Thus, if p is irreducible, then $F[x]/(p)$ is a field. Now, $F[x]/(p)$ is the set of all cosets of (p), i.e.,

$$F[x]/(p) = \{ q + (p) : q \in F[x] \}$$

But what are these cosets? Is it possible to give a better description of $F[x]/(p)$?

Exercise

Let F be a field, & let p be an irreducible polynomial in $F[x]$.

a. Let f be any polynomial in $F[x]$. Use the Division Algorithm to write

$$f = pq + r, \qquad r=0 \text{ or } 0 \le \deg(r) < \deg(p)$$

Show that f & r determine the same coset, i.e.,

$$f + (p) = r + (p).$$

b. Show that

$$F[x]/(p) = \{ r + (p) : r = 0 \text{ or } 0 \le \deg(r) < \deg(p) \}$$

Is this a listing <u>without</u> duplication? That is, does each polynomial r with $\deg(r) < \deg(p)$ determine a unique coset $r + (p)$?

c. If F is finite, how many cosets are there in $F[x]/(p)$? In particular, is $F[x]/(p)$ a finite field?

<u>Remark</u>

If writing (p) is notationally confusing, let $I = (p)$ and use that instead, e.g.,

$$F[x]/I = \{ f + I : f \in F[x] \}.$$

Factorization of Polynomials

As we know, every positive integer has a unique factorization as a product of powers of primes. The next result is the analogous theorem for polynomials over a field.

Theorem
Let F be a field, & choose $f \in F[x]$ with $\deg(f) \geq 1$.

Then either f is itself irreducible, or it can be written as a product of irreducible polynomials.

In fact,

$$f = a p_1^{m_1} \cdots p_k^{m_k} \qquad (*)$$

where: $k \geq 1$,

$a \in F$ is the leading coefficient of f,

$p_1, \ldots, p_k$ are monic & irreducible,

$m_1 > 0, \ldots, m_k > 0$.

The factorization in $(*)$ is unique up to the order of the p_k.

Proof:
We first show that f is either irreducible or is a product of irreducible polynomials. We proceed by induction on the degree of f.

Base step: $\deg(f) = 1$.

In this case $f(x) = ax + b$ with $a, b \in F$, $a \neq 0$.

Exercise: Show f is irreducible

Inductive step: Suppose the result is true for all polynomials of degree $1, \ldots, \deg(f) - 1$.

Now, if f is irreducible, then the result is true for f. So, we need to examine the case where f is not irreducible. In this case, we can write

$f = ab$ where $1 \leq \deg(a), \deg(b) < \deg(f)$.

But then by the inductive hypothesis,

$$a = c\, p_1^{m_1} \cdots p_k^{m_k} \quad \& \quad b = d\, q_1^{n_1} \cdots q_l^{n_l}$$

where $c, d \in F$ and p_i, q_i are irreducible. Hence

$$f = (cd)\, p_1^{m_1} \cdots p_k^{m_k} q_1^{n_1} \cdots q_\ell^{n_\ell}$$

is a product of irreducible polynomials - some p_i may equal some q_j, but this is not a problem.

The proof of uniqueness is similar, by induction on the degree of f - see the text for proof. ∎

Why are the integers & polynomial rings over fields so similar? The important fact in each is that it is possible to compare the "size" of elements of the ring: in the integers we have the usual ordering $1 \leq 2 \leq 3 \leq \cdots$, while in the ring $F[x]$ we have the degree of the polynomial to tell us its "size." Size is no longer an injective function on $F[x]$ (two different polynomials may have the same degree), but we have the Division Algorithm & the behavior of the degree under multiplication. Any ring that has analogues of these properties will share the properties of $\mathbb{Z}$ & $F[x]$. Such a ring is called a Euclidean ring, defined precisely as follows.

Definition

An integral domain R is a *Euclidean ring* or a *Euclidean domain* if there is a *Euclidean function* $f: R^* = R \setminus \{0\} \longrightarrow \mathbb{N}$ that satisfies:

a. $\forall\, a \neq 0, b \neq 0, \quad d(a) \leq d(ab)$

b. If $a \neq 0$ then for every $b \neq 0$ we can write

$$b = aq + r$$

where $q, r \in R$ and either $r = 0$ or $d(r) < d(a)$.

It can be shown that:

Euclidean domain $\Rightarrow$ Principal Ideal Domain (PID) $\Rightarrow$ Unique Factorization Domain (UFD) $\Rightarrow$ Integral Domain