Keith Conrad

Let K be a quadratic field. Whether or not $\mathcal{O}_K$ has unique factorization of elements is directly related to whether or not the ideals in $\mathcal{O}_K$ are all principal.

Theorem 1. *There is unique factorization of elements in $\mathcal{O}_K$ if and only if every ideal in $\mathcal{O}_K$ is a principal ideal.*

Proof. First let's suppose $\mathcal{O}_K$ has unique factorization of elements. In order to show every ideal is a principal ideal, we can focus on nonzero ideals, since the zero ideal (0) is principal.

<u>Step 1</u>: For any irreducible element π in $\mathcal{O}_K$, the ideal (π) is prime.

Let $\mathfrak{a}$ be an ideal factor of (π), say $(\pi) = \mathfrak{a}\mathfrak{b}$. We want to show $\mathfrak{a}$ is (1) or (π). Suppose $\mathfrak{a} \neq (\pi)$. Since $(\pi) = \mathfrak{a}\mathfrak{b}$, we have $(\pi) \subset \mathfrak{a}$, so having $\mathfrak{a} \neq (\pi)$ means some $\alpha \in \mathfrak{a}$ does not belong to (π), which means α is not a multiple of π. For any $\beta \in \mathfrak{b}$, we have $\alpha\beta \in \mathfrak{a}\mathfrak{b} = (\pi)$, so $\pi \mid \alpha\beta$. Because we are assuming $\mathcal{O}_K$ has unique factorization of elements, π must be an irreducible factor of either α or β. It is not a factor of α, so $\pi \mid \beta$, hence $\beta \in (\pi)$. We have shown every element of $\mathfrak{b}$ belongs to (π), so $\mathfrak{b} \subset (\pi)$. At the same time, from $(\pi) = \mathfrak{a}\mathfrak{b}$ we get $(\pi) \subset \mathfrak{b}$. Therefore $\mathfrak{b} = (\pi)$, so $(\pi) = \mathfrak{a}(\pi)$. Hence $(1) = \mathfrak{a}$.

<u>Step 2</u>: Every prime ideal in $\mathcal{O}_K$ is principal.

Let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_K$. Then $\mathfrak{p} \mid (a)$ for some integer $a > 1$, such as $a = \mathrm{N}(\mathfrak{p})$. Factor a in $\mathcal{O}_K$ into a product of irreducibles, say $a = \pi_1 \cdots \pi_r$. Then $(a) = (\pi_1) \cdots (\pi_r)$. By Step 1, each (π_i) is a prime ideal. Since $\mathfrak{p}$ is a prime ideal factor of (a), by unique factorization of ideals in $\mathcal{O}_K$ we must have $\mathfrak{p} = (\pi_i)$ for some i.

<u>Step 3</u>: Every nonzero ideal in $\mathcal{O}_K$ is principal.

By Step 2, each prime ideal in $\mathcal{O}_K$ is principal. Every nonzero ideal in $\mathcal{O}_K$ is a product of prime ideals and a product of principal ideals is principal, so every nonzero ideal in $\mathcal{O}_K$ is principal.

This completes the proof that when $\mathcal{O}_K$ has unique factorization of elements, all ideals in $\mathcal{O}_K$ are principal.

The converse result, that when all ideals in $\mathcal{O}_K$ are principal there is unique factorization of elements in $\mathcal{O}_K$, is a special case of a general theorem in abstract algebra that goes under a label like "any principal ideal domain is a unique factorization domain". Look up "principal ideal domain" in abstract algebra books (or Wikipedia) for the proof. ■

Note that in $\mathbf{Z}[\sqrt{10}]$, $4 + \sqrt{10}$ is an irreducible element but $(4 + \sqrt{10})$ is not a prime ideal (it equals $(2, \sqrt{10})(3, 1 + \sqrt{10})$, where these two factors are prime ideals). This illustrates how irreducible elements can generate nonprime ideals when $\mathcal{O}_K$ does not have unique factorization of elements.

It is *not* true in all rings that unique factorization of elements implies all ideals are principal. For example, the ring $\mathbf{Z}[X]$ has unique factorization of elements but it has many nonprincipal ideals, like $(2, X)$ (polynomials with even constant term). Only for certain special types of rings, such as $\mathcal{O}_K$ for quadratic fields K, is unique factorization of elements equivalent to all ideals being principal.