2.3. **Local rings.**

Definition. A ring A is **local** if it has precisely one maximal ideal.

Example. Every field is a local ring with maximal ideal (0).

Example. The ring $\mathbb{Z}$ is not local, since for each prime p, there is a maximal ideal (p).

Example. Let p be a prime, and let $k \geq 1$. Then the ideals of $\mathbb{Z}/(p^k)$ correspond to ideals of $\mathbb{Z}$ which contain (p^k). These are given by (n), where n divides p^k, and so the ideals of $\mathbb{Z}/(p^k)$ are the images of

$$(p^k) \subset (p^{k-1}) \subset \cdots \subset (p) \subset \mathbb{Z}.$$

The unique maximal ideal is the image of (p), so $\mathbb{Z}/(p^k)$ is local.

Example. Let k be a field, and let $A = k[x]/(x^2)$. The ideals of A are in bijection with the ideals of $k[x]$ which contain (x^2). Such an ideal is of the form (f) with f dividing x^2, which means that up to some scalar multiple it is either 1, x or x^2. So in $k[x]$ there are three ideals containing (x^2), namely $(1), (x)$ and (x^2). In A, if we let $\overline{x}$ be the image of x under the quotient map, we have three ideals total

$$(0) = (\bar{x}^2) \subset (\bar{x}) \subset (1) = A.$$

The ideal $(\bar{x})$ is the unique maximal element of A, so A is local.

Proposition. (1) *Let A be a local ring with maximal ideal $\mathfrak{m}$. Then the set of units in A is $A \setminus \mathfrak{m}$.*

(2) *Let A be a ring such that the set*

$$\mathfrak{m} = \{x \in A \mid x \text{ is not a unit}\}$$

forms an ideal. Then A is local with maximal ideal $\mathfrak{m}$.

Proof. First part: $x \in A$ is a unit $\Leftrightarrow$ x is not contained in any maximal ideal $\Leftrightarrow$ $x \notin \mathfrak{m}$.

Second part: Suppose $\mathfrak{a}$ is a maximal ideal of A, and let $x \in \mathfrak{a}$. Then x is not a unit, hence $x \in \mathfrak{m}$. It follows that $\mathfrak{a} \subseteq \mathfrak{m}$. Since $(1) \neq \mathfrak{m}$, it follows that $\mathfrak{m}$ is the unique maximal ideal of A. □

Example. Recall $\mathbb{R}(x)$, the field of real rational functions, which is the ring of expressions f/g with $f, g \in \mathbb{R}[x]$ and $g \neq 0$ (up to some equivalence relation). Let $A \subset \mathbb{R}(x)$ be the subring of those elements which can be written as

$$\frac{f}{g} \qquad f \in \mathbb{R}[x], g \in \mathbb{R}[x] \setminus (x).$$

So e.g.

$$\frac{x^2}{x+1}, \frac{x^3-2x}{5x+4}, \frac{x^3-x}{x^2-x} = \frac{x^2-1}{x-1} \in A$$

since $x+1, 5x+4, x-1 \notin (x)$, while e.g. $\frac{1}{x} \notin A$. Equivalently, A is the ring of the real rational functions which can be evaluated at 0, since we get a well-defined real number $f(0)/g(0)$ if and only if $f/g \in A$.

Claim: The ring A is local, with maximal ideal

$$\mathfrak{m} = \{f/g \in A \mid f(0)/g(0) = 0\} = \{f/g \mid f \in (x), g \in \mathbb{R}[x] \setminus (x)\}.$$

The homomorphism $A \to \mathbb{R}$ given by $f/g \mapsto f(0)/g(0)$ is surjective, with kernel $\mathfrak{m}$, so $\mathfrak{m}$ is a maximal ideal, and $A/\mathfrak{m} \cong \mathbb{R}$.[2]

3. Operations on ideals

Let A be a ring. We've seen three main sources of ideals, as principal ideals $(f) \subseteq A$ for some $f \in A$, as kernels $\ker \phi \subseteq A$ for a ring homomorphism $\phi\colon A \to B$, and by the general existence result giving us a maximal ideal $\mathfrak{m} \subset A$. This lecture, we will see a few natural operations which build new ideals from old.

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 $\mathfrak{a}_1, \ldots, \mathfrak{a}_n \subseteq A$, 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 $i_1, \ldots, i_n \in I$ 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 $\mathfrak{b}$. More generally $\sum_{i \in I} \mathfrak{a}_i$ is the smallest ideal containing each $\mathfrak{a}_i$.

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 $a_1, \ldots, a_n \in A$, then we write

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

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

$$f = xg_1 + yg_2 \qquad g_i \in \mathbb{Q}[x, y].$$

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 $f = xg_1 + yg_2$, 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 $a_1, a_2, \ldots, a_n, b \in A$, and let $1 \leq i, j \leq n$. Then we have an equality of ideals*

$$(a_1, \ldots, a_n) = (a_1, \ldots, a_{i-1}, a_i + ba_j, a_{i+1}, \ldots, a_n).$$

[2]To see that A is local, note that if $f/g \notin \mathfrak{m}$, then $f(0)/g(0) \neq 0$, so $g/f \in A$, and so f/g is a unit. Since all non-units are contained in $\mathfrak{m}$, this means $\mathfrak{m}$ is the unique maximal ideal.

Proof. For simplicity assume we want to show $(a_1, a_2) = (a_1, a_2 + ba_1)$. Clearly a_1 and $a_2 + ba_1$ lie in (a_1, a_2), so we have an inclusion $(a_1, a_2 + ba_1) \subseteq (a_1, a_2)$.

On the other hand, we have $a_1 \in (a_1, a_2+ba_1)$, and, since $a_2 = -ba_1+(a_2+ba_1)$, that $a_2 \in (a_1, a_2+ba_1)$. Thus $(a_1, a_2) \subseteq (a_1, a_2+ba_1)$, which gives the equality. $\square$

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 any set $\{\mathfrak{a}_i\}_{i \in I}$ of ideals of A, we have that $\cap_{i \in I} \mathfrak{a}_i$ 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 $f = \sum a_{ij} x^i y^j$, $a_{ij} \in \mathbb{Q}$, 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. This 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

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

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

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

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

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

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.