Euclidean Domains

Remainder Theorem $\Rightarrow$ Given $a, b \in \mathbb{Z}, b \neq 0$, $\exists\, q, r \in \mathbb{Z}$ such that $a = qb + r$ where <u>either</u> $r = 0$ or $|r| < |b|$

<u>Definition</u> Let R be an integral domain. A <u>Euclidean function</u> on R is a map $\varphi : R \setminus \{0_R\} \longrightarrow \mathbb{N} \cup \{0\}$ such that

A/ $\varphi(ab) \geq \varphi(a) \quad \forall\, a, b \in R$

B/ Given $a, b \in R$, $b \neq 0_R$ $\exists\, q, r \in R$ such that $a = qb + r$ where <u>either</u> $r = 0_R$ or $\varphi(r) < \varphi(b)$

<u>Definition</u> A <u>Euclidean domain</u> is an <u>integral domain</u> which admits a <u>Euclidean function</u>

<u>Example</u> $R = \mathbb{Z}$,
$$\begin{aligned} \mathbb{Z} \setminus \{0\} &\longrightarrow \mathbb{N} \cup \{0\} \\ a &\longrightarrow |a| \end{aligned}$$

<u>Lemma</u> B/ is equivalent to

B′/ $\forall\, a, b \in R \setminus \{0_R\}$, if $\varphi(a) \geq \varphi(b)$ $\exists\, c \in R$ such that either $a = cb$ or $\varphi(a - bc) < \varphi(a)$

<u>Proof</u>

(B/ $\Rightarrow$ B′/)

Let $a, b \in R \setminus \{0_R\}$

B/ $\Rightarrow$ $\exists\, q, r \in R$ such that $a = qb + r$ where either $r = 0_R$ or $\varphi(r) < \varphi(b)$. In either case let $c = q$.

$r = 0_R \Rightarrow \quad a = bc$

$r \neq 0_R \Rightarrow \quad \varphi(r) = \varphi(a - bc) < \varphi(b) \leq \varphi(a) \quad \Rightarrow B'/$

$(B'/ \Rightarrow B/)$

Let $a, b \in R$, $b \neq 0_R$.

$a = 0_R \Rightarrow \quad a = 0_R b \quad \Rightarrow \quad B/$

Assume $a \neq 0_R$

If $\exists c \in R$ such that $a = cb$ Let $q = c$, $r = 0_R \quad \Rightarrow B/$

Assume $b \nmid a \Rightarrow \quad a - qb \neq 0_R \quad \forall q \in R$.

Choose $q \in R$ such that $\varphi(a - qb)$ is minimal.

<u>Claim</u> $\quad \varphi(a - qb) < \varphi(b)$

Assume $\varphi(a - qb) \geq \varphi(b)$.

$b \nmid a \Rightarrow b \nmid a - qb \overset{B'/}{\Rightarrow} \exists c \in R$ such that

$\varphi((a - qb) - cb) < \varphi(a - qb)$

$\Rightarrow \varphi(a - (q + c)b) < \varphi(a - qb)$. Contradiction, by minimality of $\varphi(a - qb)$

Hence $\varphi(a - qb) < \varphi(b)$, Let $r = a - qb \quad \Rightarrow \quad B/$ $\square$

<u>Theorem</u> Let F be a field. Then
$$F[x] \setminus \{0\} \longrightarrow \mathbb{N} \cup \{0\}$$
$$f(x) \longrightarrow \deg(f(x))$$
is a Euclidean function.

<u>Proof</u>

F field $\Rightarrow$ $F[x]$ integral domain

A/ Given $f(x), g(x) \in F[x] \setminus \{0\}$

$\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x)) \geq \deg(f(x))$

B' Let $f(x) = a_0 + \dots + a_n x^n$, $g(x) = b_0 + \dots + b_m x^m$, $a_n, b_m \neq 0$

such that $\deg(f(x)) \geq \deg(g(x))$ $(\Leftrightarrow \quad n \geq m$

Let $c(x) = a_n b_m^{-1} x^{n-m}$

$\Rightarrow$ either $f(x) - c(x)g(x) = 0 \Rightarrow f(x) = c(x)g(x)$

or $f(x) - c(x)g(x) \neq 0$ and $\deg(f(x) - c(x)g(x)) < \deg(f(x))$

$\square$

<u>Theorem</u> Let R be a Euclidean domain. Given $a, b \in R \setminus \{0_R\}$ an HCF exists and can be expressed in the form $ua + vb$ for some $u, v \in R$

<u>Proof</u> (The Euclidean Algorithm)

Let φ be a Euclidean function on R

Assume WLOG $\varphi(a) \geq \varphi(b)$

If $b \mid a \Rightarrow b$ an HCF of a, b. $b = 0_R a + 1_R b$

Assume $b \nmid a$.

