Polynomials

We have already talked about polynomials. I will stick with the "intuitive approach" [rather than the *formal* one].

Since we've talked about and used polynomials before, I will skip most of this section.

Read the text (Section 4.5) if you are not comfortable with polynomials!

Degree

Theorem

If R is a domain, then for $f, g \in R[x]$, we have:

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

and

$$\deg(f + g) \leq \max\{\deg(f), \deg(g)\}.$$

The equality in the expression above always hold if $\deg(f) \neq \deg(g)$.

Remember: if $a \in R \setminus \{0\}$, then $\deg(a) = 0$ and $\deg(0) = -\infty$.

Division Algorithm

We've already discussed the *division algorithm*: given $f, g \in R[x]$, with $g \neq 0$ and its leading coefficient [i.e., the coefficient of the term of highest degree] is a *unit*, then there are $q, r \in R[x]$ such that

$$f = g \cdot q + r, \qquad \text{where } \deg(r) < \deg(g).$$

In particular, if R is a field, and $g \neq 0$, then we have q and r as above.

The procedure to find q and r is exactly the same as the one you've learned for $\mathbb{R}[x]$ in algebra or precalculus. [*If you forgot it, review!*]

Division by Polynomial of Degree One

Let's work in $R[x]$ where R is a domain. Dividing $f(x)$ by $g = x - a$, where $a \in R$, we have that

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

Hence, $r \in R$ [a constant]. Evaluating at $x = a$, we have

$$f(a) = (a-a) \cdot q(a) + r(a) = r,$$

i.e., $r = f(a)$. So,

$$f = (x-a)q + f(a), \qquad \text{for some } q \in R[x].$$

Corollary

If R is a domain and $a \in R$, then $(x-a)$ divides $f \in R[X]$ iff $f(a) = 0$.

Number of Roots

Corollary

If R is a domain and $\deg(f) = n \geq 0$, then f has at most n roots in R.

Proof.

Proceed by induction. The case $n = 0$ is trivial.
Now, assume true for $(n-1)$ and let $\deg(f) = n$. If f has no roots in R, we are done. So, assume $a \in R$ and $f(a) = 0$. Then, $f = (x - a)g$, for some $g \in R[x]$. Then, $\deg(g) = n - 1$. By the IH, g has at most $(n-1)$ roots in R.
Now, we claim if $f(b) = 0$, for $b \in R$, then either $a = b$ or $g(b) = 0$: we have that $0 = f(b) = (b - a) \cdot g(b)$. Since R is a domain [and $(b - a), g(b) \in R$], we have that either $b - a = 0$ or $g(b) = 0$, proving the claim and finishing the proof. □

Other Remarks

Note that if R is not a domain, the above result is not necessarily true: let $R = \mathbb{Z}/6\mathbb{Z}$ and $f = 2x$. Then $x = 0, 3$ are two distinct roots of f [and $\deg(f) = 1$].

We have seen in class that $F[x]$, where F is a field, is a PID [and hence noetherian and a UFD]. The idea is that we can do the long division by every non-zero element of $F[x]$. [Given I and ideal of $F[x]$, take f as an element of I with least degree. Use long division to show that $I = (f)$.]

Note that we also have an Euclidean algorithm, exactly the same as for $\mathbb{Z}$, which allows us to *explicitly* write GCDs as linear combinations of elements. [Domains in which we have an "Euclidean Algorithm" are called **Euclidean Domains**. These are always PIDs, and hence also UFDs and noetherian.]