date: monday, march 11, 2024

Ideals in $F[x]$

Recall: An ideal I in R is principal if there exists an $a \in R$ such that
$$I = \{ra \mid r \in R\} = \langle a \rangle$$
for R commutative.

eg. If $R = \mathbb{Z}$, every ideal of $\mathbb{Z}$ is principal.

eg. If $R = F[x]$ with F a field, then similar result holds.

Theorem: Every ideal I of $F[x]$ is principal.

Proof

If $I = \{0\}$, then $I = \langle 0 \rangle$, ie. it's principal.
So assume $I \neq \{0\}$. Let $p(x) \neq 0$ be in I such that
$$\deg p(x) \leq \deg q(x)$$
for all $q(x) \in I$. If $\deg p(x) = 0$, then $p(x) = c$ for some $c \in F$. So $c \in I$.
But $c^{-1} \in F \subseteq F[x]$, so $c^{-1}c = 1 \in I$. Then $I = F[x] = \langle 1 \rangle$.
So, suppose $\deg p(x) > 0$.
Claim: $I = \langle p(x) \rangle$.
"$\supseteq$" Since $p(x) \in I$, $\langle p(x) \rangle \subseteq I$.
"$\subseteq$" Let $t(x) \in I$. By division algorithm,
$$t(x) = p(x)q(x) + r(x)$$
with $r(x) = 0$ or $\deg r(x) < \deg p(x)$.
If $r(x) \neq 0$, we have
$$r(x) = \underset{\substack{\Uparrow \\ I}}{t(x)} - \underset{\substack{\Uparrow \\ I}}{p(x)}q(x) \in I$$
But $\deg r(x) < \deg p(x)$, and $p(x)$ is supposed to have smallest degree in I. This is a contradiction. So
$$t(x) = p(x)q(x) \in \langle p(x) \rangle.$$
$\square$

eg. False in $F[x,y]$.

Consider $\langle x^2, y\rangle = \{fx^2+gy \mid f,g\in F[x,y]\}$.

Claim: $\langle x^2,y\rangle$ is not principal.

Suppose $\langle x^2,y\rangle = \langle p(x,y)\rangle$. So $x^2 \in \langle p(x,y)\rangle \Rightarrow p(x,y) \mid x^2$ and
$y\in \langle p(x,y)\rangle \Rightarrow p(x,y)\mid y$.

So $p(x,y)=c$ for some $c\in F$. But then $\langle x^2,y\rangle = \langle 1\rangle$. But $1\notin \langle x^2,y\rangle$.

Contradiction.

In $\mathbb{Z}$, $\langle a\rangle$ is a maximal ideal $\Leftrightarrow$ a is prime.

Theorem: In $F[x]$, $\langle f(x)\rangle$ is a maximal ideal $\Leftrightarrow$ $f(x)$ is irreducible.

Proof

"$\Rightarrow$" Suppose $I=\langle f(x)\rangle$ is maximal and $f(x)=p(x)q(x)$. So $f(x)\in\langle p(x)\rangle$. Thus, $I\subseteq \langle p(x)\rangle$. Because I is maximal, $I=\langle p(x)\rangle$ or $\langle p(x)\rangle = F[x]$. If $I=\langle p(x)\rangle$, then $p(x)\in\langle f(x)\rangle$. So $\deg f(x)\le \deg p(x) \le \deg f(x)$. So $f(x)=p(x)$ If $\langle p(x)\rangle \in F[x]$, then $1\in\langle p(x)\rangle$. So $p(x)\mid 1$. Thus, $\deg p(x)=0$. So $f(x)$ is irreducible.

"$\Leftarrow$" Let $I=\langle f(x)\rangle$ and suppose $I\subseteq J\subseteq F[x]$. Since $J=\langle q(x)\rangle$, we have $f(x)\in\langle q(x)\rangle$, so $f(x)=p(x)q(x)$. Since $f(x)$ irreducible, $\deg q(x)=0$ or $\deg q(x)=\deg f(x)$. If $\deg q(x)=0$, $q(x)=c$. So $J=F[x]$. If $\deg q(x)=\deg f(x)$, then $f(x)=cq(x)$ so $\langle f(x)\rangle=\langle q(x)\rangle$.

