4. Coprime ideals and the Chinese remainder theorem

Definition. Two ideals $\mathfrak{a}, \mathfrak{b} \subseteq A$ are **coprime** if $\mathfrak{a} + \mathfrak{b} = (1)$.

Remark. We have $\mathfrak{a} + \mathfrak{b} = (1)$ if and only if $1 \in \mathfrak{a} + \mathfrak{b}$, so $\mathfrak{a}$ and $\mathfrak{b}$ are coprime if and only if there exist $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$ such that $a + b = 1$.

Example. In $\mathbb{Z}$, we have $(m) + (n) = (\gcd(m, n))$, so (m) and (n) are coprime if and only if $\gcd(m, n) = 1$, i.e. if m and n are coprime numbers.

Example. We have computed $(x - 2, 2x^2 - 2) = (1)$ in $\mathbb{Q}[x]$, so the ideals $(x - 2)$ and $(2x^2 - 2)$ in $\mathbb{Q}[x]$ are coprime.

Example. The ideals $(x), (y) \subset \mathbb{Q}[x, y]$ are not coprime: If $f \in (x) + (y)$, then $f = \sum a_{ij} x^i y^j$ with $a_{00} = 0$, and in particular $f \neq 1$

Proposition. *Let $\mathfrak{a}, \mathfrak{b} \subseteq A$ be ideals. If $\mathfrak{a}$ and $\mathfrak{b}$ are coprime, then $\mathfrak{ab} = \mathfrak{a} \cap \mathfrak{b}$.*

Proof. We always have $\mathfrak{ab} \subseteq \mathfrak{a} \cap \mathfrak{b}$, it remains to show $\mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{ab}$.

Since $\mathfrak{a}$ and $\mathfrak{b}$ are coprime, we can find $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$ such that $a + b = 1$. If $x \in \mathfrak{a} \cap \mathfrak{b}$, we also have

$$x = 1x = ax + bx.$$

Since $x \in \mathfrak{b}$, we have $ax \in \mathfrak{ab}$, and since $x \in \mathfrak{a}$, we have $bx \in \mathfrak{ab}$. It follows that $x \in \mathfrak{ab}$. □

Example. If m, n are coprime, then $\operatorname{lcm}(m, n) = mn$, so $(m) \cap (n) = (\operatorname{lcm}(m, n)) = (mn) = (m)(n)$.

Given rings $A_1, \ldots, A_n$, we have the **product ring**

$$\prod_{i=1}^{n} A_i = A_1 \times \cdots \times A_n,$$

whose elements are n-tuples $(a_1, \ldots, a_n)$, with $a_i \in A_i$, and with addition and multiplication defined componentwise.

Let A be a ring and $\mathfrak{a}_1, \ldots, \mathfrak{a}_n \subseteq A$ ideals. We have a homomorphism $\phi_i \colon A \to A/\mathfrak{a}_i$ for each i. We can define a product homomorphism $\phi \colon A \to \prod_{i=1}^n A/\mathfrak{a}_i$, given by

$$\phi(a) = (\phi_1(a), \ldots, \phi_n(a) = (a + \mathfrak{a}_1, a + \mathfrak{a}_2, \ldots, a + \mathfrak{a}_n).$$

Theorem (Generalised Chinese remainder theorem)**.** *Let $\mathfrak{a}_1, \ldots, \mathfrak{a}_n \subseteq A$. Assume that the $\mathfrak{a}_i$ are pairwise coprime. Then the homomorphism $\phi \colon A \to \prod_{i=1}^n A/\mathfrak{a}_i$ is surjective, and*

$$\ker \phi = \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n = \mathfrak{a}_1 \cdots \mathfrak{a}_n.$$

