Norm-Euclidean domains

The rings $\mathbb{Z}[\tau_d]$ considered last week are known as the rings of integers of the quadratic fields $\mathbb{Q}[\tau_d]$. For these rings it is sometimes the case that the norm map is also a Euclidean function. If this is the case, the ring is said to be norm-Euclidean.

Dedekind wrote a famous supplement to Dirichlet’s 1893 book Vorlesungen über Zahlentheorie. It was in this supplement that he extended Kummer’s concept of “ideal number” to a more general setting. He also showed that $\mathbb{Z}[\tau_d]$ is norm-Euclidean for

$$d = -11, -7, -3, -2, -1, 2, 3, 5, 13.$$

This list is complete for $d < 0$ but for $d > 0$ there are the following additional values

$$d = 6, 7, 11, 17, 19, 21, 29, 33, 37, 41, 57, 73.$$
Some history

Our result so far show that

\[
\text{norm-Euclidean } \Rightarrow \text{ Euclidean } \Rightarrow \text{ PID } \Rightarrow \text{ UFD}
\]

However, none of the converse implications are true.

In 1973, assuming the generalised Riemann hypothesis, Weinberger showed that for \( d > 0 \), the ring \( \mathbb{Z}[\tau_d] \) is a Euclidean domain if and only if it is a PID.

On the other hand, for \( d \in \{-163, -67, -47, -19\} \), the ring \( \mathbb{Z}[\tau_d] \) is a PID but not a Euclidean domain.

In 1994 David Clark showed that \( \mathbb{Z}[\tau_{69}] \) is a Euclidean domain but not norm-Euclidean. This was the first example of this type.

Generalities

**Theorem**

If \( \alpha \in \mathbb{Z}[\tau_d] \) and if \( N(\alpha) \) is a rational prime, then \( \alpha \) is irreducible.

**Theorem**

If \( \pi \) is a prime element of \( \mathbb{Z}[\tau_d] \), then \( \pi \) is a divisor of exactly one positive rational prime.

**Theorem**

If \( \alpha \in \mathbb{Z}[\tau_d] \), \( \alpha \neq 0 \) and \( \alpha \) is not a unit, then \( \alpha \) is a product of irreducible elements.

**Theorem**

If \( \alpha \in \mathbb{Z}[\tau_d] \), then \( N(\alpha) = |\mathbb{Z}[\tau_d]/\mathbb{Z}[\tau_d]\alpha| \).
The ring $\mathbb{Z}[i]$

**Theorem**

The ring $\mathbb{Z}[i]$ is norm-Euclidean.

**Proof.**

For $\alpha, \beta \in \mathbb{Z}[i]$ with $\beta \neq 0$ we can write $\alpha/\beta = r + is$, where $r, s \in \mathbb{Q}$. Thus there exist $x, y \in \mathbb{Z}$ such that $|r - x| \leq \frac{1}{2}$ and $|s - y| \leq \frac{1}{2}$. Therefore

$$\left| \frac{\alpha}{\beta} - (x + iy) \right|^2 = |(r - x) + i(s - y)|^2 = (r - x)^2 + s - y)^2 \leq \frac{1}{2}$$

Put $q = x + iy$ and $\rho = \alpha - q\beta$. Then $N(\rho) = |\alpha - q\beta|^2 \leq \frac{1}{2} |\beta|^2 \leq \frac{1}{2} N(\beta)$. \qed

The primes of $\mathbb{Z}[i]$

If $\pi$ is a prime element of $\mathbb{Z}[i]$, then $\pi$ divides a rational prime $p$ and we may write $p = \pi \lambda$. Then $p^2 = N(\pi)N(\lambda)$.

If $\pi = a + bi$, then $N(\pi) = a^2 + b^2 \equiv 3 \mod 4$.

i) $p = 2$. In this case $2 = i(1 - i)^2$ and $1 - i$ is a prime.

ii) $p \equiv 3 \mod 4$. In this case $N(\pi) = p^2$ and $\lambda$ is a unit. That is, $\pi$ is an associate of the rational prime $p$.

iii) $p \equiv 1 \mod 4$. In this case $-1$ is a square in $\mathbb{Z}/p\mathbb{Z}$; that is $-1 \equiv d^2 \mod p$ for some $d \in \mathbb{Z}$ and therefore $p \mid d^2 + 1 = (d + i)(d - i)$. If $p$ were prime in $\mathbb{Z}[i]$, then $p \mid d + i$ or $p \mid d - i$, which is impossible.

