

MATH 171: WORKSHEET R6

DAGAN KARP

1. EUCLIDEAN DOMAINS

Throughout this lecture, all rings are assumed commutative.

The goal of this lecture is to introduce and discuss Euclidean Domains. We already have experience with domains, i.e. rings without zero divisors, so the new ingredient here is the adjective Euclidean. There are two requirements for a domain to be considered Euclidean. First, as with Euclidean metric spaces, the domain must have a notion of “measure” or “norm.”

Definition 1. A norm N on the integral domain R is a map of sets

$$N : R \rightarrow \mathbb{N} \cup \{0\}$$

such that for any nonzero $0 \neq a, b \in R$,

$$N(a) \leq N(ab).$$

Further, if $N(a) > 0$ for all $a \neq 0$, then we say N is a positive norm.

Remark 2. This feels like a pretty lame definition of norm to me, but some people use it, including Herstein, so for consistency we’ll use it as well. If we required that N satisfied a triangle inequality $N(a + b) \leq N(a) + N(b)$ or $N(ab) \leq N(a)N(b)$, it would feel much more like a norm to me. But, alas, we’ll make no such requirement.

In addition to the requirement of norm, a Euclidean domain has a good notion of divisibility.

Definition 3. The integral domain R is called a Euclidean domain if there is a norm N on R such that if $a, b \in R$ and $b \neq 0$, then there exists elements $q, r \in R$ such that

$$a = qb + r,$$

where $r = 0$ or $N(r) < N(b)$. The element q is called the quotient and r the remainder.

This feels very much like ordinary division of integers, and indeed is a direct generalization.

Example 4. The integers \mathbb{Z} are a Euclidean domain with $N(a) = |a|$. First, note that $|\cdot|$ is indeed a map of sets $\mathbb{Z} \rightarrow \mathbb{N} \cup \{0\}$ and that $|0| = 0$.

Now we need to know that division works in \mathbb{Z} . For sport, let’s prove this directly.

Claim. For any $a, b \in \mathbb{Z}$ with $b > 0$, there exist unique $q, r \in \mathbb{Z}$ such that

$$a = qb + r \qquad 0 \leq r < b.$$

Proof. (Existence) If $a \geq 0$, we proceed by induction. First, suppose $a < b$. Then choosing $q = 0$ and $r = a$, we are done.

Now suppose $a \geq b$. To induce, we also suppose that our claim is satisfied and

$$a = qb + r.$$

We must inspect $a + 1$. But

$$a + 1 = qb + r + 1.$$

So, if $r + 1 < b$, then our proof is complete. But $r < b$ by hypothesis, so $r + 1 \leq b$. The remaining possibility is thus $r + 1 = b$. In that case

$$a + 1 = qb + r + 1 = qb + b = b(q + 1),$$

and our quotient is $q + 1$ and remainder 0. Hence the proof holds in case $a \geq 0$.

Now suppose $a < 0$. Then $-a > 0$ and by the above, there exist q, r such that $-a = qb + r$ and $0 \leq r < b$. If $r = 0$, then

$$a = b(-q) + 0$$

and the claim holds. Otherwise $r > 0$, and

$$a = b(-q) - r = b(-q - 1) + (b - r),$$

and the claim holds with quotient $-q - 1$ and remainder $0 \leq b - r < b$.

(Uniqueness) Assume that $a = qb + r = q'b + r'$ with $0 \leq r, r' < b$. Then

$$-b < r - r' < b.$$

Also, this difference

$$r - r' = b(q - q')$$

is a multiple of b . Any nonzero integer multiple of b is either greater than or equal to b or less than or equal to $-b$. Therefore $r - r'$ must be zero. Hence also $qb = q'b$ and so $q = q'$. \square

As with the integers, there is an algorithm for division in Euclidean domains.

Definition 5. The Euclidean algorithm for two elements a, b in an integral domain R is a list of divisions

$$\begin{aligned} a &= q_0 b + r_0 \\ b &= q_1 r_0 + r_1 \\ r_0 &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\vdots \\ r_{n-1} &= q_{n+1} r_n, \end{aligned}$$

Proposition 10. If a and b are nonzero elements in the commutative ring R such that the ideal generated by a and b is principal, $(a, b) = (d)$, then $d = \gcd(a, b)$.

Remark 11. An integral domain such that every ideal generated by two elements is principal is called a *Bezout domain*.

Proposition 12. Let R be an integral domain. Let $d, d' \in R$. If $(d) = (d')$, then there exists a unit $u \in R$ such that $d' = ud$.

Proof. If $d = 0$ we are done. Otherwise, we have $d = xd'$ and $d' = yd$. Thus $d = xyd$, and hence $d(1 - xy) = 0$. Thus $xy = 1$ and both x and y are units. \square

Theorem 13. Let R be a Euclidean domain and let $0 \neq a, b \in R$. Let $d = r_n$ be the last nonzero remainder in the Euclidean algorithm of a and b . Then

- (1) $d = \gcd(a, b)$
- (2) $(d) = (a, b)$.

Remark 14. Note that (2) above implies there exist elements $x, y \in R$ such that

$$d = ax + by.$$

Theorem 15. Suppose that $ax_0 + by_0 = c$. Then all solutions x, y of the equation $ax + by = c$ are of the form

$$\begin{aligned} x &= x_0 + m \frac{b}{(a, b)} \\ y &= y_0 - m \frac{a}{(a, b)}, \end{aligned}$$

for some integer m .

Proof. Dummit and Foote, problem (8.1) # 4.

Remark 16. Note that the equation

$$ax + by = c$$

has integer solutions $x, y \in \mathbb{Z}$ if and only if c is in the ideal generated by a and b . But this ideal is generated by the greatest common divisor $(a, b) = (d)$. Thus the equation is solvable if and only if $c \in (d)$, i.e. c is a multiple of d . To repeat, an integral solution to this equation exists if and only if c is divisible by the greatest common divisor of a and b . In that case, all solutions are given by the above theorem.

Example 17. The equation

$$3x + 12y = 17$$

has no solutions, as 17 is prime, but $(3, 12) = 3$. In particular, 17 is not a multiple of 3.