Content:

Proposition Let F be a field. If $f(x) \in F[x]$ and $a \in F$, then a is a root of $f \Leftrightarrow (x - a) \mid f(x)$.

Theorem Let $f(x) \in F[x]$ such that $\deg f(x) = n$. Then $f(x)$ has at most n roots in F.

Theorem Let F be a field. Then $F[x]$ is a principal ideal domain.

Definition addition and multiplication in $F = \{[a, b] \mid (a, b) \in X\}$.

Proposition Let F be a field. If $f(x) \in F[x]$ and $a \in F$, then a is a root of $f \Leftrightarrow (x - a) \mid f(x)$.

Proof:
Follows from lemma given Monday.

Theorem Let $f(x) \in F[x]$ such that $\deg f(x) = n$. Then $f(x)$ has at most n roots in F.

Proof:
We will prove the theorem by induction on n.
Let $n = 0$. Then $f(x) = c \neq 0$. So $f(x)$ has 0 roots.
Assume the theorem is true for any degree less than n.
If f has no roots, we're done.
So assume f has a root a in F.
Thus $\exists\ q(x) \in F[x]$ such that $f(x) = (x - a)q(x)$.
So $\deg q(x) = n - 1$.
Thus, we know $q(x)$ has at most $n - 1$ roots.
Let $b \neq a$ be a root of $f(x)$ in F.
So $f(b) = 0$. Thus $0 = f(b) = (b - a)q(b)$.
Since F is an integral domain, $q(b) = 0$.
So $\forall\ b \in F$ such that b is a root of $f(x)$, $b \neq a$, b is also a root of $q(x)$.
So $f(x)$ can have at most $n - 1$ roots from $q(x)$ plus the root a.

Theorem Let F be a field. Then $F[x]$ is a principal ideal domain.

Proof:
We know it's an integral domain, so we only need to show it is principal.
Let I be an ideal in $F[x]$ such that $I \neq \{0\}$.
Let $g(x) \in I$ such that $\deg g(x) \leq \deg h(x)\ \forall\ h(x) \in I, h(x) \neq 0$.
Let $f(x) \in I$. By the division algorithm, $\exists\ !\ q(x), r(x) \in F[x]$ such that $f(x) = g(x)q(x) + r(x)$ where $r(x) = 0$ or $\deg r(x) < \deg g(x)$.
Since I is an ideal, $g(x)q(x) \in \mathrm{I}$, thus $r(x) = f(x) - g(x)q(x) \in I$.
Since $g(x)$ is of minimal degree in I, $r(x)$ must be 0.
Thus, $f(x) = g(x)q(x)$, hence $f(x) \in (g(x))$.
$\therefore\ I \subseteq (g(x))$. Since $(g(x)) \subseteq I$, then $I = (g(x))$.
Thus, $F[x]$ is a principal ideal domain.

Field of Fractions (3.2)

Let R be an integral domain. Let $X = \{(a, b) \in R \times R \mid b \neq 0\}$.
Define ~ by $(a, b) \sim (c, d) \Leftrightarrow ad = bc$.

Note ~ is an equivalence relation.
Since $\forall\ (a, b) \in R \times R$, $ab = ab$, then $(a, b) \sim (a, b)$, so ~ is reflexive.
Since $ad = bc \Rightarrow da = cb$, then $(a, b) \sim (c, d) \Rightarrow (c, d) \sim (a, b)$,
then ~ is symmetric.
If $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$, then $ad = bc$ and $cf = de$.
Thus, $adf = bcf$ and $bcf = bde$. So $af = be$.
(But, if $c = 0$, then $adf = 0 = bde$. Consider, $adcf = bcde$.
Then $cd(af - be) = 0$. So $cd = 0$ or $af = be$. If $af = be$, we're done.
If $cd = 0$, then we know $c = 0$ as $d \neq 0$. So $ad = b \bullet 0 = 0$.
Since $d \neq 0$, then $a = 0$. Similarly, $e = 0$. Thus $af = 0 \bullet f = 0 = b \bullet 0 = be$.)

Let $[a, b]$ be the equivalence class of (a, b). That is,
$[a, b] = \{(c, d) \in X \mid (a, b) \sim (c, d)\}$.

Example $R = \mathbb{Z}$. $[1, 2] = \{(x, 2x) \in X \mid x \in \mathbb{Z}\}$
$(1, 2) \sim (2, 4) \sim (3, 6) \sim \cdots$

Definition Let $F = \{[a, b] \mid (a, b) \in X\}$. Define $+$ *and* $\bullet$ on F as
$[a, b] + [c, d] = [ad + bc, bd]$
$[a, b] \bullet [c, d] = [ac, bd]$.

We need to check if these operations are well-defined.
Assume $[a, b] = [x, y]$ and $[c, d] = [z, w]$. Then
$ay = bx$ and $cw = dz$. So
$aycw = bxdz$. Thus,
$acyw = bdxz$. This gives us that
$[ac, bd] = xz, yw]$. And so
$[a, c] \bullet [c, d] = [x, y] \bullet [z, w]$. Also, by substitution,
$(ad + bc)yw = adyw + bcyw = bxdw + bydz = bd(xw + yz)$, so
$[ad + bc, bd] = [xw + yz, yw]$. Thus,
$[a, b] + [c, d] + [x, y] \neq [z, w]$.
And so $\bullet$ and $+$ are well-defined.

To show that F is a field, we need to verify the associativity axioms and the distributivity law. Associativity falls out quickly, but check distributivity as an exercise.

Let $[a, b]$, $[c, d]$, and $[e, f] \in$ F.
Then $[a, b]([c, d] + [e, f]) = [a, b] \bullet [cf + de, df\,] = [a(cf + de), bdf\,]$. And
$[a, b] \bullet [c, d] + [a, b] \bullet [e, f] = [ac, bd] + [ae, bf] = [acbf + bdae, bdbf]$
Since $a(cf + de)bdbf = acfbdbf + adebdbf = bdf(acbf + bdae)$, then
$[a(cf + de), bdf\,] = [acbf + bfdae, bdbf]$. So the distributive property holds.

What's 0? $[0, b]$, $b \neq 0$.
What's 1? $[a, a]$, $a \neq 0$.
$[a, a] \bullet [c, d] = [ac, ad]$. Since $acd = adc$, then $[c, d] = [ac, ad]$.

Now, we need to show each element in F has an inverse.
Let $[a, b] \in F$ such that $[a, b] \neq 0_F$.
$[a, b] \bullet [\ \_\_\_\_, \_\_\_\_\ ] = 1_F$.
We need $a \bullet \_\_\_\_ = b \bullet \_\_\_\_$, so it must be $[a, b] \bullet [b, a] = 1_F$.
But, is it possible for $[x, y] = 0_F$ if $x \neq 0$?
If so, then $[x, y] \bullet [0, c] \Rightarrow xc = y \bullet 0 = 0$. Since $c \neq 0$, then $x = 0$.
So $[x, y] = 0_F \Leftrightarrow x = 0$. So, we can be sure $[b, a] \neq 0$, hence it is our inverse for $[a, b]$.