3. Lecture 3 – Operations on ideals

Let A be a ring. We've seen two ways of constructing ideals, either as principal ideals $(f) \subseteq A$ for some $f \in A$, or by the general existence result giving us a maximal ideal $\mathfrak{m} \subset A$.

There are a few natural operations we have access to in order to build more ideals.

3.1. Addition.

Definition (Addition)**.** Let $\mathfrak{a}, \mathfrak{b} \subseteq A$ be ideals. The set

$$\mathfrak{a} + \mathfrak{b} = \{a + b \mid a \in \mathfrak{a}, b \in \mathfrak{b}\} \subseteq A$$

is an ideal. Given a sequence $\mathfrak{a}_1, \dots, \mathfrak{a}_n \subseteq A$, the set

$$\mathfrak{a}_1 + \cdots + \mathfrak{a}_n = \{a_1 + \cdots + a_n \mid a_i \in \mathfrak{a}_i\}$$

is an ideal. Given an collection of ideals $\{\mathfrak{a}_i\}_{i \in I}$, the sum $\sum_{i \in I} \mathfrak{a}_i$ has as elements all finite sums $a_{i_1} + \cdots + a_{i_n}$, where $i_1, \dots, i_n \in I$ and $a_{i_j} \in \mathfrak{a}_{i_j}$.

Remark. The ideal $\mathfrak{a} + \mathfrak{b}$ is the smallest ideal containing both $\mathfrak{a}$ and $\mathfrak{b}$. Similar statements hold for the more general versions.

Example. In $\mathbb{Z}$, given ideals (m) and (n), with $m, n > 0$, we have the ideal

$$(m) + (n) = \{xm + yn \mid x, y \in \mathbb{Z}\}.$$

We know that $(m) + (n) = (k)$ for some integer k, and we know that $(m) + (n)$ is the smallest ideal containing (m) and (n). This means that k must be the biggest number dividing both m and n, and so $k = \gcd(m, n)$.

Definition. If $a_1, \dots, a_n \in A$, then we write

$$(a_1, \dots, a_n) = (a_1) + (a_2) + \cdots + (a_n) = \{x_1 a_1 + \cdots + x_n a_n \mid x_i \in A\}.$$

An ideal that can be written in this form is called **finitely generated**.

Example. In the ring $\mathbb{Q}[x, y]$, we have the ideal (x, y). This consists of all polynomials f which can be written in the form

$$f = x g_1 + y g_2 \qquad g_i \in \mathbb{Q}[x, y].$$

Writing

$$f = \sum_{i,j \geq 0} a_{ij} x^i y^j \qquad a_{ij} \in \mathbb{Q},$$

we have $f \in (x, y)$ if and only if $a_{00} = 0$. On the one hand, if $f = x g_1 + y g_2$, then clearly $a_{00} = 0$. On the other, if $a_{00} = 0$, we can write

$$f = x\Big(\sum_{i \geq 1} \sum_{j \geq 0} a_{ij} x^{i-1} y^j\Big) + y\Big(\sum_{j \geq 1} a_{0j} y^{j-1}\Big) \in (x, y).$$

Lemma (A computational trick)**.** *Let $a_1, a_2, b \in A$. Then we have an equality of ideals*

$$(a_1, a_2) = (a_1, a_2 + b a_1).$$

Proof. We clearly have $a_1 \in (a_1, a_2)$, and $a_2 + b a_1 \in (a_1, a_2)$. This means that $(a_1, a_2 + b a_1) \subseteq (a_1, a_2)$.

On the other hand, we have $a_1 \in (a_1, a_2 + b a_1)$, and, since $a_2 = -b a_1 + (a_2 + b a_1)$, that $a_2 \in (a_1, a_2 + b a_1)$. Thus $(a_1, a_2) \subseteq (a_1, a_2 + b a_1)$, and we are done. □

Example. In the ring $\mathbb{Z}$, we have

$$(5,7) = (5,7-5) = (5,2) = (5-2\cdot 2,2) = (1,2) = (1,2-2\cdot 1) = (1,0) = (1).$$

You may recognize this as the Euclidean algorithm for finding the greatest common divisor of two integers.

Example. In $\mathbb{Q}[x]$, we have

$$(x-2,2x^2-2) = (x-2,(2x^2-2)-2x(x-2)) = (x-2,4x-2) = (x-2,4x-2-4(x-2)) = (x-2,6).$$

Since 6 lies in the ideal, so must $\frac{1}{6}6 = 1$, so $(x-2,2x^2-2) = (1)$.

Definition (Intersection)**.** Let $\mathfrak{a},\mathfrak{b} \subseteq A$ be ideals, then $\mathfrak{a}\cap\mathfrak{b} \subseteq A$ is also an ideal. Similarly given $\{\mathfrak{a}_i\} \subseteq A$, we have $\cap_{i\in I}\mathfrak{a}_i$ is an ideal.

Remark. The ideal $\mathfrak{a}\cap\mathfrak{b}$ is the biggest ideal contained in $\mathfrak{a}$ and in $\mathfrak{b}$.