We have an isomorphism

$$A/\cap_{i=1}^n \mathfrak{a}_i \cong \prod_{i=1}^{n} A/\mathfrak{a}_i.$$

Proof assuming $n = 2$: We first show ϕ is surjective: It's enough to show that $(1, 0), (0, 1) \in \phi(A)$, since if $\phi(x_1) = (1, 0)$ and $\phi(x_2) = (0, 1)$, then for an arbitrary element $(b_1 + \mathfrak{a}_1, b_2 + \mathfrak{a}_2) \in A/\mathfrak{a}_1 \times A/\mathfrak{a}_2$ we have

$$\begin{aligned}\phi(b_1 x_1 + b_2 x_2) &= \phi(b_1)\phi(x_1) + \phi(b_2)\phi(x_2) \\ &= (b_1 + \mathfrak{a}_1, b_1 + \mathfrak{a}_2)(1, 0) + (b_2 + \mathfrak{a}_1, b_2 + \mathfrak{a}_2)(0, 1) = (b_1 + \mathfrak{a}_1, b_2 + \mathfrak{a}_2).\end{aligned}$$

Coprimality of $\mathfrak{a}_1$ and $\mathfrak{a}_2$ means there are $a_1 \in \mathfrak{a}_1, a_2 \in \mathfrak{a}_2$ such that $a_1 + a_2 = 1$. But now

$$\phi(a_1) = (a_1 + \mathfrak{a}_1, a_1 + \mathfrak{a}_2) = (a_1 + \mathfrak{a}_1, (1 - a_2) + \mathfrak{a}_2) = (0, 1).$$

Similarly we get $\phi(a_2) = (1, 0)$.

It is clear that $\phi(x) = 0$ is equivalent to $x \in \mathfrak{a}_1 \cap \mathfrak{a}_2$, so $\ker \phi = \mathfrak{a}_1 \cap \mathfrak{a}_2$. As $\mathfrak{a}_1, \mathfrak{a}_2$ are coprime, we have $\mathfrak{a}_1 \cap \mathfrak{a}_2 = \mathfrak{a}_1\mathfrak{a}_2$.

Finally, the fundamental homomorphism theorem gives

$$A/\cap_{i=1}^n \mathfrak{a}_i = A/\ker\phi \cong \phi(A) = \prod_{i=1}^n A/\mathfrak{a}_i.$$

□

Example (Chinese remainder theorem)**.** If $k_1, \ldots, k_n$ are pairwise coprime integers, then $\mathbb{Z}/\prod k_i \cong \prod \mathbb{Z}/(k_i)$. In particular if $n = \prod p_1^{e_1} \ldots p_k^{e_k}$ is the prime factorisation of an integer n, we have

$$\mathbb{Z}/(n) = \prod \mathbb{Z}/(p_i^{e_i})$$

Example. Since $(x-2), (2x^2-2) \subseteq \mathbb{Q}[x]$ are coprime, we have

$$\mathbb{Q}[x]/(x-2)(2x^2-2) = \mathbb{Q}[x]/((x-2)(2x^2-2)) = \mathbb{Q}[x]/(x-2) \times \mathbb{Q}[x]/(2x^2-2) \cong \mathbb{Q} \times \mathbb{Q}(\sqrt{2}).$$

Further operations on ideals

4.1. **Ideal quotient.**

Definition. Let $\mathfrak{a}, \mathfrak{b} \subseteq A$ be ideals. The ideal quotient $(\mathfrak{a} : \mathfrak{b}) \subset A$ is the set of $x \in A$ such that $x\mathfrak{b} \subseteq \mathfrak{a}$, i.e. the set of x such that for every $b \in \mathfrak{b}$, we have $xb \in \mathfrak{a}$. It is easy to check that this is an ideal.

Example. If $\mathfrak{a} \subseteq A$ is an ideal, then $(\mathfrak{a} : \mathfrak{a}) = (1)$, since $x \in (\mathfrak{a} : \mathfrak{a})$ means that $xa \in \mathfrak{a}$ for all $a \in \mathfrak{a}$. Since $\mathfrak{a}$ is closed under multiplication from A, this holds for all $x \in A = (1)$.

