
Lecture 3. Radicals, local rings and modules; first examples

Let I be an ideal in R , we define the **radical** of I to be the ideal

$$\sqrt{I} = \{r \in R \mid r^n \in I \text{ for some } n > 0\}$$

An ideal I is called a **radical ideal** if $I = \sqrt{I}$. Note that $\sqrt{I}$ is itself a radical ideal, that is, $\sqrt{\sqrt{I}} = \sqrt{I}$.

◁ Show that $\sqrt{I}$ is an ideal. (Use that if $x^n \in I$ and $y^m \in I$ for some $n, m > 0$, then

$$(x + y)^{n+m-1} = \sum_{i+j=n+m-1} r_{i,j} x^i y^j, \quad r_{i,j} \in R$$

is also in I , as in the summands either $i \geq n$ or $j \geq m$.)

Proposition 2.7. $\sqrt{I} = \bigcap_{\mathfrak{p} \supset I} \mathfrak{p}$.

Proof. If $\mathfrak{p}$ is a prime ideal containing I , then $x^n \in I \subset \mathfrak{p}$ implies $x \in \mathfrak{p}$ hence $\sqrt{I} \subset \mathfrak{p}$. Conversely, if $x \notin \sqrt{I}$, then consider the multiplicative set $S = \{1, x, x^2, \dots\}$, which is disjoint from I since no power of x lies in I . By Krull's lemma (Proposition 2.6), there exists a prime ideal containing I and disjoint from S , hence not containing x . $\square$

In particular, if we take $I = (0)$ in the previous proposition, we see that

$$\sqrt{(0)} = \{r \in R \mid r^n = 0 \text{ for some } n > 0\}$$

is the intersection of all prime ideals of R . This is called the **nilradical** and is denoted $\mathcal{N}(R)$. The elements of the nilradical are called the **nilpotent** elements.

The intersection of all maximal ideals of a ring R is called the **Jacobson radical** of R and is denoted $\mathcal{J}(R)$.

◁ Show that $x \in \mathcal{J}(R)$ if and only if $1 - xy$ is a unit of R for all $y \in R$ (uses Zorn's lemma via Proposition 2.4).

◁ Show that $\sqrt{I \cdot J} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.

◁ Show that a maximal ideal is a prime ideal and a prime ideal is a radical ideal.

◁ Show that if a prime ideal $\mathfrak{p} = I \cap J$ for ideals I and J , then $\mathfrak{p} = I$ or $\mathfrak{p} = J$.

An important class of rings is given by the following.

Definition 2.8. A ring R is called a **local ring** if it has a unique maximal ideal $\mathfrak{m}$.

► In a local ring R , the unique maximal ideal $\mathfrak{m}$ coincides with the Jacobson radical of R .

◁ Show that in a local ring R , the units in R are precisely the elements in $R \setminus \mathfrak{m}$ (uses Zorn's lemma via Proposition 2.4); conversely, a ring R whose non-units form an ideal is a local ring.

Proposition 2.9. (*Prime avoidance*) Suppose that I is an ideal contained in $\bigcup_{i=1}^n \mathfrak{p}_i$ for some prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_n$, then $I \subset \mathfrak{p}_j$ for some j .

Proof. We argue by induction on n . The case $n = 1$ is trivial. For each i , we try to choose $x_i \in I \setminus \bigcup_{j \neq i} \mathfrak{p}_j$. If no such x_i exists for some i , then I is contained in a union of $n-1$ prime ideals and we are done by induction. So assume that for each i there exists $x_i \in I$ with $x_i \notin \bigcup_{j \neq i} \mathfrak{p}_j$. Since $I \subset \bigcup_{j=1}^n \mathfrak{p}_j$, we then have $x_i \in \mathfrak{p}_i$. Consider the element

$$y = \sum_{i=1}^n x_1 x_2 \dots x_{i-1} x_{i+1} \dots x_n$$

By construction, $y \in I$. For each i , the i^{th} summand $x_1 x_2 \dots x_{i-1} x_{i+1} \dots x_n$ is not in $\mathfrak{p}_i$, since $\mathfrak{p}_i$ is prime and none of its factors lies in $\mathfrak{p}_i$, whereas every other summand contains x_i and so lies in $\mathfrak{p}_i$. Hence $y \notin \mathfrak{p}_i$ for every i , which contradicts $I \subset \bigcup_{i=1}^n \mathfrak{p}_i$. $\square$

► The name comes from reading the statement in the contrapositive. If I is not contained in any single $\mathfrak{p}_j$, then there is an element $x \in I$ lying in none of the $\mathfrak{p}_j$. That element “avoids” all the primes at once. So the lemma is a tool for finding elements of an ideal that avoid finitely many prime ideals.

