2.2 Euclidean Domains

The sets of integers and of polynomials (for any field of coefficients) have:

(a) Addition that associates and commutes.

(b) An additive identity element 0 and additive inverses of everything.

(c) Multiplication that associates, commutes and distributes with addition.

(d) A multiplicative identity element 1.

(e) A cancellation rule: if $a \neq 0$ and $ab = ac$, then $b = c$.

(f) Division with remainders.

Any set D with addition and multiplication rules that has all the properties (a)-(e) above is called an **integral domain**. A field is one kind of integral domain, and the integers and polynomials are another. Condition (f) will be part of the definition of a **Euclidean domain**.

Definition: An element $a \in D$ of an integral domain is called a **unit** if it has a multiplicative inverse element, which we denote a^{-1} or $1/a$. There is always at least one unit in any integral domain, namely the multiplicative identity 1.

Note: Units are the things we call "not interesting" when we factor.

Examples: (a) In a field F, all the elements except 0 are units.

(b) In $F[x]$, the constant polynomials are the units (Corollary 2.1.2).

(c) 1 and -1 are the integer units.

Definition: A function:

$$\deg : D - \{0\} \to \mathbb{R}^+ \cup \{0\}$$

is called a **degree function** if it has the following properties:

(i) deg converts multiplication to addition:

$$\deg(ab) = \deg(a) + \deg(b)$$

(ii) deg detects the units of the integral domain:

$$\deg(a) = 0 \text{ if and only if } a \text{ is a unit}$$

Example: The degree of a polynomial in §2.1 is a degree function:

$$\deg(a(x)) = \text{ the ordinary degree of } a(x)$$

This is what Proposition 2.1.1 and Corollary 2.1.2 tell us. Notice that the range of this degree function is the set of whole numbers.

To define the degree of an *integer*, I need to remind you of the:

Natural Logarithm: This is defined for all positive real numbers by:

$$\ln(x) = \int_1^x \frac{1}{t} dt$$

from which it follows immediately that $\ln(1) = 0$ and

$$\ln(x) < \ln(y) \quad \text{whenever} \quad x < y$$

(in other words, $\ln(x)$ is an **increasing** function of x).

If x and y are fixed positive real numbers, then:

$$\int_x^{xy} \frac{1}{t} dt = \int_1^y \frac{1}{xs}(xds) = \int_1^y \frac{1}{s} ds = \ln(y)$$

using the substitution $t = xs$ (and $dt = xds$). But then:

$$\ln(xy) = \int_1^{xy} \frac{1}{t} dt = \int_1^x \frac{1}{t} dt + \int_x^{xy} \frac{1}{t} dt = \ln(x) + \ln(y)$$

Proposition 2.2.1. *The "natural log of the absolute value:"*

$$deg(a) = ln(|a|)$$

is a degree function for the integers.

Proof: If $a = 0$, then $\deg(a) = \ln(0)$ is undefined. Otherwise $|a| \geq 1$, and then $\deg(a) = \ln(|a|) \geq 0$, so deg has the required domain and range.

Next, -1 and 1 are the only integers with $\ln(|a|) = 0$, and these are the integer units. This gives Property (ii). And finally,

$$\ln(|ab|) = \ln(|a||b|) = \ln(|a|) + \ln(|b|)$$

is what we require for Property (i). So $\ln(|a|)$ is a degree function.

Remark: The smallest range of this degree function is $\{0 = \ln(1), \ln(2), \ln(3), ...\}$ which is not the set of whole numbers, but like the set of natural numbers and the set of whole numbers, this set **does** satisfy the well-ordered axiom. This will be important for us later.

Definition: An integral domain D with degree function is called a **Euclidean domain** if it has division with remainders: For all $a, b \in D - \{0\}$, either:

(a) $a = bq$ for some q, so b **divides** a (b is a **factor** of a), or else:

(b) $a = bq + r$ with $\deg(r) <\ \deg(b)$, and r is the **remainder**.

Examples: (a) $F[x]$ is a Euclidean domain, with the ordinary degree function.

