1-28-1994

Polynomial rings.

If R is a ring, the **ring of polynomials in x with coefficients in R** is denoted $R[x]$. It consists of all formal sums

$$\sum_{i=0}^{\infty} a_i x^i,$$

where $a_i = 0$ for all but finitely many values of i.

(If the idea of "formal sums" worries you, replace a formal sum with the infinite vector whose components are the coefficients of the sum.)

If $n > 0$ and $a_n \neq 0$, and n is the largest integer with this property, the polynomial has **degree** n. A nonzero constant polynomial has degree 0. The zero polynomial is defined by convention to have degree $-\infty$. (This is necessary in order to make the dgree formulas work out.)

Polynomials are added componentwise, and multiplied using the "convolution" formula:

$$\sum_{i=0}^{\infty} a_i x^i + \sum_{i=0}^{\infty} b_i x^i = \sum_{i=0}^{\infty} (a_i + b_i) x^i$$

$$\left(\sum_{i=0}^{\infty} a_i x^i\right) \cdot \left(\sum_{j=0}^{\infty} b_j x^j\right) = \sum_{i=0}^{\infty} c_k x^k, \quad \text{where} \quad c_k = \sum_{i+j=k} a_i b_j$$

These formulas say that you compute sums and products as usual.

If $f \in R[x]$, write $\deg f$ to denote the degree of f. It's easy to show that the degree function satisfies the following properties:

$$\deg(f + g) = \max(\deg f, \deg g)$$

$$\deg(f \cdot g) = \deg f + \deg g$$

The verifications amount to writing out the formal sums (with a little attention paid to the case of the zero polynomial).

Example. Recall that a **unit** in a ring R is an element which has a multiplicative inverse. Let F be a field, and let $F[x]$ be the polynomial ring in one variable over F. The units in $F[x]$ are exactly the nonzero elements of F.

It's clear that the nonzero elements of F are invertible in $F[x]$, since they're already invertible in F. Suppose conversely that $f(x) \in F[x]$ is invertible, so $f(x)g(x) = 1$ for some $g(x) \in F[x]$. Then $\deg f + \deg g = \deg 1 = 0$, which is impossible unless f and g both have degree 0. In particular, f is a nonzero constant, i.e. an element of F. $\square$

The degree function in $R[x]$ is a special case of a **valuation**.

Definition. Let R be an integral domain. A **Euclidean valuation** on R is a function $\nu : R - \{0\} \to \mathbb{Z}^+ \cup \{0\}$ which satisfies the following properties:

(a) For all $f, g \in R$, $g \neq 0$, there exist $q, r \in R$ such that

$$f = gq + r, \quad \text{and either} \quad r = 0 \quad \text{or} \quad \nu(r) < \nu(g).$$

(b) If $f, g \in R$ and $f, g \neq 0$, then $\nu(f) \leq \nu(fg)$.

An integral domain with a Euclidean valuation is called a **Euclidean domain**.

Obviously, the intent of property (a) is to imitate the Division Algorithm. Property (b) is clearly satisfied by the degree function for a polynomial ring.

Example. The absolute value function $|\cdot|$ on $\mathbb{Z}$ is a Euclidean valuation. $\square$

Recall that an ideal I in a commutative ring R is **principal** if $I = \langle x \rangle = Rx$. That is, the ideal consists of all multiples of a single element by ring elements. A PID (**principal ideal domain**) is an integral domain in which every ideal is principal.

Theorem. Every Euclidean domain is a PID.

Proof. The idea is to use property (a) as substitute for the Division Algorithm and emulate the proof that subgroups of cyclic groups are cyclic.

Let R be a Euclidean domain. Let I be an ideal. I want to show that I is principal. As usual, a candidate for a generator ought to be "smallest" in some sense, and the valuation ν provides a way of measuring "smallness".

First, if $I = \{0\}$, then $I = \langle 0 \rangle$, which is principal.

Assume then that $I \neq \{0\}$, and consider the set

$$\{\nu(x) \mid x \in I, x \neq 0\}.$$

This is a subset of the nonnegative integers, and by well-ordering it must have a smallest element $\nu(x_0)$, where $x_0 \in I$ and $x_0 \neq 0$. I claim that $I = \langle x_0 \rangle$.

