EUCLIDEAN RINGS

**Vocabulary:** Euclidean

One of the main ways to prove that a ring is a PID in practice is to show that it is Euclidean.

| Definition. Suppose $R$ is an integral domain. A norm on $R$ is any function $N: R \to \mathbb{Z}_{\geq 0}$. The function $N$ is said to be a positive norm provided that $N(r) > 0$ for all nonzero $r$. We call $N$ a multiplicative norm if $N(ab) = N(a)N(b)$. Some examples: The normal absolute value on $\mathbb{Z}$ is a positive norm. The norm map $N(a + bi) = a^2 + b^2$ on the Gaussian Integers $\mathbb{Z}[i]$ is a positive norm. If $k$ is a field, then we can define a norm on $k[x]$ by $N(p(x)) = \deg p$ for $p \neq 0$ and $N(0) = 0$. We can be a bit more clever and make our norm positive and multiplicative by choosing some positive integer $c \geq 2$ and defining $N(p) = c^{\deg(p)}$ for $p \neq 0$ and $N(0) = 0$.

**Definition.** An integral domain $R$ is called an Euclidean Domain provided that there is a positive norm $N$ on $R$ such that for any two elements $a, b \in R$ with $b \neq 0$ there exist $q$ and $r \in R$ with

$$a = bq + r$$

and $N(r) < N(b)$. The element $q$ is called the quotient and the element $r$ is called the remainder of the division.

(80) Let $k$ be a field. Show that $k$ is Euclidean with respect to the norm that $N(0) = 0$ and $N(x) = 1$ for $x \neq 0$.

(81) Let $k$ be a field. Verify that $k[x]$ is Euclidean with respect to the norm $N(p) = c^{\deg(p)}$ discussed at the end of the paragraph above.

(82) Let $R$ be an integral domain with multiplicative norm $N$, and let $K$ be its field of fractions. For $\frac{a}{b} \in K$, define

$$N\left(\frac{a}{b}\right) = \frac{N(a)}{N(b)}$$

(a) Show that $N(\cdot)$ is a well defined function $K \to \mathbb{Q}_{\geq 0}$.

(b) Show that $R$ is Euclidean if and only if, for each $x \in K$, there is an $r \in R$ such that $N(x - r) < 1$.

(83) Verify that $\mathbb{Z}[i]$ is Euclidean with respect to the norm $N(a + bi) = a^2 + b^2$. Show that $q$ and $r$ need not be unique by considering $a = 3 + 5i$ and $b = 2$ in $\mathbb{Z}[i]$.

The main use of the Euclidean condition is through the following Theorem:

**Important:** Show that every Euclidean domain is a PID.

Here are some bonus fun problems about Euclidean domains.

(85) Let $p$ be a positive prime integer. Show that $p$ is of the form $a^2 + b^2$ if and only if $-1$ is a square modulo $p$.

(86) Show that $\mathbb{Z}[\sqrt{-2}]$ is Euclidean, with respect to the norm $N(a + b\sqrt{-2}) = a^2 + 2b^2$.

(87) Show that $\mathbb{Z}[\sqrt{-3}]$ is not Euclidean, with respect to the norm $N(a + b\sqrt{-3}) = a^2 + 3b^2$, but that $\mathbb{Z}\left[\frac{1 + \sqrt{-3}}{2}\right]$ is Euclidean with respect to the norm $N\left(\frac{c+d\sqrt{-3}}{2}\right) = \frac{c^2 + 3d^2}{4}$.

(88) Let $R$ be a Euclidean domain. Show that there is some ideal $I$, other than $(1)$, such that every nonzero residue class in $R/I$ is represented by a unit of $R$. Deduce that $\mathbb{Z}\left[\frac{1 + \sqrt{-19}}{2}\right]$ is not Euclidean for any norm function.

For your convenience, the back side of this worksheet contains scale diagrams of $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{-2}]$, $\mathbb{Z}[\sqrt{-3}]$ and $\mathbb{Z}[\frac{1 + \sqrt{-3}}{2}]$. In each case, $N(x) = |x|^2$, where $| |$ is Euclidean distance measured on the page.

---

1 Under various circumstances, it can be reasonable to define the degree of the 0 polynomial to be $-\infty$, $-1$, $0$ or $\infty$. We do not take a stand on this issue here.

2 The primes $p$ for which this occurs are precisely 2 and the primes which are 1 mod 4. Here is a quick proof that $-1$ is a square modulo any prime $p$ which is 1 mod 4: $-1 \equiv (p-1)! \equiv (1)^{(p-1)/2} ((p-1)/2)!^2 \equiv ((p-1)/2)!^2 \mod p$. And here is a quick proof that $-1$ is not a square modulo primes which are 3 mod 4: By this problem, such a prime would be of the form $a^2 + b^2$, and $a^2 + b^2$ cannot be 3 mod 4.