Example. If $\mathfrak{a} \subseteq A$ is an ideal and $b \in A$, then $x \in (\mathfrak{a} : (b))$ if and only if $xb \in \mathfrak{a}$.

Proof: If $x \in (\mathfrak{a} : (b))$, then since $b \in (b)$, we have $xb \in \mathfrak{a}$. Conversely, suppose $xb \in \mathfrak{a}$. The elements of (b) are all of the form yb with $y \in A$, and we then have $x(yb) = y(xb) \in \mathfrak{a}$, so $x \in (\mathfrak{a} : (b))$.

Definition. The **annihilator** of an ideal $\mathfrak{a} \subseteq A$ is defined as

$$\mathrm{Ann}(\mathfrak{a}) = (0 : \mathfrak{a}) = \{x \in A \mid xa = 0 \qquad \forall a \in \mathfrak{a}\}$$

The annihilator of an element $a \in A$ is

$$\mathrm{Ann}(a) = \mathrm{Ann}((a)) = (0 : (a)) = \{x \in A \mid xa = 0\}.$$

Example. An element $a \in A$ is a zero-divisor if and only if $\mathrm{Ann}(a) \neq (0)$.

4.2. **Nilpotents and radicals.**

Definition. An element a of a ring A is **nilpotent** if there exists an $n \geq 1$ such that $x^n = 0$. The set of nilpotent elements of A is called the **nilradical** of A, denoted $\mathfrak{N}$.

Proposition. *The nilradical of A is an ideal.*

Proof. If $a \in \mathfrak{N}$, and $x \in A$, then it is easy to see that $-a \in \mathfrak{N}$ and $xa \in \mathfrak{N}$. To see that $\mathfrak{N}$ is closed under addition, observe that if $a, b \in \mathfrak{N}$, we have $m, n \geq 0$ such that $a^m = b^n = 0$. Now compute

$$(a+b)^{m+n} = \sum_{i=0}^{m+n} \binom{m+n}{i} a^i b^{m+n-i}.$$

If $i \geq m$, then $a^i = 0$, while if $i < m$, then $m + n - i \geq n$ so $b^{m+n-i} = 0$. Hence all terms vanish, so $(a+b)^{m+n} = 0$ and $a + b \in \mathfrak{N}$. □

Theorem. *The nilradical $\mathfrak{N}$ of A is the intersection of all prime ideals of A.*

Half of the proof. Easy half: If $f \in A$ is nilpotent and $\mathfrak{p}$ is prime ideal, then $f^n = 0 \Rightarrow f^n \in \mathfrak{p} \Leftrightarrow f \in \mathfrak{p}$. This gives us $\mathfrak{N} \subseteq \cap_{\mathfrak{p} \text{ prime}} \mathfrak{p}$.

Hard half: If $f \in A$ is contained in all prime ideals of A, then f is nilpotent. □

Example. Let A be an integral domain. Then f nilpotent $\Rightarrow$ f a zero-divisor $\Rightarrow$ $f = 0$, so $\mathfrak{N} = (0)$.

Example. In $\mathbb{Z}/(p^k)$, we have just one prime ideal $(p)/(p^k)$, so $\mathfrak{N} = (p)/(p^k)$.

Definition. Let A be a ring, $\mathfrak{a} \subseteq A$ an ideal. The **radical** of $\mathfrak{a}$, denoted $\sqrt{\mathfrak{a}}$ (note [AM] uses $\mathfrak{r}(\mathfrak{a})$), is the set of $x \in A$ such that there is an $n \geq 1$ such that $x^n \in \mathfrak{a}$.

Example. The nilradical $\mathfrak{N} = \sqrt{(0)}$.