Thus $p = N(\pi) = a^2 + b^2 = (a + bi)(a - bi)$.

Up to associates, the primes of $\mathbb{Z}[i]$ are: $1 + i$, the rational primes $p \equiv 3 \mod 4$, and the factors $a + bi$ of the rational primes $p \equiv 1 \mod 4$, where $p = a^2 + b^2$. 


Primitive polynomials

We now turn our attention to factorisation in polynomial rings. We have already mentioned that if \( F \) is a field, then \( F[x] \) is a Euclidean domain and hence a PID.

A polynomial ring in more than one variable is never a PID but we shall see that all polynomial rings over a field are UFDs.

Definition

A polynomial \( f = a_0 + a_1 x + \cdots + a_m x^m \) in \( A[x] \) is primitive if \( A = (a_0, a_1, \ldots, a_n) \); that is, the coefficients of \( f \) have no common factors in \( A \) other than units.

Gauß’s Lemma

Lemma (Gauß)

The polynomials \( f \) and \( g \) are primitive if and only if \( fg \) is primitive.

Proof.

Suppose that \( f = a_0 + a_1 x + \cdots + a_m x^m \), \( g = b_0 + b_1 x + \cdots + b_n x^n \) and \( fg = c_0 + c_1 x + \cdots + c_{m+n} x^{m+n} \). Then \( c_j = \sum_i a_i b_{j-i} \) and therefore \((c_0, c_1, \ldots, c_{m+n}) \subseteq (a_0, \ldots, a_m) \cap (b_0, \ldots, b_n)\).

It follows immediately that if \( fg \) is primitive, then \( f \) and \( g \) are primitive.
Proof (continued)

Conversely, suppose that \( f \) and \( g \) are primitive but that \( c = (c_0, \ldots, c_{m+n}) \neq A \).

Choose a maximal ideal \( m \) containing \( c \) and then choose \( r \) and \( s \) as large as possible such that \( a_r \notin m \) and \( b_s \notin m \).

Then \( cr^s + \cdots + arb_s + \cdots \in m \), hence \( arb_s \in m \), which is a contradiction.

Thus if \( f \) and \( g \) are primitive, then \( fg \) is primitive.

Content and reduced expressions

Let \( A \) be a UFD and let \( K \) be its field of fractions. If \( f \in K[x] \) and \( f(x) = a_0 + a_1x + \cdots + a_mx^m \), then we can write \( f(x) = cf_1(x) \), where \( c \in K \) and \( f_1(x) \in A[x] \) is primitive; this is called a reduced expression for \( f \).

The element \( c \) is defined up to a unit factor and called the content of \( f \).

It follows from Gauß’s lemma that if \( f = cf_1 \) and \( g = dg_1 \) are reduced expressions for \( f \) and \( g \), then \( fg = cd_{f_1}g_1 \) is a reduced expression for \( fg \).

Lemma

Let \( A \) be a UFD, let \( K \) be the field of quotients of \( A \) and let \( f(x) \) be a primitive polynomial in \( A[x] \). Then \( f(x) \) is irreducible in \( A[x] \) if and only if \( f(x) \) is irreducible in \( K[x] \).
The polynomial ring of a UFD

**Theorem**

*If A is a UFD, then A[x] is a UFD.*

**Corollary**

*If A is a UFD, then A[x_1, \ldots, x_n] is a UFD.*

**Corollary**

*If k is a field, then k[x_1, \ldots, x_n] is a UFD.*

Nilpotents and the radical

An element x is **nilpotent** if x^n = 0 for some n > 0. A ring is **reduced** if 0 is its only nilpotent element.

The set Spec(A) of all prime ideals of a ring A is called the **spectrum** of A.

**Theorem**

*The set \( \mathfrak{N} \) of all nilpotent elements of a ring A is an ideal of A called the nilradical. The ring A/\( \mathfrak{N} \) is reduced.*

**Theorem**

\[ \mathfrak{N} = \bigcap_{p \in \text{Spec}(A)} p. \]