1.8 Extension and Contraction

Let $f : A \to B$ be a ring homomorphism.

If $I \lhd A$ define the **extension** I^{e} of I (**with respect to** f) to be

$$I^{\mathrm{e}} \;=\; \langle\, f(I)\, \rangle \;.$$

$\uparrow$ $\uparrow$

ideal generated in B

Thus

$$I^{\mathsf{e}} \;=\; \left\{ \sum_{i=1}^{n} y_i\, f(x_i) \;\middle|\; n \geq 1\,, \quad y_i \in B\,, \;\; x_i \in I \quad (\forall i) \right\}$$

Typically I^{e} is much larger than $f(I)$.

e.g. If $f : \mathbb{Z} \to \mathbb{Q}$ is the identity embedding then

$$\{0\} \neq I \;\lhd\; \mathbb{Z} \qquad \Longrightarrow \qquad I^{\mathsf{e}} \;=\; \mathbb{Q}\,.$$

If $J \lhd B$ define the **contraction** J^{c} of J (**with respect to** f) to be

$$J^{\mathsf{c}} \;=\; f^{-1}(J) \;=\; \{\, x \in A \mid f(x) \in J \,\} \,.$$

Easy to see:

$$\boxed{J^{\mathsf{c}} \lhd A \,.}$$

We have already noted (on page 62) that

the property of an ideal being **prime** is preserved under contraction.

However, primeness need not be preserved under extension:

e.g. If $f : \mathbb{Z} \longrightarrow \mathbb{Q}$ is the identity embedding and $p \in \mathbb{Z}$ is prime then $p\mathbb{Z}$ is a prime ideal in $\mathbb{Z}$, but $(p\mathbb{Z})^{\mathsf{e}} = \mathbb{Q}$ is not prime in $\mathbb{Q}$.

In general, $f : A \longrightarrow B$ factorizes

$$\begin{array}{ccc} A & \xrightarrow{\quad f \quad} & B \\ & {\scriptstyle s}\searrow \quad \nearrow{\scriptstyle i} & \\ & f(A) & \end{array}$$

where s is surjective and i is injective.

For the surjective branch of the factorization, the relationship between ideals is described by an easy modification of an earlier Proposition (page 38):

Proposition: There is a one-one correspondence between ideals of $f(A)$ and ideals of A containing $\ker f$, and prime ideals correspond to prime ideals.

There is no known simple relationship between prime ideals of $f(A)$ and prime ideals of B .

Example (Gaussian integers):

Consider extension with respect to the identity embedding of $\mathbb{Z}$ in $\mathbb{Z}[i]$.

The nonzero prime ideals of $\mathbb{Z}$ have the form $p\mathbb{Z}$ where $p \in \mathbb{Z}$ is prime, but

$$(p\mathbb{Z})^{\mathsf{e}} \;=\; \{\, p\alpha \;\mid\; \alpha \in \mathbb{Z}[i] \,\} \;=\; p\,\mathbb{Z}[i]$$

may or may not be prime in $\mathbb{Z}[i]$.

The full story is as follows:

(i) $2\mathbb{Z}[i] \;=\; (1+i)^2\mathbb{Z}[i] \;=\; \big((1+i)\mathbb{Z}[i]\big)^2$;

(ii) if $p \equiv 1 \pmod 4$ then $p\mathbb{Z}[i]$ is the product of two distinct prime ideals;

(iii) if $p \equiv 3 \pmod 4$ then $p\mathbb{Z}[i]$ is prime in $\mathbb{Z}[i]$.

To explain part of this, we exploit the following

Fact: $\mathbb{Z}[i]$ is a UFD.

— which in turn follows from other facts:

$\mathbb{Z}[i]$ is a **Euclidean domain (ED)**;

EDs are PIDs, and PIDs are UFDs.

— a branch of general theory that may be explored later when we discuss Gauss' Theorem.

Thus in $\mathbb{Z}[i]$, all irreducibles are primes (and conversely).

Proof of (i): $(1+i)^2 = 2i$

so $(1+i)^2$ and 2 differ by a unit in $\mathbb{Z}[i]$,

so generate the same principal ideal. Thus

$$2\mathbb{Z}[i] = (1+i)^2\mathbb{Z}[i] = \big((1+i)\mathbb{Z}\big)^2 .$$

[General fact: if $a, b \in A$ then $(aA)(bA) = abA$.]

But $|1+i|^2 = 2$ so $1+i$ is irreducible in $\mathbb{Z}[i]$, so is a prime element.

Hence $(1+i)\mathbb{Z}[i]$ is a prime ideal of $\mathbb{Z}[i]$ and (i) is proved.

Proof of (ii)**:** This follows from a theorem of Fermat:

> If p is a positive prime integer congruent to 1 mod 4, then
>
> $$p = x^2 + y^2 \qquad (\exists x, y \in \mathbb{Z}^+)$$

(proved for example in LeVeque “Elementary theory of numbers”).

In this case, $p = (x+iy)(x-iy)$, so

$$p\mathbb{Z}[i] = \big((x+iy)\,\mathbb{Z}[i]\big)\,\big((x-iy)\,\mathbb{Z}[i]\big)\ .$$

But $x \pm iy$ is irreducible (because $|x \pm iy|^2 = p$),

so $x \pm iy$ is prime.

Also neither $x+iy$ nor $x-iy$ is a multiple of the other

(since they do not differ by a unit, noting that $x \neq y$).

Hence $p\mathbb{Z}[i]$ is a product of two distinct prime ideals, proving (ii).

Proof of (iii)**:** Let p be a prime congruent to 3 mod 4. We show p is irreducible. Suppose

$$p \;=\; \alpha\beta \qquad (\exists \alpha, \beta \in \mathbb{Z}[i]) \; .$$

Then

$$p^2 = |p|^2 = |\alpha|^2 \, |\beta|^2 ,$$

so $|\alpha|^2$ must be 1 , p or p^2 .

Suppose $|\alpha|^2 = p$, and write $\alpha = a + bi$ for some integers a, b .

Then

$$p = a^2 + b^2$$

is odd, so one of a , b is odd and the other even.

If $a = 2k$, $b = 2l + 1$ for some integers k , l , then

$$\begin{aligned} p &= a^2 + b^2 \\ &= 4k^2 + 4l^2 + 4l + 1 \\ &\equiv 1 \mod 4 , \end{aligned}$$

contradicting that p is congruent to 3 mod 4.

Similarly a odd and b even leads to a contradiction.

Hence $|\alpha|^2 = 1$, in which case α is a unit,

or $|\alpha|^2 = p^2$, in which case $|\beta|^2 = 1$ and β is a unit.

This proves p is irreducible, so prime.

Hence $p\mathbb{Z}[i]$ is a prime ideal and (iii) is proved.