$B, \Rightarrow \quad a = q_1 b + r_1$ where $r_1 \neq 0_R$ and $\varphi(r_1) < \varphi(b)$

$B, \Rightarrow \quad b = q_2 r_1 + r_2$ where $r_2 = 0_R$ <u>or</u> $\varphi(r_2) < \varphi(r_1)$

If $r_2 = 0_2$ <u>stop</u>. If not repeat.

$B, \Rightarrow \quad r_1 = q_3 r_2 + r_3$ where $r_3 = 0_R$ or $\varphi(r_3) < \varphi(r_2)$

If $r_3 = 0$ <u>stop</u>. If not repeat

Observe $\varphi(b) > \varphi(r_1) > \varphi(r_2) > \varphi(r_3)$

$\mathbb{N} \cup \{0\}$ bounded below $\Rightarrow$ Eventually we must stop

$$\left.\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ r_2 &= q_4 r_3 + r_4 \\ &\vdots \\ r_{n-2} &= q_n r_{n-1} + r_n \\ r_{n-1} &= q_{n+1} r_n \end{aligned}\right\} \quad r_i \neq 0_R \;\; \forall\, i \in \{1, \dots, n\}$$

<u>Claim</u> r_n is an HCF of a, b.

Move up tower

Start from Bottom

$$\begin{aligned} a &= q_1 b + r_1 && \Rightarrow r_n \mid a \\ b &= q_2 r_1 + r_2 && \Rightarrow r_n \mid b \\ r_1 &= q_3 r_2 + r_3 && \Rightarrow r_n \mid r_1 \\ r_2 &= q_4 r_3 + r_4 && \Rightarrow r_n \mid r_2 \\ &\vdots && \quad\vdots \\ r_{n-2} &= q_n r_{n-1} + r_n && \Rightarrow r_n \mid r_{n-2} \\ r_{n-1} &= q_{n+1} r_n && \Rightarrow r_n \mid r_{n-1} \end{aligned}$$

Let $d \mid a$ and $d \mid b$

start from Top

Move down tower

$$\begin{aligned} a &= q_1 b + r_1 && \Rightarrow d \mid r_1 \\ b &= q_2 r_1 + r_2 && \Rightarrow d \mid r_2 \\ r_1 &= q_3 r_2 + r_3 && \Rightarrow d \mid r_3 \\ r_2 &= q_4 r_3 + r_4 && \Rightarrow d \mid r_4 \\ &\vdots && \quad\vdots \\ r_{n-2} &= q_n r_{n-1} + r_n && \Rightarrow d \mid r_n \\ r_{n-1} &= q_{n+1} r_n \end{aligned}$$

Finally we need to prove $\exists\, u, v \in R$ such that $r_n = ua + vb$

Start from Top $\longrightarrow$

$$
\begin{aligned}
a &= q_1 b + r_1 &&\Rightarrow\ r_1 = u_1 a + v_1 b \quad \left(\begin{matrix} u_1 = 1_R \\ v_1 = -q_1 \end{matrix}\right)\\
b &= q_2 r_1 + r_2 &&\Rightarrow\ r_2 = u_2 a + v_2 b \text{ for some } u_2, v_2 \in R\\
r_1 &= q_3 r_2 + r_3 &&\Rightarrow\ r_3 = u_3 a + v_3 b \text{ for some } u_3, v_3 \in R\\
r_2 &= q_4 r_3 + r_4 &&\Rightarrow\ r_4 = u_4 a + v_4 b \text{ for some } u_4, v_4 \in R\\
&\ \ \vdots && \qquad\quad \vdots\\
r_{n-2} &= q_n r_{n-1} + r_n &&\Rightarrow\ r_n = u_n a + v_n b \text{ for some } u_n, v_n \in R\\
r_{n-1} &= q_{n+1} r_n
\end{aligned}
$$

Move down tower

More formally

$$
\begin{aligned}
r_i &= u_i a + v_i b\\
r_{i+1} &= u_{i+1} a + v_{i+1} b \quad \Rightarrow \quad r_{i+2} = \overbrace{(u_i - q_{i+2} u_{i+1})}^{u_{i+2}\ =}\, a\\
r_i &= q_{i+2} r_{i+1} + r_{i+2} \qquad\qquad\qquad + \underbrace{(v_i - q_{i+2} v_{i+1})}_{=\ v_{i+2}}\, b
\end{aligned}
$$

$\square$

Exercise If c is an HCF of a,b then $\frac{ab}{c}$ is an LCM.