3/30/11

(Fix): <u>Recall</u> R is an integral domain, R is called a <u>Euclidean Domain</u> if $\exists$ $d: R\setminus\{0\} \to \mathbb{N}$ and
1) $\forall\, a,b \in R\setminus\{0\}$, $d(a) \le d(ab)$
2) $\forall\, a \in R$, $b \in R\setminus\{0\}$, $\exists$ $q, r \in R$ with $a = bq + r$ where either $r = 0$ or $d(r) < d(b)$

<u>Examples</u>
1) $\mathbb{Z}$, $d(n) = |n|$
2) $\mathbb{F}$ a field, $\mathbb{F}[x]$ with $d(p(x)) = \text{degree}(p)$.

Proving that $\mathbb{F}[x]$ is a Euclidean Domain:
If $p, q \in \mathbb{F}[x]$, $p, q \ne 0$, then

$$p(x) = \sum_{i=0}^{n} \alpha_i x^i \quad \text{and} \quad q(x) = \sum_{j=0}^{m} \beta_j x^j$$

where α_i's and β_j's are elements of $\mathbb{F}$.
Suppose $\alpha_n, \beta_m \ne 0$. Then $\deg(p) = n$, $\deg(q) = m$

$$p(x)q(x) = \alpha_n x^n \cdot \beta_m x^m + \Sigma\,(\text{garbage of lower deg})$$
$$= \alpha_n \beta_m x^{n+m} + \Sigma\,(\text{garbage})$$

$\deg(p \cdot q) = n + m \ge \deg(p), \deg(q)$
so, $d(p) = \deg(p)$ satisfies $d(pq) \ge d(p)$

Prove 2nd part:
$p, q \in \mathbb{F}[x]$, $q \ne 0$

$$p(x) = \sum_{i=0}^{n} \alpha_i x^i \quad \text{and} \quad q(x) = \sum_{j=0}^{m} \beta_j x^j$$

Suppose $n \ge m$. $\exists$ division algorithm

$$\begin{array}{r l}
 & \frac{\alpha_n}{\beta_m} x^{n-m} \\ \hline
\sum_{j=0}^{m} \beta_j x^j \; \Big) & \sum_{i=0}^{n} \alpha_i x^i \\
 & - \sum_{j=0}^{m} \frac{\beta_j \alpha_n}{\beta_m} x^{j+n-m} \qquad = \alpha_n x^n + \sum_{j=0}^{m-1} \frac{\beta_j \alpha_n}{\beta_m} x^{j+n-m}
\end{array}$$

Keep on going ...
finally either get: $p(x) = q(x)s(x)$ or
$p(x) = q(x)t(x) + s(x)$ with $\deg(r) < \deg(q)$,
(if $\deg(r) \ge \deg(q)$, perform division of r by q)

Def: let R be an integral domain. An ideal in R is called principal if (let I = ideal) there is an $x \in R$ with $I = \{y \cdot x : y \in R\}$.

Note: $\{y \cdot x : y \in R\}$ is an ideal.
Check this is a subring:
Recall R an integral domain $\Rightarrow xy = yx$
If $y_1 x$ and $y_2 x \in \langle x \rangle$, then $-y_2 x \in \langle x \rangle$
Then $y_1 x - y_2 x = (y_1 - y_2)(x)$ [distributivity]
$\in \langle x \rangle$

So, $\langle x \rangle$ is an abelian group.
If $y_1 x, y_2 x \in \langle x \rangle$ then

$$\begin{aligned} y_1 x\, y_2 x &= y_1 (x\, y_2) x \quad \text{[associativity]} \\ &= y_1 (y_2 x) x \quad \text{[commutativity]} \\ &= \underbrace{(y_1 y_2 x)}_{y_3 \in R} x \quad \text{[associativity]} \\ &\in \langle x \rangle \end{aligned}$$

Terminology: if $x \in R$, $\langle x \rangle$ is called the ideal generated by x.

Def: R an integral domain, R is called a principal ideal domain if $\forall$ ideals $I \subseteq R$ $\exists$ an $x \in R$ where $I = \langle x \rangle$.

Examples:

1) $R = \mathbb{Z}$ is a principal ideal domain. [euclidian domain]
(We've already proved this.)

2) $R = \mathbb{Z}\left[\frac{1 + i\sqrt{19}}{2}\right] = \left\{n + m\left(\frac{1 + i\sqrt{19}}{2}\right) : n, m \in \mathbb{Z}\right\}$ [not euclidean domain]

3) $R = \mathbb{F}[x]$ where $\mathbb{F}$ is a field. [euclidean domain]

Proof is a consequence of the following:

Thm: Every Euclidean domain is a principal ideal domain.

Pf: let $I \subseteq R$ be an ideal. WTS $\exists$ an $x \in R$, $I = \langle x \rangle$. Let $d: R\setminus\{0\} \to \mathbb{N}$ be the Euclidean domain function. Let $0 \neq x \in I$ be an element with $d(x)$ minimal (well-ordering principle of the natural numbers).

Goal: Show $I = \langle x \rangle$

let $0 \neq x \in I$. Apply division algorithm to obtain $q, r \in R$ with $y = xq + r$.

Either $r = 0$ or $d(r) < d(x)$.

But since I is an ideal, $xq \in I$, and also, $y - xq \in I$ but $y - xq = r \in I$.

Since $d(x)$ is minimal in I we can't have $d(r) < d(x)$. So, $r = 0$ and then $y = xq = qx \in \langle x \rangle$

Hence, $I = \langle x \rangle$ ∎

Notation: if $x, y \in R$, we write $x \mid y$ (x divides y) if $\exists$ $z \in R$, $y = xz$ (R an integral domain)

Field $\Rightarrow$ Euclidean domain $\Rightarrow$ Principal Ideal domain $\Rightarrow$ unique factorization domain.