Proposition. *The set $\mathfrak{r}(\mathfrak{a})$ is an ideal, and equals the intersection of the prime ideals containing $\mathfrak{a}$.*

The proofs are generalisations of the corresponding statements for the nilradical. Alternatively one can use the following:

Proposition. *Let $\mathfrak{N}$ be the nilradical of $A/\mathfrak{a}$, and let $\phi\colon A \to A/\mathfrak{a}$ be the quotient homomorphism. Then $\sqrt{\mathfrak{a}} = \phi^{-1}(\mathfrak{N})$.*

Proof. Let $x \in A$. Then $x \in \sqrt{\mathfrak{a}}$ is equivalent to $x^n \in \mathfrak{a}$ for some $n \geq 1$, which is equivalent to $\phi(x)^n = \phi(x^n) = 0$ for some $n \geq 1$. □

Example. Let $n \geq 1$ have prime factorisation $n = p_1^{e_1} \cdots p_k^{e_k}$. Then $m \in \mathbb{Z}$ lies in $\sqrt{(n)}$ if and only if there is an $k \geq 1$ such that $m^k \in (n)$, which is if and only if m^k is divisible by n. If every p_i divides m, then $m^{\max e_i}$ is divisible by n. If some p_i does not divide m, then m^k is never divisible by n.

This means m lies in $\mathfrak{r}((n))$ if and only if m is divisible by each p_i, which is the same as saying m is divisible by $p_1 \ldots p_k$. We get

$$\sqrt{(n)} = (p_1 \cdots p_k).$$

Example. Consider $\mathbb{Q}[x]$ and the ideal (x^m). Then $f \in \sqrt{(x^m)}$ is equivalent to f^n is divisible by x^m for some $n \geq 1$. Let

$$f = a_0 + a_1 x + \cdots + a_d x^d.$$

Then if $a_0 \neq 0$, we have $f^n = a_0^n + x(\ldots)$, so $f^n \notin (x^m)$ for all $n \geq 1$. If $a_0 = 0$, then $f^m = a_1^m x^m + x^{m+1}(\ldots)$, so $f^m \in (x^m)$. Thus $f \in \sqrt{(x^m)}$ if and only if $a_0 = 0$, which is if and only if $f \in (x)$. We've shown

$$\sqrt{(x^m)} = (x).$$

4.3. **Extension and contraction of ideals.**

Definition. Let $\phi\colon A \to B$ be a homomorphism, let $\mathfrak{a} \subseteq A$ and $\mathfrak{b} \subseteq B$ be ideals. The **extension** of $\mathfrak{a}$ is the smallest ideal in B containing $\phi(\mathfrak{a})$, denoted $\phi(\mathfrak{a})B$ or $\mathfrak{a}^e$. The **contraction** of $\mathfrak{b}$ is $\phi^{-1}(\mathfrak{b}) \subseteq A$, also denoted $\mathfrak{b}^c$.

Both of these are ideals.

Remark. The image $\phi(\mathfrak{a}) \subseteq B$ is not itself an ideal, take e.g. the homomorphism $\phi\colon \mathbb{Q} \to \mathbb{R}$, where $\phi(\mathbb{Q})$ is not an ideal in $\mathbb{R}$.

Concretely, the elements of $\mathfrak{a}^e$ are all finite sums $b_1\phi(a_1) + \cdots + b_n\phi(a_n)$ with $a_i \in \mathfrak{a}$, $b_i \in B$.

Proposition. *Let $\phi\colon A \to B$ be a ring homomorphism, and let $\mathfrak{p} \subset B$ be a prime ideal. Then $\phi^{-1}(\mathfrak{p})$ is a prime ideal of A.*

Proof. If $a, a' \in A \setminus \phi^{-1}(\mathfrak{p})$, then $\phi(a), \phi(a') \notin \mathfrak{p}$, so $\phi(aa') = \phi(a)\phi(a') \notin \mathfrak{p}$. This means $aa' \notin \phi^{-1}(p)$, so $\phi^{-1}(\mathfrak{p})$ is prime. □