Greatest Common Divisor (Appendix to Chapter 2)

In this appendix to chapter 2, we introduce the gcd in an alternative form to the textbook. It closely resembles Proposition 6.29 in Section 6.4. This approach is mathematically equivalent to the approach in the textbook.

Proposition 2.37. *Let $m, n \in \mathbb{Z}$. If $m \cdot n = 1$ then either $m = n = 1$ or $m = n = -1$.*

The following proposition follows easily from Propositions 1.20 and 1.25.iii.

Proposition 2.38. *Let $m, n \in \mathbb{Z}$. The following are equivalent:*

i) $m|n$

ii) $m|(-n)$

iii) $(-m)|n$

iv) $(-m)|(-n)$

Due to this proposition, discussion about divisibility, can be, and often is, restricted to the set

$$\mathbb{N}_0 = \mathbb{N} \cup \{0\} = \{0, 1, 2, 3, 4, \dots\}$$

of non-negative integers. Moreover, using Prop. 2.11, one can easily show that if $m, n \in \mathbb{N}_0$, and $m|n$, then the integer j such that $n = j \cdot m$, can be chosen to be an element of $\mathbb{N}_0$.

Recall that a "*partial order*" is a binary relation which is *reflexive*, *transitive*, and *anti-symmetric*. The following proposition tells us that *divisibility*, restricted to the set $\mathbb{N}_0$ is a *partial order*.

Proposition 2.39. *Let $m, n, p \in \mathbb{N}_0$.*

i) $m|m$, (reflexive)

ii) If $m|n$ and $n|p$ then $m|p$, (transitive)

iii) If $m|n$ and $n|m$ then $m = n$. (anti-symmetric)

Proof. (iii) Assume $m, n \in \mathbb{N}_0$, $m|n$, and $n|m$. There are integers $j, k \in \mathbb{N}_0$ such that

$$n = j \cdot m \qquad \text{and} \qquad m = k \cdot n, \tag{1}$$

from where we get $n = j \cdot k \cdot n$. Consider two cases: either $n = 0$ and from (1) and Prop. 1.14 we get $m = 0$; or $n \neq 0$, and from Axioms 1.3 and 1.5, we get $j \cdot k = 1$. Using now Prop. 2.37 we have $j = k = 1$, which in combination with (1) yield $m = n$. □

Given $m, n \in \mathbb{N}_0$, a "*common divisor*" of m and n is an integer $k \in \mathbb{N}_0$ such that $k|m$ and $k|n$. We say that k is a "*greatest common divisor*" of m and n, if it is a common divisor and any common divisor of m and n is also a divisor of k.

To write it in symbols, k is a greatest common divisor of m and n means:

- $k|m$,
- $k|n$,
- $(\forall j \in \mathbb{N}_0)(j|m, j|n \Rightarrow j|k)$.

From anti-symmetry in Prop. 2.39.iii, we get

Corollary 2.40. *Let $m, n \in \mathbb{N}_0$. If m and n have a greatest common divisor, then it is unique.*

Because of Corollary 2.40 we start using the definite article "*the*" with *greatest common divisor*, when it exists, and the greatest common divisor of m and n will be denoted by $\gcd(m, n)$.

We now show some cases when the gcd exists.

Proposition 2.41. *For any $m, n \in \mathbb{N}_0$,*

i) $1|m$ *and* $m|0$,

ii) $\gcd(m, m) = m$,

iii) If $m|n$ *then* $\gcd(m, n) = m$.

iv) $\gcd(1, m) = 1$, *and* $\gcd(m, 0) = m$.

v) If $\gcd(m, n)$ *exists, then so does* $\gcd(n, m)$, *and they are equal.*

Proof. (iv) Follows at once from 2.41.i and 2.41.iii. □

It turns out that $\gcd(m, n)$ always exists for any $m, n \in \mathbb{N}_0$, but the proof of this fact has to wait until Chapter 6. We already have from Prop. 2.41.iii, that $\gcd(0, 0) = 0$. In Prop. 6.29 it will be shown that when either $m \neq 0$ or $n \neq 0$, the smallest element of the set

$$S = \{k \in \mathbb{N} | k = mx + ny \quad \text{forsome} \quad x, y \in \mathbb{Z}\}$$

is the $\gcd(m, n)$.