Example. Given $m,n \geq 0$, we have $(m),(n) \subseteq \mathbb{Z}$, and moreover

$$(m)\cap(n) = \{k\in\mathbb{Z} \mid m|k \text{ and } n|k\} = \{k\in\mathbb{Z} \mid \operatorname{lcm}(m,n)|k\} = (\operatorname{lcm}(m,n)).$$

Example. Working in $\mathbb{Q}[x,y]$, we have that $(x)\cap(y)$ is the ideal consisting of those f which can be written both as xg and as yh. Writing $f = \sum a_{ij}x^iy^j$, $a_{ij}\in\mathbb{Q}$, the first condition becomes $a_{0j} = 0$ for all j, while the second becomes $a_{j0} = 0$ for all j. It follows that $f\in(x)\cap(y)$ if and only if $a_{ij} = 0$ whenever i or j is 0, which is the same as saying $f\in(xy)$, so $(x)\cap(y) = (xy)$.

Definition (Product)**.** Given two ideals $\mathfrak{a},\mathfrak{b}$, the **product ideal** is

$$\mathfrak{a}\mathfrak{b} = \{\sum_{i=1}^{n} a_ib_i \mid a_i\in\mathfrak{a}, b_i\in\mathfrak{b}\},$$

i.e. the set of elements which are finite sums of products of elements from $\mathfrak{a}$ and $\mathfrak{b}$. Given $\mathfrak{a}_1,\ldots,\mathfrak{a}_k$, the product $\mathfrak{a}_1\cdots\mathfrak{a}_k$ is defined similarly

$$\mathfrak{a}_1\cdots\mathfrak{a}_k = \{\sum_{i=1}^{n} a_{i1}\cdots a_{ik} \mid a_{ij}\in\mathfrak{a}_j\}.$$

Example. Let $m,n\in\mathbb{Z}$, then

$$(m)(n) = \{\sum_{i=1}^{k} a_ib_i \mid a_i\in(m), b_i\in(n)\} \overset{\substack{a_i=l_im \\ b_i=j_in}}{=} \{\sum_{i=1}^{n} l_imj_in \mid l_i,j_i\in\mathbb{Z}\} = (mn).$$

Example. More generally, given $a_1,a_2,\ldots,a_n\in A$, we have

$$(a_1)(a_2)\cdots(a_n) = (a_1a_2\cdots a_n) \subseteq A$$

Remark. We always have $\mathfrak{a}_1\cdots\mathfrak{a}_n \subseteq \mathfrak{a}_1\cap\cdots\cap\mathfrak{a}_n$.

Example. The union of two ideals is usually not an ideal, e.g. $(2)\cup(3)$ is not an ideal of $\mathbb{Z}$.

There are various rules for manipulating these three operations (intersection, addition and multiplication) of ideals, e.g. $\mathfrak{a}(\mathfrak{b}+\mathfrak{c}) = \mathfrak{a}\mathfrak{b}+\mathfrak{a}\mathfrak{c}$. The set of ideals with operations of addition and multiplication forms a semiring, i.e. a structure with all the ring axioms except additive inverses.

3.2. **Coprime ideals.**

Definition. We say that two ideals $\mathfrak{a}, \mathfrak{b} \in A$ are **coprime** if $\mathfrak{a} + \mathfrak{b} = (1)$.

Remark. Since an ideal equals (1) if and only if it contains the element 1, we have that $\mathfrak{a} + \mathfrak{b}$ 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 know that $(m)+(n) = (\gcd(m, n))$, so (m) and (n) are coprime if and only if $\gcd(m, n) = 1$, i.e. if the numbers m and n are coprime.

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

Example. If $f \in (x) + (y) \subseteq \mathbb{Q}[x, y]$, then $f = \sum a_{ij} x^i y^j$ where we must have $a_{00} = 0$. This means that $1 \notin (x) + (y)$, so (x) and (y) are not coprime.

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

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

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

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

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

Recall that 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 addition and multiplication defined componentwise.

Given ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_n \subseteq A$, we have homomorphisms $A \to A/\mathfrak{a}_i$ for each i, and we can take a product homomorphism $\phi\colon A \to \prod_{i=1}^{n} A/\mathfrak{a}_i$ given by

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

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*

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

hence we have an isomorphism

$$A/\prod \mathfrak{a}_i = A/\ker \phi \cong \phi(A) = \prod A/\mathfrak{a}_i.$$

Proof assuming $n = 2$: ϕ is surjective: It's enough to show that $(1, 0), (0, 1) \in \phi(A)$, since if $\phi(x_1) = (1, 0)$ and $\phi(x_2) = (0, 1)$, since every element $(b_1 + \mathfrak{a}_1, b_2 + \mathfrak{a}_2)$ is then equal to $\phi(b_1 x_1 + b_2 x_2)$.

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

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

and 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 $\ker \phi = \mathfrak{a}_1 \cap \mathfrak{a}_2$, and we know that $\mathfrak{a}_1 \cap \mathfrak{a}_2 = \mathfrak{a}_1 \mathfrak{a}_2$. □

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. In the example above, we showed $(x-2), (2x^2-2) \subseteq \mathbb{Q}[x]$ are coprime. We therefore have

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

Main ideas:

- Sum of ideals
- Intersection of ideals
- Products of ideals
- The ideal $(a_1, \ldots, a_n)$
- Coprime ideals
- The Chinese remainder theorem