A Few Notes on Field Theory (WIP)

David Meyer

dmm@{1-4-5.net,uoregon.edu}

Last update: September 23, 2019

1 Introduction

TBD

2 Fields and the Division Algorithm

Definition 2.1. Let f and g be polynomials in $F[x]$. Then we say that f divides g, or g is divisible by f, if there is a polynomial h with $g = fh$.

For integers, the greatest common divisor of two integers a and b is the largest integer dividing both a and b. This definition doesn't quite work for polynomials. In particular, while we cannot talk about "largest" polynomial in the same manner as we do for integers, we can talk about the degree of a polynomial.

Recall that the degree of a nonzero polynomial f is the largest integer m for which the coefficient a_m of x^m is nonzero. For example, if $f(x) = a_n x^n + \ldots + a_1 x + a_0$ with $a_n \neq 0$, then the degree of $f(x)$, written $\deg f$, is n. The degree function allows us to measure size of polynomials.

There is one extra complication with this definition of $\deg f$. Consider for example that any polynomial of the form ax^2 with $a \neq 0$ divides x^2 and x^3. Thus, there isn't a unique polynomial of highest degree that divides a pair of polynomials. To pick one out, we consider monic polynomials, polynomials whose leading coefficient is 1. For example, x^2 is the monic polynomial of degree 2 that divides both x^2 and x^3, while $5x^2$ is not monic.

As a piece of terminology, we will refer to an element $f \in F[x]$ as a polynomial over F .

Definition 2.2. Let f and g be polynomials over F, where f and g are not both zero. Then a greatest common divisor of f and g, $\gcd(f, g)$, is a monic polynomial of largest degree that divides both f and g.

The problem with Definition 2.2 has to do with uniqueness. Could there be more than one greatest common divisor of a pair of polynomials? The answer is no, and we will prove this after we prove the analogue of the division algorithm. The main reason for assuming that the coefficients of our polynomials lie in a field is to ensure that the division algorithm is valid. Before we prove it, we need a simple lemma about degrees. For convenience, we set $\deg 0 = -\infty$. We also make the convention that $-\infty + -\infty = -\infty$ and $-\infty + n = -\infty$ for $n \in \mathbb{Z}$. The point of these conventions is to make the statement in the following lemma and other results as simple as possible.

Lemma 2.1. Let F be a field and let f and g be polynomials over F. Then $\deg fg = \deg f + \deg g$.

Proof: If either $f = 0$ or $g = 0$, then the equality $\deg fg = \deg f + \deg g$ is true by our convention above. So, suppose that $f \neq 0$ and $g \neq 0$. Write $f = a_n x^n + \ldots + a_0$ and $g = b_m x^m + \ldots + b_0$ with $a_n \neq 0$ and $b_m \neq 0$. Therefore, $\deg f = n$ and $\deg g = m$. The definition of polynomial multiplication yields

$$fg = (a_n b_m)x^{(n+m)} + (a_n b_{m-1} + a_{n-1} b_m)x^{n+m-1} + \ldots + a_0 b_0$$

Since every field is an integral domain and since the coefficients come from a field we know that there are no zero divisors and so we can conclude that $a_n b_m \neq 0$, and so $\deg fg = n + m = \deg f + \deg g$, as desired. $\square$

Proposition 2.1. (Division Algorithm) Let F be a field and let f and g be polynomials over F with f nonzero. Then there are unique polynomials q and r with $g = qf + r$ with $\deg r < \deg f$.

Proof: Let $\mathcal{S} = \{t \in F[x] \mid t = g - qf \text{ for some } q \in F[x]\}$. Now, we know $\mathcal{S} \neq \emptyset$ since $g \in \mathcal{S}$ (see Equation 2 below). We also know that by the well ordering property of the integers [1] there is a polynomial r of least degree in $\mathcal{S}$. By definition there is a $q \in F[x]$ with $r = g - qf$ so $g = qf + r$.

So we need to see that $\deg r < \deg f$. So suppose that $\deg r \geq \deg f$, say with $n = \deg f$ and $m = \deg r$. If $f = a_n x^n + \ldots + a_0$ and $r = r_m x^m + \ldots + r_0$ with $a_n \neq 0$ and $r_m \neq 0$, then by the method of long division of polynomials, we see that $r = (r_m a_n^{-1})x^{m-n} f + r'$ with $\deg r' < m = \deg r$. But then

$$\begin{array}{rcll} g & = & gf + r & \# \; g \in \mathcal{S} \text{ and well ordering principle} \\ & = & qf + (r_m a_n^{-1})x^{m-n} f + r' & \# \; r = (r_m a_n^{-1})x^{m-n} f + r' \\ & = & (q + r_m a_n^{-1} x^{m-n})f + r' & \# \text{ factor out } f \\ & \Longrightarrow & r' \in \mathcal{S} & \# \; r' = g - (q + r_m a_n^{-1} x^{m-n})f \in \mathcal{S} \end{array}$$

Since $\deg r' < \deg r$, $r' \in \mathcal{S}$ contradicts our choice of r (the assumption that r was the polynomial of least degree in $\mathcal{S}$). Therefore $\deg r \geq \deg f$ is false so $\deg r < \deg f$ is true and this proves existence of q and r.