$\square$

$\boxed{\text{Practice Problems}}$

A. Apply division algorithm to $a(x)=4x^5-x^3+x^2+4$ in $\mathbb{Z}_5[x]$.
$b(x)=x^3-2$

$$
\begin{array}{r l}
 & 4x^2-1 \\
x^3-2 \,\big) & 4x^5-x^3+x^2+4 \\
 & -(4x^5 \qquad -8x^2) \\
 & \qquad -x^3+9x^2+4 \\
 & \qquad -(-x^3 \qquad +2) \\
 & \qquad\qquad 9x^2+2 \equiv 4x^2+2 \pmod 5
\end{array}
$$

$4x^5-x^3+x^2+4=(4x^2-1)(x^3-2)+4x^2+2 \pmod 5$

B. For any polynomial $p(x) \in \mathbb{R}[x]$, we know $p(x)$ has at most $\deg p(x)$ roots.
Show this is false in $\mathbb{Z}_{10}[x]$.

Consider $p(x) = 5x$ which has $\deg p(x) = 1$.
But $x = 0, 2, 4, 6, 8 \in \mathbb{Z}_{10}$ are all roots.

C. Rational Root Test
Suppose $p(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$. If $\frac{r}{s} \in \mathbb{Q}$ is a root, then $r | a_0$ and $s | a_n$ $(\gcd(r,s) = 1)$.

$\frac{r}{s} \in \mathbb{Q}$ a root $\Rightarrow a_n\left(\frac{r}{s}\right)^n + a_{n-1}\left(\frac{r}{s}\right)^{n-1} + \cdots + a_1\left(\frac{r}{s}\right) + a_0 = 0$.

$$\Leftrightarrow \frac{a_n r^n + a_{n-1} r^{n-1} s + \cdots + a_1 r s^{n-1} + a_0 s^n}{s^n} = 0$$

Then, $a_n r^n = s(-a_{n-1} r^{n-1} - \cdots - a_0 s^{n-1})$. We have that $\gcd(r,s) = 1$, so $s | a_n r^n$ implies $s | a_n$.
Also, $a_n r^n + \cdots + a_1 r s^{n-1} = -a_0 s^n$. So $r(a_n r^{n-1} + \cdots + a_1 s^{n-1}) = -a_0 s^n$. So $r | a_0 s^n$ but since $\gcd(r,s) = 1$, we have that $r | a_0$.

Show $7x^2 + 2$ has no rational roots.

Suppose $r | 2$ and $s | 7$. Then $r = \pm 1, \pm 2$ and $s = \pm 1, \pm 7$. So distinct possible roots are $\pm 1, \pm 2, \pm \frac{1}{7}, \pm \frac{2}{7}$ from

$s \backslash r$	1	-1	2	-2
1	$1/1$	$-1/1$	$2/1$	$-2/1$
-1	$1/-1$	$-1/-1$	$2/-1$	$-2/-1$
7	$1/7$	$-1/7$	$2/7$	$-2/7$
-7	$1/-7$	$-1/7$	$2/-7$	$-2/-7$

By plugging these into $7x^2 + 2$, none of them are roots.

D. Prove $x^p + a$ is reducible for any $a \in \mathbb{Z}_p$ in $\mathbb{Z}_p[x]$ (p prime).

If $a=0$, $x^p + 0 = x x^{p-1}$ <— reducible.
If $a \neq 0$, $a \in \mathbb{Z}_p^{(*)}$. So $|a| = p-1 \Rightarrow a^{p-1} \equiv 1 \pmod p$
$\Rightarrow a^p = a$.
In particular, $(-a)^p = -a$. So $-a$ is a root of $x^p + a$ since
$(-a)^p + a = -a + a = 0$. So $x^p + a = (x+a)(*)$.