(b) $\mathbb{Z}$ is a Euclidean domain with $\log(|a|)$ as its degree function.

Confession: We saw in §1.1 that $\mathbb{N}$ (not $\mathbb{Z}$) has division with remainders. This can easily be modified to incorporate the negatives, however. In fact, it works even better when we allow negative remainders, since we can make their absolute values even smaller. That is, we can arrange:

$$a = bq + r \text{ with } |r| \leq \frac{1}{2}|b|$$

which the degree function sees as $\deg(r) \leq \deg(b) - \log(2)$.

Example: Divide 1000 by 501 with remainders:

As natural numbers: $1000 = 501(1) + 499$ with a (large) remainder of 499.

As integers: $1000 = 501(2) + (-2)$ with a (much smaller) remainder of -2.

Another Example: Divide 900 by 200 with remainders:

As natural numbers: $900 = 200(4) + 100$.

As integers, we could take that or equally well: $900 = 200(5) + (-100)$

In general, when $|r| = \frac{1}{2}|b|$, there are two possibilities for r.

Now that we have a general definition of a Euclidean domain, we'll reexamine Euclid's algorithm and refine the fundamental theorem of arithmetic for integers and polynomials (and all Euclidean domains).

Euclid's algorithm: If D is a Euclidean domain and the degree function has a range set that satisfies the well-ordered axiom, then each sequence of divisions with remainders eventually stops:

$$\begin{array}{ccccc} a & = & bq_1 & + & r_1 \\ b & = & r_1q_2 & + & r_2 \\ r_1 & = & r_2q_3 & + & r_3 \\ & \vdots & & & \\ r_k & = & r_{k+1}q_{k+2} & & \text{STOP} \end{array}$$

and the last remainder r_{k+1} is a common divisor of greatest degree.

Proof: First, we prove that each of the sequences of divisions with remainders eventually stops. Given one of them, consider the set of all degrees of all the remainders:

$$S = \{\deg(r_1), \deg(r_2), \deg(r_3), ...\}$$

Since $\deg(r_1) > \deg(r_2) > \deg(r_3) > ...$, the well-ordered axiom says there is smallest element of S, which is the degree of the last remainder!

To see that r_{k+1} is a common divisor of a and b, we work our way back up Euclid's algorithm, starting with the last line. Namely:

$$r_k = r_{k+1}q_{k+2}$$

shows that r_{k+1} divides r_k.

Next:

$$\begin{array}{rcccc} r_{k-1} & = & r_k q_{k+1} & + & r_{k+1} \\ & = & (r_{k+1} q_{k+2}) q_{k+1} & + & r_{k+1} \\ & = & r_{k+1} (q_{k+2} q_{k+1} & + & 1) \end{array}$$

shows that r_{k+1} divides r_{k-1}. As we work our way up and substitute, we see that r_{k+1} divides **all** the remainders, and it divides a and b as well, so that r_{k+1} is a common divisor of a and b (and all other remainders, too!).

To see that r_{k+1} has greatest degree among all the common divisors, we work our way down Euclid's algorithm. The first equation:

$$a = bq_1 + r_1$$

can be rewritten as

$$r_1 = a + (-q_1)b$$

showing that r_1 is a linear combination of a and b. Then:

$$r_2 = b + (-q_2)r_1 = b + (-q_2)(a + (-q_1)b) = (-q_2)a + (1 + q_1 q_2)b$$

so r_2 is a linear combination of a and b, too, and as we work our way down, every remainder is a linear combination of a and b, down to:

$$r_{k+1} = ua + vb$$

for some pair of elements $u, v \in D$.

Now if d is any common divisor of a and b, then $a = dq$ and $b = dq'$, and:

$$r_{k+1} = udq + vdq' = d(uq + vq') \text{ so } d \text{ divides } r_{k+1}$$

But then

$$\deg(d) + \deg(uq + vq') = \deg(r_{k+1})$$

so $\deg(d) \leq \deg(r_{k+1})$. Thus r_{k+1} has the possible greatest degree of any common divisor of a and b!

