cdot n = n^{-1} \cdot u(x)f(x) + n^{-1} \cdot v(x)p(x)$
So $1 = (n^{-1}u(x))f(x) + (n^{-1}v(x))p(x)$
Multiply both sides by $g(x)$ This is another key trick—if you need something about g, and you don't have any g's, look for a place where multiplying in a g might be useful:
So $g(x) = (n^{-1}u(x))f(x)g(x) + (n^{-1}v(x))p(x)g(x)$
Recall $f(x)g(x) = p(x)q(x)$
So $g(x) = (n^{-1}u(x))p(x)q(x) + (n^{-1}v(x))p(x)g(x)$
$g(x) = p(x)[(n^{-1}u(x))q(x) + (n^{-1}v(x))g(x)]$ which means $p(x) \mid g(x)$

So in case 1, if $p(x) \nmid f(x)$ then $p(x) \mid g(x)$ so either $p(x) \mid f(x)$ or $p(x) \mid g(x)$

Case 2: $d(x)$ is an associate of $p(x)$
That means $p(x) = m \cdot d(x)$ where $m \in F$ and $m \neq 0$
m is a unit so we can also write:
$m^{-1} p(x) = d(x)$
Then we can put this together with $f(x) = d(x)a(x)$ to get
$f(x) = m^{-1} p(x)a(x) = p(x)[m^{-1}a(x)]$
so $p(x) \mid f(x)$ which contradicts the assumption $p(x) \nmid f(x)$, so this is not a possible outcome in the case where $p(x) \nmid f(x)$.

Thus we have proved that if $p(x) \nmid f(x)$ then $p(x) \mid g(x)$
And therefore $p(x) \mid f(x)$ or $p(x) \mid g(x)$
And hence $p(x)$ is prime.

This finishes the second case, so we can say that a polynomial $p(x) \in F[x]$ is irreducible if and only if it is prime.

The thing I'd like you to know about the proof of theorem 59

To prove that a polynomial $f(x)$ can be factored into irreducible factors, the only thing we need to know is that if you can factor $f(x) = a(x)b(x)$, and neither $a(x)$ nor $b(x)$ is a constant, then $\deg(a(x)) < \deg(f(x))$ and $\deg(b(x)) < \deg(f(x))$. That means if you make a factor tree, then every time you go down a level, the degrees of the polynomials get smaller.

It's pretty easy to see that any polynomial of degree 1 is irreducible.

That means if you make a factor tree out of a polynomial $f(x)$, eventually you're going to get down to all irreducible polynomials: $f(x) = p_1(x)p_2(x)...p_n(x)$ where $p_i(x)$ is irreducible for all $1 \leq i \leq n$

Now we can imagine that you might be able to do this in a different way:
$f(x) = q_1(x)q_2(x)...q_m(x)$ where $q_i(x)$ is irreducible for all $1 \leq i \leq m$

Because the p's and q's are also prime, however, we can say that for every $1 \leq i \leq n$ there is a $j = s(i)$ such that $p_i \mid q_j$ and because they are both prime and irreducible we can say that $p_i(x)$ and $q_j(x)$ are associates. The prime property is what lets us say that any two different factorization into irreducible, non-constant polynomials:
$f(x) = p_1(x)p_2(x)...p_n(x)$ and $f(x) = q_1(x)q_2(x)...q_m(x)$ have to be the same factorization in disguise, where they actually have the same number of factors ($n = m$) and the p's and q's can be paired up into associates: polynomials that are the same except for being multiplied by a unit.

When we talk about prime numbers and irreducible polynomials, the fact those integers and polynomials have both the prime and the irreducible property is what lets us make unique factorizations.