For a field $F$, the set $D = F[x]$ of polynomials with coefficients in $F$ is a domain. We defined the degree function

$$\deg : F[x] \to \mathbb{Z}_{\geq 0} \cup \{-\infty\},$$

where $\deg(0) := -\infty$, satisfying

$$\deg(fg) = \deg(f) + \deg(g),$$
$$\deg(f + g) \leq \max(\deg(f), \deg(g)).$$

We’ve shown that $D$ admits a “division algorithm”: for all $f, g \in F[x], g \neq 0$, there exist unique polynomials $q, r$ such that

$$f = qg + r, \quad \deg r < \deg g.$$

**Ideals.** To talk about the analogue of integer combinations, using the notion of an ideal. For a domain $D$, an **ideal** is a subset $I \subseteq D$ such that

1. $I$ is non-empty,
2. for all $a, b \in I$, we have $a + b \in I$ and $-a \in I$,
3. for all $c \in D$ and $a \in I$, we have $ca \in I$.

Consequences: if $a \in I$, then $-a = (-1)a \in I$ by (3). Since $I$ is non-empty, $0 = a - a \in I$.

Examples:

1. Fix $a \in D$, and consider $I := \{ ca \mid c \in D \}$. Then $I$ is an ideal. We have two notations for this:

$$\{ ca \mid c \in D \} = Da = (a).$$

   Such an ideal is called **principal**.

   For instance, $\mathbb{Z}d = (d) = \{ ds \mid s \in \mathbb{Z} \}$ is the set of integer multiplies of $d$.

2. Fix $a_1 \in D$, and consider $a_1, a_2 \in D$. Let $I := \{ c_1a_1 + c_2a_2 \mid c_1, c_2 \in D \}$. Then $I$ is an ideal. We have two notations for this:

$$\{ c_1a_1 + c_2a_2 \mid c_1, c_2 \in D \} = Da_1 + Da_2 = (a_1, a_2).$$

   For instance, $\mathbb{Z}a + \mathbb{Z}b = (a, b) = \{ ma + nb \mid m, n \in \mathbb{Z} \}$ is the set of integer combinations of $a$ and $b$. Our big theorem says that such ideals are also principal.

---

*Date: April 25, 2016.*
(3) Fix $c \in F$. Let $I \subseteq F[x]$ be the \textbf{vanishing ideal} of $c$, defined by
\[ I := \{ f \in F[x] \mid f(c) = 0 \}. \]

Then $I$ is an ideal: prove this directly: (1) $0 \in I$ (meaning the $0$-polynomial), since $c$ is always a root of the zero polynomial; (2) if $f, g \in I$, then $(f+g)(c) = f(c)+g(c) = 0$ so $f+g \in I$; (3) if $f \in I$ and $h \in F[x]$, then $(hf)(c) = h(c)f(c) = h(c)0 = 0$.

In fact, vanishing ideals are always principal.

\textbf{Proposition.} Fix $c \in F$, and let $I = \{ f \in F[x] \mid f(c) = 0 \}$ be the vanishing ideal of $c$. Then $I = (x-c)$.

\textbf{Proof.} Here is what the claim says: for $f \in F[x]$, we have that
\[ f(c) = 0 \iff f \text{ can be factored } (x-c)g. \]

We know this is true. We can actually give a direct proof, using the division algorithm applied to $f$ and $g = (x-c)$: there exist unique $q, r \in F[x]$ such that
\[ f = (x-c) \cdot q + r, \quad \deg r < \deg(x-c) = 1. \]

Thus $r$ is a constant polynomial, i.e., $r \in F \subseteq F[x]$. Plugging in $x = c$ gives
\[ f(c) = (c-c) \cdot q(c) + r \quad \implies \quad f(c) = r. \]

That is,
\[ f = (x-c) \cdot q + f(c). \]

Uniqueness means that $f \in I$ iff $f(c) = 0$. \hfill \Box

\textbf{Principal ideals.} The big theorem about GCD for integers amounts to the following.

\textbf{Proposition.} Every ideal $I \subseteq \Z$ is principal (i.e., of the form $Zd := \{ nd \mid n \in \Z \}$ for some $d$, and in fact for a unique non-negative $d$.)

\textbf{Proof.} If $I = \{0\}$, then $I = \Z0$. So suppose there exists a non-zero element $a$ in $I$. Since $a \in I$ implies $-a \in I$, there must be a positive element in $I$.

Let $d$ be the \textit{smallest} positive element in $I$. I claim that $I = Zd$. First note that since $d \in I$, $nd \in I$ for any $n \in \Z$, so $Zd \subseteq I$.

Next I prove that $I \subseteq Zd$. Let $a \in I$. By the division algorithm, there exist $q, r \in \Z$ with $0 \leq r < d$ such that $a = qd + r$. Since $a, qd \in I$, we have that $r = a - qd \in I$. Since $0 \leq r < d$ and $d$ is the smallest positive element in $I$, we must have $r = 0$, i.e., $a = qd$, so $a \in Zd$. \hfill \Box

By this result, for any $a, b \in \Z$, we have $Za + Zb = Zd$ for a unique $d \geq 0$. This is just the GCD.

We can prove the same thing for $D = F[x]$.

\textbf{Proposition.} Every ideal $I \subseteq F[x]$ is principal.

\textbf{Proof.} If $I = \{0\}$, there is nothing to prove so suppose $I$ contains a non-zero element. Choose $f \in I \setminus \{0\}$ whose degree $\deg f$ is \textit{minimal} among such elements. This is always possible because $\deg : I \setminus \{0\} \rightarrow \Z_{\geq 0}$, by the well-ordering property. It is clear that $F[x]f \subseteq I$. I’ll show $I \subseteq F[x]f$.

Suppose $g \in I$, and use the division algorithm to find $q, r \in F[x]$ such that
\[ g = qf + r, \quad \deg r < \deg f. \]
Because $g, f \in I$, then $r = g - qf \in I$. Because $f$ has minimal degree among non-zero elements of $I$, we must have $r = 0$, so $q = qf \in F[x]f$. □

A principal ideal domain (or PID) is a domain in which every ideal is principal. Both $\mathbb{Z}$ and $F[x]$ are PIDs.

Example. Most domains are not PIDs. Here is one: $D = \mathbb{Z}[x]$, the set of polynomials with integer coefficients.

Let $I$ be the set of polynomials $f = \sum_{k=0}^{n} a_k x^k$ with integer coefficients ($a_k \in \mathbb{Z}$) such that $a_0$ is an even integer. Exercise. $I$ is an ideal in $\mathbb{Z}[x]$. Exercise. $I = (2, x)$. Harder exercise. $I$ is not principal, i.e., there is no $g \in \mathbb{Z}[x]$ such that $I = (g)$. (Idea: the identity $\deg(fg) = \deg(f) + \deg(g) \ldots$)