Definition: A common divisor of greatest degree will be called a **gcd**.

Two Examples: First, an integer example. Start with 750 and 144.

$$\begin{array}{rcl} 750 & = & 144(5) + 30 \\ 144 & = & 30(5) + (-6) \\ 30 & = & (-6)(-5) \end{array}$$

First we go up Euclid's algorithm and substitute:

$$\begin{array}{rclclcl} 30 & = & (-6)(-5) & & & & \\ 144 & = & 30(5) + (-6) & = & (-6)(-5)(5) + (-6) & = & (-6)(-24) \\ 750 & = & 144(5) + 30 & = & (-6)(-24)(5) + (-6)(-5) & = & (-6)(-125) \end{array}$$

to see that -6 is a common divisor of 144 and 750.

Then we go down Euclid's algorithm:

$$\begin{array}{rclcl} 30 & = & 750+144(-5) & & \\ -6 & = & 144+30(-5) & = & 144+(750+144(-5))(-5) \\ & & & = & 750(-5)+144(26) \end{array}$$

to see that -6 is a linear combination of 750 and 144.

Next, a polynomial example. Start with x^4-1 and x^3+x in $\mathbb{Q}[x]$.

$$\begin{array}{rcl} x^4-1 & = & (x^3+x)(x)+(-x^2-1) \\ x^3+x & = & (-x^2-1)(-x) \end{array}$$

First we go up Euclid's algorithm and substitute:

$$\begin{array}{rclcl} x^3+x & = & (-x^2-1)(-x) & & \\ x^4-1 & = & (x^3+x)(x)+(-x^2-1) & = & (-x^2-1)(-x)(x)+(-x^2-1) \\ & & & & (-x^2-1)(-x^2+1) \end{array}$$

to see that $-x^2-1$ is a common divisor. Then we go down:

$$(-x^2-1) \quad = \quad (x^4-1)+(x^3+x)(-x)$$

to see that $-x^2-1$ is a linear combination of the polynomials.

Note: Unlike the natural numbers, gcd's in $\mathbb{Z}$ and $F[x]$ are not unique. In the first example, 6 would have been a perfectly good gcd, and in the second, x^2+1, or even $\frac{1}{2}x^2+\frac{1}{2}$ would have been possible gcd's.

Proposition 2.2.2. *Every gcd of a and b is a linear combination of a and b.*

Proof: Start with the linear combination from Euclid's algorithm:

$$r_{k+1} = ua+vb$$

If d is any gcd, then d divides r_{k+1} (see the proof of Euclid's algorithm above). So $r_{k+1}=dq$. But $\deg(r_{k+1})=\deg(d)$ (because both of them are gcds). This tells us $\deg(q)=0$, so q is a **unit**. That means $d=r_{k+1}/q$, and:

$$d=(u/q)a+(v/q)b$$

is a linear combination of a and b.

Example: We said 6 is a gcd of 750 and 144. We multiply:

$$-6=750(-5)+144(26)$$

from Euclid's algorithm by the unit -1 to get:

$$6=750(5)+144(-26)$$

Definition: An element p of positive degree in a Euclidean domain is **prime** if its only factors of smaller degree are units.

Example: In $F[x]$, the primes are, of course, the prime polynomials. The integer primes are p and $-p$, where p are the natural number primes.

Proposition 2.2.3. *Suppose p is a prime in a Euclidean domain D and $a \in D$ is another element of D. If p does not divide a, then 1 is a gcd of p and a.*

Proof: Suppose d is a gcd of p and a. Since p is a prime and d divides p, then either $\deg(d) = 0$ or else $\deg(d) = \deg(p)$.

If $\deg(d) = \deg(p)$, let $p = dq$. Then $\deg(q) = 0$, so q is a unit, so $d = p/q$ and p divides d, which divides a, which is not allowed.

But if $\deg(d) = 0$, then 1 is also a gcd of p and a because 1 obviously divides both p and a and $\deg(1) = \deg(d) = 0$. In other words, if a unit is a gcd of p and a, then the special unit 1 is also a gcd of p and a.

