

For nonzero integers a and b , the relation $a \mid b$ is the same as $a\mathbf{Z} \supset b\mathbf{Z}$. Think about an example: $2 \mid 6$ and $2\mathbf{Z} \supset 6\mathbf{Z}$ (not $6\mathbf{Z} \supset 2\mathbf{Z}$): multiples of 6 are even but not the other way around, in general.

Let K be a quadratic field. We will show in the theorem below that divisibility of ideals in \mathcal{O}_K is related to reverse containment of the ideals in a similar way to the situation for integers above. We will need a lemma about ideals contained in a principal ideal first.

Lemma 1. *For any nonzero ideal \mathfrak{a} in \mathcal{O}_K , suppose $\mathfrak{a} \subset (t)$ for some $t \in \mathcal{O}_K$. Then the set $\frac{1}{t}\mathfrak{a} = \{\frac{\alpha}{t} : \alpha \in \mathfrak{a}\}$ is an ideal in \mathcal{O}_K .*

Proof. Since $(t) = t(1)$,

$$\mathfrak{a} \subset t(1) \implies \frac{1}{t}\mathfrak{a} \subset (1) = \mathcal{O}_K.$$

It is easy to see $\frac{1}{t}\mathfrak{a}$ is closed under addition and subtraction, so it is an additive group. For any $x \in \mathcal{O}_K$ and $\frac{\alpha}{t} \in \frac{1}{t}\mathfrak{a}$, we have $x \cdot \frac{\alpha}{t} = \frac{x\alpha}{t}$ and $x\alpha \in \mathfrak{a}$ since \mathfrak{a} is an ideal in \mathcal{O}_K . Thus $\frac{x\alpha}{t} \in \frac{1}{t}\mathfrak{a}$, which shows $\frac{1}{t}\mathfrak{a}$ swallows multiplication by \mathcal{O}_K . ■

Theorem 1. *For any two nonzero ideals \mathfrak{a} and \mathfrak{b} in \mathcal{O}_K , $\mathfrak{a} \supset \mathfrak{b}$ if and only if $\mathfrak{a} \mid \mathfrak{b}$.*

Proof. If $\mathfrak{a} \mid \mathfrak{b}$ then $\mathfrak{a}\mathfrak{c} = \mathfrak{b}$ for some ideal \mathfrak{c} . Thus $\mathfrak{b} = \mathfrak{a}\mathfrak{c} \subset \mathfrak{a}$, so $\mathfrak{a} \supset \mathfrak{b}$.

Conversely, if $\mathfrak{a} \supset \mathfrak{b}$, then we get $\mathfrak{a}\bar{\mathfrak{a}} \supset \mathfrak{b}\bar{\mathfrak{a}}$, so $(N(\mathfrak{a})) \supset \mathfrak{b}\bar{\mathfrak{a}}$. By the lemma, the set $\frac{1}{N(\mathfrak{a})}\mathfrak{b}\bar{\mathfrak{a}}$ is an ideal in \mathcal{O}_K . Call it \mathfrak{c} :

$$\mathfrak{c} = \frac{1}{N(\mathfrak{a})}\mathfrak{b}\bar{\mathfrak{a}}.$$

Then

$$\mathfrak{a}\mathfrak{c} = \mathfrak{a} \cdot \frac{1}{N(\mathfrak{a})}\mathfrak{b}\bar{\mathfrak{a}} = \frac{1}{N(\mathfrak{a})}\mathfrak{a}\mathfrak{b}\bar{\mathfrak{a}} = \frac{1}{N(\mathfrak{a})}(N(\mathfrak{a}))\mathfrak{b} = (1)\mathfrak{b} = \mathfrak{b},$$

so $\mathfrak{a} \mid \mathfrak{b}$. ■

This theorem is somewhat special to rings like \mathcal{O}_K . In general rings it is always true that $\mathfrak{a} \mid \mathfrak{b} \implies \mathfrak{a} \supset \mathfrak{b}$ but it is usually false that $\mathfrak{a} \supset \mathfrak{b} \implies \mathfrak{a} \mid \mathfrak{b}$.