We still have to show the uniqueness of q and r. To do this, suppose that $g = qf + r$ and $g = q'f + r'$ for some polynomials $q, q', r, r' \in F[x]$, and with both $\deg r < \deg f$ and $\deg r' < \deg f$. Then $qf + r = q'f + r'$, so $(q - q')f = r' - r$. Taking degrees and using Lemma 2.1, we have

$$\deg(q - q') + \deg f = \deg(r' - r) \tag{1}$$

Since $\deg r < \deg f$ and $\deg r' < \deg f$, we have $\deg(r' - r) < \deg f$. However, if $\deg(q' - q) \geq 0$ (and we know that $\deg(r' - r) < \deg f$), we get a contradiction of Equation 1. In particular, the only way for this to happen is for $\deg(q' - q) = \deg(r' - r) = -\infty$, and the only way for that to happen is if $q' - q = 0 = r' - r$. So $q' = q$ and $r' = r$, which shows uniqueness. $\square$

Proposition 2.2. Let F be a field and let f and g be polynomials over F, with not both f and g zero. Then $\gcd(f, g)$ exists and is unique. Furthermore, there are polynomials h and k with $\gcd(f, g) = hf + kg$.

Proof: Here we have to show that $\gcd(f, g)$ exists and that it is unique. To show that $\gcd(f, g)$ exists, let $\mathcal{S} = \{hf + kg : h, k \in F[x]\}$. Then $\mathcal{S}$ contains nonzero polynomials f and g (at least), since for some $f' \in \mathcal{S}$

$$\begin{array}{rcll} f' & = & hf + kg & \text{\# definition of elements of } \mathcal{S} \\ & = & 1 \cdot f + 0 \cdot g & \text{\# let } h = 1 \text{ and } k = 0 \\ & = & f & \text{\# so } f \in \mathcal{S} \end{array} \tag{2}$$

Likewise for g (let $h = 0$ and $k = 1$). So $f, g \in \mathcal{S}$. But this means that there is a nonzero polynomial $d \in \mathcal{S}$ of smallest degree by the well ordering principle [1], so we can write $d = hf + kg$ for some $h, k \in F[x]$. By dividing by the leading coefficient of d, we may assume that d is monic without changing the condition that d is the polynomial of least degree in $\mathcal{S}$.

Now the claim is that $d = \gcd(f, g)$. To show that d is a common divisor of f and g, first consider f. By the division algorithm, we can write f as $f = qd + r$ for some polynomials q and r with $\deg(r) < \deg(d)$. Then

$$
\begin{array}{lcll}
f & = & qd + r & \# \ f \in \mathcal{S} \text{ by Equation 2}, \mathcal{S} \text{ has a division algorithm} \\
& \implies & r = f - qd & \# \text{ solve for } r \\
& \implies & r = f - q(hf + kg) & \# \ d = hf + kg \\
& \implies & r = f - qhf - qkg & \# \text{ arithmetic} \\
& \implies & r = (1 - qh)f + (-qk)g & \# \ F[x] \text{ is closed under } */+ \text{ so } r \text{ is of the form } hf + kg \\
& \implies & r \in \mathcal{S} & \# \ \mathcal{S} = \{hf + kg : h, k \in F[x]\}
\end{array}
\tag{3}
$$

So $r \in \mathcal{S}$. Now, if $r \neq 0$ we have contradiction since we assumed that $\deg(r) < \deg(d)$ and that d was the polynomial of lowest degree in $\mathcal{S}$. Thus r must equal 0, which shows that $f = qd$, and so d divides f. Similarly, d divides g and so d is a common divisor of f and g.

If e is any other common divisor of f and g, then e divides any combination of f and g; in particular, e divides $d = hf + kg$. This forces $\deg(e) \leq \deg(d)$ by Lemma X. Thus, d is the monic polynomial of largest degree that divides f and g, so d is a greatest common divisor of f and g. This shows that $\gcd(f, g)$ exists.

To show that $\gcd(f, g)$ is unique, suppose that d and d' are both monic common divisors of f and g of largest degree. By Equation 3, we can write both d and d' as combinations of f and g. In addition, the argument above shows that d divides d' and vice-versa. If $d' = ad$ and $d = bd'$, then $d = bd' = bad$. Taking degrees shows that $\deg(ba) = 0$, which means that a and b are both constants. However since d and d' are monic, for $d' = ad$ to be monic it must be that $a = 1$. Thus, $d' = ad = d$. This shows that the greatest common divisor is unique, completing the proof.

3 Acknowledgements

References

[1] MIT OCW. The Well Ordering Principle. https://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-042j-mathematics-for-computer-science-spring-2015/readings/MIT6_042JS15_Session3.pdf, 2015. [Online; accessed 23-Sep-2019].