Proposition 2.2.4. *In a Euclidean domain, every prime that divides ab must divide a or divide b (or it divides both a and b).*

Proof: If p divides ab, then $ab = pq$ for some q. If p doesn't divide a, then 1 is a gcd of p and a (Proposition 2.2.3), and by Proposition 2.2.2

$$1 = up + va$$

for some u and v. If we multiply through by b, we get:

$$b = bup + vab = bup + vqp = p(tu + vq)$$

so p divides b. That is, if p doesn't divide a, then it must divide b. So p must divide either a or b (or both) !!

Definition: Primes p and p' are **associated** if $p' = pu$ for some unit $u \in D$.

Proposition 2.2.5. *If p divides p', then p is associated to p'.*

Proof: If p divides p', they both have positive degree, since they are primes, and so $\deg(p) = \deg(p')$ by definition of a prime. But then $p' = pq$, and it follows as usual, taking degrees, that q is a unit.

Examples: (a) In $\mathbb{Z}$, the primes p and $-p$ are associated.

(b) In $F[x]$, primes $f(x)$ and $kf(x)$ (for any constant k) are associated.

The Fundamental Theorem of Arithmetic Revisited: In a Euclidean domain, every element of positive degree factors as a product of finitely many primes. Moreover, if:

$$p_1 \cdots p_n = a = p'_1 \cdots p'_m$$

are two factorizations of a, then each of the p's is associated to one of the p''s and vice versa (so there are the same number of p's as p''s)

Proof: The fact that factorizations exist is the well-ordered axiom. We've seen this twice already! The second part needs a proof, though.

If $p_1 \cdots p_n = p'_1 \cdots p'_m$, then in particular, p_1 divides $p'_1(p'_2 \cdots p'_m)$, so by Proposition 2.2.4 either p_1 divides p'_1 or else p_1 divides $p'_2 \cdots p'_m$. If p_1 divides p'_1, then p_1 and p'_1 are associated by Proposition 2.2.5.

Otherwise p_1 divides $p_2'(p_3' \cdots p_m')$, and continuing in this fashion, eventually p_1 is associated to one of the p''s. Similarly, every p_i is associated to one of the p_j''s, and reversing the argument, every p_j' is associated to one of the p_i's.

Example: There are two possible prime factorizations of 15:

$$(3)(5) = 15 = (-3)(-5)$$

and 3 is associated to -3 and 5 is associated to -5.

There are many prime factorizations of $x^2 - 1$ in $\mathbb{Q}[x]$. Examples:

$$(x-1)(x+1) = x^2 - 1 = (\frac{1}{2}x + \frac{1}{2})(2x-2)$$

and $x - 1$ is associated to $2x - 2$ and $x + 1$ is associated to $\frac{1}{2}x + \frac{1}{2}$.

Finishing up the proof of Proposition 1.2.5: We needed to show that there is only one fraction in lowest terms representing each rational number. That is, we need to know that if:

$$\frac{a}{b} \sim \frac{a'}{b'}$$

and both are in lowest terms, then $a = a'$ and $b = b'$. If any of them is 1 or -1, the result is obvious. Otherwise we factorize them:

$$a = p_1 \cdots p_n, \quad a' = p_1' \cdots p_m', \quad b = q_1 \cdots q_l, \quad b' = q_1' \cdots q_k'$$

and then:

$$ab' = p_1 \cdots p_n \cdot q_1' \cdots q_k' = q_1 \cdots q_l \cdot p_1' \cdots p_m' = ba'$$

and we can assume that all the q's and q's are positive, since b and b' are positive. But remember that a and b have no common factors, so **every** q must be associated, in fact **equal** to one of the q''s. And a' and b' have no common factors, so each q' is equal one of the q's. But then $b = b'$ and then $a = a'$ (cancellation law!) and we're done.

The same argument gives another useful result:

Proposition 2.2.6. *If a/b is in lowest terms, and*

$$\frac{a}{b} \sim \frac{a'}{b'}$$

then a divides a' and b divides b'.

