Euclidean Domains

A *Euclidean domain* is an integral domain R which can be equipped with a function

$$d : R\backslash\{0\} \to \mathbb{N}$$

such that for all $a \in R$ and $b \neq 0$, $b \in R$ we can write

$$a = qb + r$$

for some $q, r \in R$ with $r = 0$ or $d(r) < d(b)$.

For example. $\mathbb{Z}$ with $d(n) = |n|$ is a Euclidean Domain; also, for any field k, $k[X]$ with $d(f) = \deg(f)$ is a Euclidean Domain. (WARNING: In the second example above, it is essential that k be a field.)

We shall prove that every Euclidean Domain is a Principal Ideal Domain (and so also a Unique Factorization Domain). This shows that for any field k, $k[X]$ has unique factorization into irreducibles. As a further example, we prove that $\mathbb{Z}\left[\sqrt{-2}\,\right]$ is a Euclidean Domain.

Proposition 1. *In a Euclidean domain, every ideal is principal.*

Proof. Suppose R is a Euclidean domain and $I \lhd R$. Then EITHER $I = \{0\} = (0)$ OR we can take $a \neq 0$ in I with $d(a)$ least; then for any $b \in I$, we can write $b = qa + r$ with $r = 0$ or $d(r) < d(a)$; but $r = q - ba \in I$ and so by minimality of $d(a)$, $r = 0$; thus $a|b$ and $I = (a)$. $\square$

Corollary 2. *If k is a field then every ideal in $k[X]$ is principal.*

Corollary 3. *Let k be a field. Then every polynomial in $k[X]$ can be factorized into primes=irreducibles, and the factorization is essentially unique.*

Corollary 4. *Every element of the ring $\mathbb{Z}\left[\sqrt{-2}\,\right]$ can be factorized into primes= irreducibles, and the factorization is essentially unique.*

Proof. By Theorem 1, it is enough to show that $\mathbb{Z}\left[\sqrt{-2}\,\right]$ is a Euclidean Domain. To this end, define $N : \mathbb{Z}\left[\sqrt{-2}\,\right] \to \mathbb{N}$ by

$$N\left(a + b\sqrt{-2}\,\right) = a^2 + 2b^2 \left(= \left|a + b\sqrt{-2}\right|^2\right) \quad (a, b \in \mathbb{Z})\,.$$

Note that we can extend N to a function $N : \mathbb{Q}\left[\sqrt{-2}\,\right] \to \mathbb{Q}$ defined similarly by

$$N\left(a + b\sqrt{-2}\,\right) = a^2 + 2b^2 \left(= \left|a + b\sqrt{-2}\right|^2\right) \quad (a, b \in \mathbb{Q}).$$

Note also that given any $a + b\sqrt{-2}, c + d\sqrt{-2} \in \mathbb{Q}\left[\sqrt{-2}\,\right]$ we have

$$N\left(\left(a + b\sqrt{-2}\,\right)\left(c + d\sqrt{-2}\,\right)\right) = N\left(a + b\sqrt{-2}\,\right) N\left(c + d\sqrt{-2}\,\right).$$

Now, suppose we are given $a+b\sqrt{-2}, c+d\sqrt{-2} \in \mathbb{Z}\left[\sqrt{-2}\right]$ with $c+d\sqrt{-2} \neq 0$. Then

$$\frac{a+b\sqrt{-2}}{c+d\sqrt{-2}} = \frac{\left(a+b\sqrt{-2}\right)\left(c-d\sqrt{-2}\right)}{c^2+2d^2} = e+f\sqrt{-2} \in \mathbb{Q}\left[\sqrt{-2}\right].$$

Pick $g, h \in \mathbb{Z}$ such that $|e-g|, |f-h| \leq \frac{1}{2}$ and set

$$\begin{aligned} q &= g+h\sqrt{-2} \\ r &= a+b\sqrt{-2} - q\left(c+d\sqrt{-2}\right). \end{aligned}$$

Then $a+b\sqrt{-2} = q\left(c+d\sqrt{-2}\right)+r$ and

$$\begin{aligned} N(r) &= N\Big(\left(c+d\sqrt{-2}\right)\left((e-g)+(f-h)\sqrt{-2}\right)\Big) \\ &= N\left(c+d\sqrt{-2}\right) N\left((e-g)+(f-h)\sqrt{-2}\right) \\ &\leq \frac{3}{4} N\left(c+d\sqrt{-2}\right) \\ &< N\left(c+d\sqrt{-2}\right). \end{aligned}$$

□