Appendix week 8

1) In the proofs of both the Division Theorem and of the existence of the gcd we make use of the fact that a non-empty finite set of real numbers has a maximal element. In the notes we justify this by saying it can be found in finite time by choosing two elements, comparing and keeping the largest, then taking another element and comparing the two you now have, keeping the largest. Continue. This is not a rigorous proof, but for a rigorous proof see Proposition 11.2.3 in PJE.

2) For $a, b \in \mathbb{Z}$ with $b > 0$ let $a = bq + r$ with $0 \leq r < b$. I left it to the student to check that

$$D(b, r) \subseteq D(a, b).$$

To see if you got it right I give the proof here:

Assume $t \in D(b, r)$ is given. So, by the definition of $D(b, r)$ we have $t|b$ and $t|r$. So there exist $m, n \in \mathbb{Z}$ for which $b = tm$ and $r = tn$. But then

$$a = bq + r = tmq + tn = t(mq + n).$$

Since $mq + n \in \mathbb{Z}$ we deduce $t|a$. So we have both $t|a$ and $t|b$, hence $t \in D(a, b)$ by the definition of $D(a, b)$.

True for all $t \in D(b, r)$ means $D(b, r) \subseteq D(a, b)$ as required. ■

Alternative definition of GCD.

Recall that $d = \gcd(a, b)$ if, and only if, 1) $d|a$ and $d|b$, 2) if $c|a$ and $c|b$ then $c \leq d$. So d is **a** common divisor of a and b and d is the **greatest** of all common divisors.

Theorem 1 *The integer d satisfies*

1) $d|a$ and $d|b$, 2) if $c|a$ and $c|b$ then $c \leq d$

if, and only if, d satisfies

i) $d|a$ and $d|b$, ii) If $c|a$ and $c|b$ then $c|d$.

Proof. Note that conditions 1) and i) are identical so we need only show that if d satisfies 1) and 2) then it satisfies ii) and if d satisfies i) and ii) then it satisfies 2).

One way is trivial.

Assume d satisfies i) and ii). Assume $c|a$ and $c|b$. Then, by ii) $c|d$. Yet $c|d \Rightarrow c \leq d$ so we have shown $c|a$ and $c|b \Rightarrow c \leq d$ which is 2), as required.

Assume d satisfies 1) and 2). Assume $c|a$ and $c|b$ and, for contradiction, that $c \nmid d$.

The Division Theorem implies there exist $q, r \in \mathbb{Z}$ such that $d = cq + r$ with $0 < r < c$ ($r \neq 0$ since $c \nmid d$).

Since 1) and 2) imply $d = \gcd(a, b)$, Bezout's Lemma ensures there exist $a, b \in \mathbb{Z}$ such that $d = am + bn$.

Reinterpret 2) as implying there exist $s, t \in \mathbb{Z}$ such that $a = sc$ and $b = tc$.

Putting this all together gives

$$cq + r = d = am + bn = c\,(sm + tn)\,,$$

which rearranges to

$$r = c\,(sm + tn - q)\,, \quad \text{that is, } c|q.$$

This contradicts $0 < r < c$. Hence the last assumption is false, thus $c|d$. Therefore we have shown that if $c|a$ and $c|b$ then $c|d$, which is ii) as required. ■

This leads to

Definition 2 ***Alternative definition of GCD.*** *Let a and b be integers, at least one of which is non-zero. Then the* ***greatest common divisor*** *is the unique positive integer d such that*

i) $d|a$ and $d|b$, i.e. d is a common divisor,

ii) if $c|a$ and $c|b$ then $c|d$.