Proof: Again we factorize. And again, we conclude as above that each q is equal to one of the q''s. This is enough to let us conclude that b divides b'. Of course there may be **more** q''s than q's, so it may be that $b \neq b'$. But anyway, let $b' = bc$. Then $ba' = ab' = abc$ cancels to give $a' = ac$, so a divides a' as well (with the same quotient c).

2.2.1 Euclidean Domain Exercises

6-1 Suppose D is an integral domain and $ab = 0$. Prove that $a = 0$ or $b = 0$.

6-2 Exactly one of the following is a degree function for the integers. Figure out which it is, and explain why the others don't qualify.

(a) The "absolute value minus one" function:

$$\deg(a) = |a| - 1$$

(b) The zero function:

$$\deg(a) = 0$$

(c) The "natural log of the square" function:

$$\deg(a) = \ln(a^2)$$

6-3 For each of the following pairs of integers:

(i) Find a gcd.

(ii) Express your gcd as a linear combination of the integers.

(a) 37 and 100 (b) -77 and 91 (c) $777,777$ and $100,100$

6-4 For each of the following pairs of polynomials (in $\mathbb{Q}[x]$):

(i) Find a gcd.

(ii) Express your gcd as a linear combination of the polynomials.

(a) x^5 and $x^3 + 1$ (b) $x^{12} - 1$ and $x^8 - x^6 + x^2 - 1$

6-5 Consider again the Gaussian integers $\mathbb{Z}[i] = \{a + bi\}$ from §1.4.

(a) Show that $\log(|a + bi|) = \log(\sqrt{a^2 + b^2})$ is a degree function.

There is a long division for Gaussian integers! Given $a + bi$ and $c + di$, with $\deg(c+di) < \deg(a+bi)$, let $p+qi$ be the closest Gaussian integer to the complex number:

$$\frac{a+bi}{c+di} = \frac{(a+bi)(c-di)}{c^2+d^2} = \frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2}i$$

Then $p + qi$ is the quotient Gaussian integer.

Next, define $r + si$ by:

$$a + bi = (c + di)(p + qi) + (r + si)$$

This is the remainder, which does satisfy $\deg(r + si) < \deg(c + di)$.

(b) Long divide the Gaussian integer $10 + 5i$ by $2 + 3i$.

(c) Find a gcd of $5 + 5i$ and $4 + 2i$.

6-6 A **power series** in the variable x is a (usually infinite) sum:

$$f(x) = a_d x^d + a_{d+1}x^{d+1} + a_{d+2}x^{d+2} + ... \quad (a_d \neq 0,\ d \geq 0)$$

where the coefficients all belong to a field F. Power series are added and multiplied as polynomials are added and multiplied, and they are easily seen to satisfy properties (a)-(d) of the beginning of this section.

The set of power series is denoted by $F[[x]]$. In $\mathbb{Q}[[x]]$:

(a) Find the multiplicative inverse of $1 + (a/b)x$.

(b) Find the multiplicative inverse of $1 + 2x + 3x^3 + 4x^4 + ...$

Hint: This power series is the derivative of $1 + x + x^2 + ... = 1/(1 - x)$.

(c) The units in $F[[x]]$ are exactly the power series satisfying $d = 0$. Assuming this fact (which I could ask you to prove, but I won't!) show that the function:

$$\deg(a_d x^d + a_{d+1}x^{d+1} + a_{d+2}x^{d+2} + ...) = d$$

is a degree function for the power series.

(d) Prove that x has no multiplicative inverse in any $F[[x]]$.

(e) Prove that $F[[x]]$ satisfies property (e) at the beginning of this section, so it is an integral domain.

Finally, $F[[x]]$ satisfies a strong form of division with remainders. Namely, if $\deg(f(x)) \leq \deg(g(x))$, then:

$$f(x) \ \textbf{divides}\ g(x)$$

(I am telling you this. If you want to prove it, go for it!)

In other words, this is division with remainders without remainders! So $F[[x]]$ is yet another example of a Euclidean domain.