Let $x \in I$. By property (a), there are elements q and r such that

$$x = qx_0 + r, \quad \text{and either} \quad r = 0 \text{ or } \nu(r) < \nu(g).$$

However, $x \in I$, $qx_0 \in I$, so $r = x - qx_0 \in I$. It follows that $\nu(r) < \nu(x_0)$ is impossible, since x_0 was an element of minimal ν in I. Therefore, $r = 0$, and $x = qx_0$. Hence, $I = \langle x_0 \rangle$, and R is a PID. $\square$

Theorem. (**Division Algorithm**) Let F be a field, and let $f, g \in F[x]$. Suppose that $g \neq 0$. There exist $q, r \in F[x]$ such that

$$f(x) = g(x)q(x) + r(x), \quad \text{and} \quad \deg r(x) < \deg g(x).$$

Proof. The idea is to imitate the proof of the Division Algorithm for $\mathbb{Z}$.

Let

$$S = \{f(x) - g(x)q(x) \mid q(x) \in F[x]\}.$$

The set $\{\deg s(x) \mid s(x) \in S\}$ is a subset of the nonnegative integers, and therefore must contain a smallest element by well-ordering. Let $r(x) \in S$ be an element in S of smallest degree, and write

$$r(x) = f(x) - g(x)q(x), \quad \text{where} \quad q(x) \in F[x].$$

I need to show that $\deg r(x) < \deg g(x)$.

If $r(x) = 0$, then since $g(x) \neq 0$, $\deg g(x) \geq 0 > -\infty = \deg r(x)$.

Suppose then that $r(x) \neq 0$. Assume toward a contradiction that $\deg r(x) \geq \deg g(x)$. Write

$$r(x) = r_n x^n + \cdots + r_1 x + r_0$$

$$g(x) = g_m x^m + \cdots + g_1 x + g_0$$

where $r_n, g_m \neq 0$, and $n \geq m$.

The polynomial

$$r(x) - \frac{r_n}{g_m} x^{n-m} g(x) = (r_n x^n + \cdots + r_1 x + r_0) - \left(r_n x^n + \frac{r_n}{g_m} x^{n-1} + \cdots\right)$$

will have degree less than n, since the n-th degree terms cancel out.

However,

$$r(x) - \frac{r_n}{g_m} x^{n-m} g(x) = f(x) - g(x)q(x) - \frac{r_n}{g_m} x^{n-m} g(x) = f(x) - g(x)\left(q(x) + \frac{r_n}{g_m} x^{n-m} g(x)\right),$$

which is an element of S.

I've found an element of S of smaller degree than $r(x)$, which is a contradiction. $\times$ It follows that $\deg r(x) < \deg g(x)$, and this completes the proof. □

Corollary. If F is a field, then $F[x]$ is a Euclidean domain with the degree function as a valuation.

Proof. $\deg f \le \deg(fg)$, and the Division Algorithm shows that property (a) for a valuation holds. □

Corollary. Let F be a field, and let $f(x) \in F[x]$, where $\deg f(x) = n \ge 0$. Then:

(a) If c is a root of $f(x)$ in F, then $x - c \mid f(x)$.

(b) $f(x)$ has at most n roots in F.

Proof. (I haven't discussed **roots** of polynomials formally, but I'll take the usual intuitive notion as a guide, since it won't cause any problems. A more careful discussion will come later.)

Suppose $f(c) = 0$. Write

$$f(x) = (x - c)q(x) + r(x), \quad \text{where} \quad \deg r(x) < \deg(x - c) = 1.$$

Then $\deg r(x) = 0$ or $\deg r(x) = -\infty$.

In the first case, r is a nonzero constant. However, this implies that

$$0 = f(c) = 0 \cdot g(c) + r(c) \neq 0. \times$$

Hence, $r(x) = 0$, and $f(x) = (x - c)q(x)$.

If $c_1, \ldots, c_m$ are the distinct roots of f in F, then

$$(x - c_1) \cdots (x - c_m) \mid f(x).$$

Taking degrees on both sides gives $m \le \deg f(x)$. □

Example. The quadratic polynomial $(x - 2)(x - 6) \in \mathbb{Z}_{12}[x]$ has roots $x = 0$, $x = 2$, $x = 6$, $x = 8$. The previous result does not apply, because $\mathbb{Z}_{12}$ is not a field. □

Definition. An element r in a ring R is **irreducible** if and only if $r = ab$ implies that either a or b is a unit.

Example. If F is a field, then the units in $F[x]$ are exactly the nonzero elements of F. A polynomial $f(x) \in F[x]$ is irreducible if and only if $f(x) = g(x)h(x)$ implies that either g or h is a constant. $x^2 + 1$ is irreducible in $\mathbb{Q}[x]$; it is not irreducible in $\mathbb{C}[x]$, because $x^2 + 1 = (x + i)(x - i)$. □

Corollary. Let F be a field. A polynomial of degree 2 or 3 in $F[x]$ is irreducible if and only if it has no roots in F. □