

Unless otherwise specified, assume that R is a commutative ring with 1.

1. Let $R = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$.
 - (a) Show that R is an integral domain with 1.
 - (b) Show that $U(R) = \{\pm 1\}$.
 - (c) Show that 3 is irreducible in R .
 - (d) Show that $a = 2 + \sqrt{-5}$ and $b = 2 - \sqrt{-5}$ are both irreducible in R .
 - (e) Conclude that $3 \nmid 2 + \sqrt{-5}$ and $3 \nmid 2 - \sqrt{-5}$ in R .
 - (f) Conclude that 3 is irreducible but not prime in R , thus R is not a PID.

2. Let $m \in \mathbb{N}$ be square-free.
 - (a) Show that $\mathbb{Q}[\sqrt{m}] = \{r + s\sqrt{m} : r, s \in \mathbb{Q}\}$, and that $\mathbb{Q}[\sqrt{m}]$ is a field. It is thus its own field of fractions, which we will denote by $\mathbb{Q}(\sqrt{m})$.
 - (b) Show that R_m is an integral domain with 1.
 - (c) Show that $\mathbb{Q}(\sqrt{m})$ is the field of fractions for R_m .
 - (d) Show that R_m is the set of all those $r + s\sqrt{m} \in \mathbb{Q}(\sqrt{m})$ that are roots of a monic quadratic polynomial $x^2 + cx + d \in \mathbb{Z}[x]$. [This is the reason for the variation in the definition of R_m when $m \equiv 1 \pmod{4}$.]

3. For any $x = r + s\sqrt{m} \in \mathbb{Q}(\sqrt{m})$, define the norm of x to be $N(x) = r^2 - ms^2$.
 - (a) Show that $N(xy) = N(x)N(y)$.
 - (b) Show that $N(x) \in \mathbb{Z}$ if $x \in R_m$.
 - (c) Show that $u \in U(R_m)$ if and only if $N(u) = \pm 1$.
 - (d) Use (c) to show that $U(R_{-1}) = \{\pm 1, \pm i\}$, $U(R_{-3}) = \{\pm 1, \pm(1 \pm \sqrt{-3})/2\}$, and $U(R_m) = \{\pm 1\}$ for all other negative square-free m in \mathbb{Z} .

4. Let a and b be nonzero elements of a Euclidean domain such that $a \mid b$ and $d(a) = d(b)$. Show that a and b are associates.

5. Prove that if $m = -3, -7$, or -11 , then R_m is Euclidean with $d(r) = |N(r)|$ for all nonzero $r \in R_m$. [Hint: Mimic the proof of the same result for $m = -2, -1, 2$, and 3 , but choose $d \in \mathbb{Z}$ nearest to $2t$ and then $c \in \mathbb{Z}$ so that c is as near to $2s$ as possible with $c \equiv d \pmod{2}$, then set $q = (c + d\sqrt{m})/2$.]