Principal ideals

In this lecture we continue studying ideals, focusing on the new concept of a principal ideal.

First we introduce some notation. Let R be a commutative ring and $a \in R$. We write

$$aR = \{ar : r \in R\} \subset R$$

Then aR is an ideal in R. To check this, note $0 = a0 \in (a)$; if $ar, ar' \in (a)$ then $ar - ar' = a(r - r') \in aR$; and if $ar \in aR$ and $r' \in R$ then $r'(ar) = a(rr') \in aR$. The ideal $aR \subset R$ is called the *principal ideal* generated by $a \in R$. Another common notation for aR is (a).

Example: The ideals $(n) = n\mathbb{Z} \subset \mathbb{Z}$ are principal ideals.

Example: Let R be any commutative ring. Then $0R = (0) = \{0\}$ is the zero ideal, and $1R = (1) = R$ is the ideal which is the whole ring. These are both principal ideals.

▶ **Let R be a commutative ring.**

(i) If $I \subset R$ is an ideal and $a \in I$ then $(a) \subset I$.

(ii) If $a = ub$ for u a unit, then $(a) = (b)$.

These are straightforward from the definitions. For example, let us prove (ii). If $a = ub$ where u is a unit, then if $ar \in aR$ we have $ar = (ub)r = b(ur) \in bR$, so $(a) \subset (b)$. And if $br \in (b)$ then $br = (u^{-1}a)r = a(u^{-1}r) \in (a)$, so $(b) \subset (a)$. We conclude $(a) = (b)$.

Example: Consider the ring $R = \mathbb{Z}[\sqrt{-3}]$. Last lecture we defined a homomomorphism

$$\phi : R \longrightarrow \mathbb{Z}_4$$

$$\phi(a + b\sqrt{-3}) = a + b \pmod 4.$$

Consider the ideal $\ker(\phi)$. Note that $\phi(1 - \sqrt{-3}) = 1 - 1 = 0 \pmod 4$, so $1 - \sqrt{-3} \in \ker(\phi)$. We obtain an inclusion of ideals $(1 - \sqrt{-3}) \subset \ker(\phi)$.

Is it also true that $\ker(\phi) \subset (1 - \sqrt{-3})$? To rephrase this question, let $a + b\sqrt{-3} \in \ker(\phi)$, i.e. $a + b \equiv 0 \pmod 4$. Then, can we write $a + b\sqrt{-3}$ as a multiple of $1 - \sqrt{-3}$, i.e

$$a + b\sqrt{-3} = (1 - \sqrt{-3})(c + d\sqrt{-3})$$

for some $c, d \in \mathbb{Z}$? Note that the right hand side of this last equation becomes

$$(c + 3d) + (d - c)\sqrt{-3}$$

and so we must have $a = c + 3d$ and $b = d - c$. Solving for c, d we get $c = (a - 3b)/4$, $d = (a + b)/4$ which are integers because $a + b$ is a multiple of 4. Thus the answer is "yes", so that $\ker(\phi) \subset (1 - \sqrt{-3})$. Consequently we have

$$\ker(\phi) = (1 - \sqrt{-3})$$

Thus the kernel of this homomorphism is a principal ideal, generated by $1 - \sqrt{-3}$.

The following gives an example of an ideal which is not principal.

Example (non-principal ideal): We modify our homomorphism from above: define

$$\psi : R = \mathbb{Z}[\sqrt{-3}] \longrightarrow \mathbb{Z}_2$$

$$\psi(a + b\sqrt{-3}) = a + b \pmod 2.$$

Note again $1 - \sqrt{-3} \in \ker(\psi)$. We will argue that $\ker(\psi)$ is *not* principal. Suppose for a contradiction that $\ker(\psi)$ is principal, i.e. there is some for some $a + b\sqrt{-3} \in R$ such that

$$\ker(\psi) = (a + b\sqrt{-3})$$

In other words, $\ker(\psi)$ is the principal ideal generated by $a + b\sqrt{-3}$. Necessarily $a + b \equiv 0 \pmod 2$. Now since $1 - \sqrt{-3} \in \ker(\psi)$, we must have

$$1 - \sqrt{-3} = (a + b\sqrt{-3})(c + d\sqrt{-3})$$

for some $c, d \in \mathbb{Z}$. Note that since $\sqrt{-3}$ appears on the left side of this equation we can assume b and d are not both zero, for if they are both zero then the right hand side is a real number. Take the squared norms of both sides to obtain

$$4 = |1 - \sqrt{-3}|^2 = |a + b\sqrt{-3}|^2 |c + d\sqrt{-3}|^2 = (a^2 + 3b^2)(c^2 + 3d^2)$$

Noting that $a, b, c, d \in \mathbb{Z}$, $a + b \equiv 0 \pmod 2$, and one of b, d is non-zero, we must have $a, b, c \in \{1, -1\}$ and $d = 0$; or $a \in \{2, -2\}$, $c \in \{1, -1\}$ and $b = d = 0$. The only choices among these possibilities which solve the equation $1 - \sqrt{-3} = (a + b\sqrt{-3})(c + d\sqrt{-3})$ are $a = c = 1, b = -1, d = 0$ and $a = c = -1, b = 1, d = 0$. We conclude

$$a + b\sqrt{-3} = \pm(1 - \sqrt{-3})$$

Thus under our current assumption that $\ker(\psi)$ is principal, we obtain

$$\ker(\psi) = (1 - \sqrt{-3}) = \ker(\phi)$$

However, note that $\psi(2) = 0 \pmod 2$ so that $2 \in \ker(\psi)$, while $\phi(2) = 2 \not\equiv 0 \pmod 4$, so $2 \notin \ker(\phi)$. We conclude that $\ker(\psi) \neq \ker(\phi)$. We have a contradiction. Thus $\ker(\psi)$ cannot be a not principal ideal.