Greatest Common Divisor (Appendix to Chapter 6)

This appendix replaces material in chapter 6 from the book. Especifically, from the middle of page 62, right after the comment following Proposition 6.28, to the middle of page 63, right before Proposition 6.30.

Recall from the appendix to chapter 2, that for $m, n \in \mathbb{N}_0$, we say $k \in \mathbb{N}_0$ is a "*common divisor* of m and n, if it is a divisor of both m and n. We say k is a "*greatest common divisor*" of m and n if it is a common divisor of m and n, and it is divisible by any common divisor of m and n. In other words, if k is the "*largest*" (in terms of divisibility) among all common divisors of m and n.

We proved that if m and n have a greatest common divisor, then it is unique. We have not proved yet that any m and n in $\mathbb{N}_0$ have a greatest common divisor. We did prove, however, in Proposition 2.41, that if one of them is 0, then the other one is their greatest common divisor. We also proved existence of gcd in other special cases. Now we want to prove that any two natural numbers have a gcd.

Let $m, n \in \mathbb{N}$ and consider the set

$$S = \{k \in \mathbb{N} | k = xm + yn \text{ for some } x, y \in \mathbb{Z}\}$$

consisting of all natural numbers that are "*linear combinations*" of m and n.

By definition this is a subset of $\mathbb{N}$, and clearly $m, n \in S$. Just take $x = 1, y = 0$ for m and $x = 0, y = 1$ for n. So, S is a non-empty subset of $\mathbb{N}$. By Theorem 2.32, the Well-Ordering Principle, S has a smallest element, call it d.

Proposition 6.29. *Let $m, n \in \mathbb{N}$. Then d, the smallest element of S described above, is the greatest common divisor of m and n.*

Proof. **Claim**: for any $k \in S$, we have $d|k$. Let $k \in S$ be arbirary. There are $x, y \in \mathbb{Z}$ such that

$$k = xm + yn.$$

Since $d \in S$, there are $\alpha, \beta \in \mathbb{Z}$ such that

$$d = \alpha m + \beta n.$$

By Theorem 6.13, the Division Algorithm, there are integers q, r such that

$$k = qd + r \quad \text{and} \quad 0 \leq r < d.$$

We now have

$$\begin{aligned} r &= k - qd \\ &= (xm + yn) - q(\alpha m + \beta n) \\ &= (x - q\alpha)m + (y - q\beta)n \end{aligned}$$

Since $r < d$, by minimality of d as an element of S, we cannot have r as an element of S. Since r is a linear combination of m and n, the only thing that will keep it outside S is not being a natural number. Since we know $0 \leq r$, this forces $r = 0$, and d is a divisor of k, as claimed.

Since $m, n \in S$, as pointed out earlier, it follows that d is a common divisor of m and n. Now, let $j \in \mathbb{N}$ be a common divisor of m and n. We want to show that $j|d$. There are $a, b \in \mathbb{Z}$ such that

$$m = aj \quad \text{and} \quad n = bj.$$

It follows that

$$\begin{aligned} d &= \alpha m + \beta n \\ &= \alpha aj + \beta bj \\ &= (\alpha a + \beta b)j \end{aligned}$$

showing that $j|d$, as intended. □

Combining the previous proposition with Propositions 2.38, 2.40 and 2.41, we get that any two integers have a unique greatest common divisor in $\mathbb{N}_0$.

The claim in the proof of Proposition 6.29, shows that d is not only the smallest element of S in the sense of the partial order $\leq$, but it is also the smallest element of S in the sense of the partial order $|$.