

GCDs and Other Beastly Beasts

At this point in our discussion your textbook lists a few cool consequences of the Division Algorithm as applied to polynomials: see pages 256 and 257 for details. I encourage you to examine a couple of these results involving polynomials as functions.

Let's move on to a different but related topic: common divisors.

Definitions. If k is a field and $f(x), g(x) \in k[x]$ then any $c(x) \in k[x]$ such that $c(x)|f(x)$ and $c(x)|g(x)$ is called a _____ of f and g .

If at least one of f and g is not the zero polynomial, then a _____ of f and g , denoted $(f(x), g(x))$, is a monic _____ $d(x) \in k[x]$ of $f(x)$ and $g(x)$ of least degree. (Recall that $d(x)$ is called *monic* if its leading coefficient is 1_k .) If $f = g = 0$ holds, then $(f(x), g(x)) = 0$ by definition.

The first question is an existence issue (then we'll get on to one of "form"):

Proposition (3.56). If k is a field, then (f, g) is defined for any pair of polynomials $f, g \in k[x]$.

Proof. Obviously we may assume that at least one of f and g is nonzero. In this case, the set of common divisors is nonempty. Why?

Moreover, the degree of any common divisor is bounded above by a certain fixed value. Which value is that?

Thus we can pick a common divisor (there exists at least one!) of maximal degree. Why can we always find a *monic* one?

Example. At this point we have only very simplistic methods for computing greatest common divisors. How, for example, can you compute $(2x^2 + x - 3, x^2 - 2x + 1)$ in $\mathbb{Z}[x]$?

Now let's show that (f, g) can be written in a very particular manner (this should look familiar!):

Theorem (3.57). If k is a field and $f, g \in k[x]$ then a greatest common divisor (f, g) can be written as a linear combination of f and g . That is, there exist polynomials $s(x), t(x) \in k[x]$ such that

$$(f(x), g(x)) = s(x)f(x) + t(x)g(x).$$

Proof. Assuming either $f \neq 0$ or $g \neq 0$ (why can we assume this?), let's consider the set

$$I = \{s(x)f(x) + t(x)g(x) \mid s, t \in k[x]\}.$$

Before we get started, this notation suggests *what* about the set I ?

How are we guaranteed that $I \neq \emptyset$?

Since $I \neq \emptyset$, we can pick a monic polynomial $d(x)$ of *least* degree in I . How can we be sure that $d(x)$ is indeed monic?

Since d has the form we want it to, all we have to do is show that it's a greatest common divisor.

First of all, we can use the Division Algorithm to show that $d|f$:

Similarly $d|g$. Now suppose $c(x)$ is any other common divisor of f and g . How can we show that $c|d$ (and thus that $\deg(c) \leq \deg(d)$)?

From the proof above follows the uniqueness of the greatest common divisor:

Corollary (3.58). Let k be a field and $f, g \in k[x]$. Then (f, g) exists and is unique.

Proof. Let d and d' both be greatest common divisors. Since $d|d'$ and $d'|d$, we can show that $d' = ud$ for some unit $u(x) \in k[x]$. But what do units in $k[x]$ look like, and what's this say about d and d' , since both are monic?