2.3 Modules

A **module** M over R is an abelian group $(M, +)$ together with a map $R \times M \rightarrow M$, $(r, m) \mapsto rm$ which satisfies:

$$\begin{aligned} (r_1 r_2)m &= r_1(r_2 m) \\ (r_1 + r_2)m &= r_1 m + r_2 m \\ r(m_1 + m_2) &= r m_1 + r m_2 \\ 1m &= m \end{aligned}$$

In other words, it is an abelian group on which R acts linearly. If $R = \mathbb{Z}$, then an R -module is the same thing as an abelian group. If R is a field k , then an R -module is a k -vector space. R is a module over itself. A **submodule** of a module M is a subgroup $N \subset M$ such that $rn \in N$ for all $r \in R$ and $n \in N$. A submodule of a ring R is just the same thing as an ideal in that ring. To a module M , we can associate an ideal via the **annihilator** construction

$$\text{ann}(M) := \{r \in R : rm = 0 \text{ for all } m \in M\}.$$

Given an ideal I , we can consider R/I as an R -module. For such modules, we have $I = \text{ann}(R/I)$. The modules of the form R/I are called **cyclic** modules. They have the property that they can be generated by a single element, that is, there exists $x \in M$ such that $M = R \cdot x$.

More generally, we say that an R -module M is **finitely generated** (as a module) if there exist finitely many elements $x_1, \dots, x_m \in M$ such that $M = R \cdot x_1 + R \cdot x_2 + \dots + R \cdot x_m$.

< Show that if $M = R \cdot x$ is a cyclic module, then M is isomorphic as an R -module to a module of the form $R/\text{ann}(M)$.

For $m \in M$, we can also define an ideal $\text{ann}(m) := \{r \in R : rm = 0\}$. Then, by definition, $\text{ann}(M) = \bigcap_{m \in M} \text{ann}(m)$.

Proposition 2.10. *Let M be an R -module and let $m \in M$ be non-zero. Suppose that $\text{ann}(m)$ is maximal, with respect to inclusion, among the annihilators of non-zero elements of M ; that is, there is no non-zero $m' \in M$ with $\text{ann}(m') \supsetneq \text{ann}(m)$. Then $\text{ann}(m)$ is a prime ideal.*

Proof. Write $I = \text{ann}(m)$. Then I is proper since $1 \cdot m = m \neq 0$. Given $ab \in I$, suppose that $a \notin I$. Then $am \neq 0$. On the other hand, we have $\text{ann}(am) \supset I$. By hypothesis, it cannot be larger, hence $\text{ann}(am) = I$. Now, it follows that b annihilates am , hence $b \in I$. $\square$

A prime ideal of the form $\text{ann}(m)$ with $m \neq 0$ is called an **associated prime** of M . Proposition 2.10 says that the maximal annihilators are associated primes. The converse fails: for $R = k[x, y]$ and $M = R/(x^2, xy)$, both $\text{ann}(\bar{y}) = (x)$ and $\text{ann}(\bar{x}) = (x, y)$ are associated primes, but (x) is not maximal among annihilators.

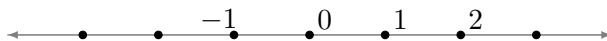
3 Examples

Let's have some examples to play with.

■ k will always denote a field.

There are two main classes of rings that are of interest. Polynomial rings (and their quotients) with field coefficients and rings of integers of algebraic number fields (finite ring extensions of $\mathbb{Z}$). The former class may be referred to as “geometric” as it relates to Algebraic Geometry and the latter class may be referred to as “arithmetic” as it relates to Number Theory.

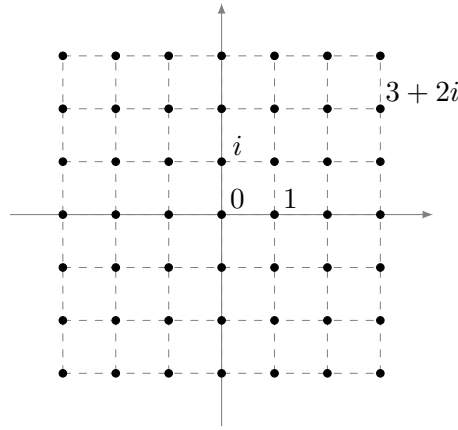
The most fundamental ring is $\mathbb{Z}$ which you encountered in nursery. Prime ideals of $\mathbb{Z}$ are (p) for p a prime number and (0) .



The polynomial ring in one variable $k[X]$ which you encountered in school is also fundamental. The prime ideals are (f) for f an irreducible polynomial and (0) . If k is algebraically closed, then the only monic irreducible polynomials are $X - \lambda$, $\lambda \in k$.

Both $\mathbb{Z}$ and $k[X]$ are Euclidean domains, hence PID, and so UFD.

The simplest quadratic extension is the ring of Gaussian integers $\mathbb{Z}[i]$. We can draw a picture of it as follows:



< Show that $\mathbb{Z}[i]$ is a Euclidean domain using the norm $|a + bi| = a^2 + b^2$. (Use the fact that disks of unit norm centred at Gaussian integers cover all of the complex plane.)

< Show that for a non-zero $a \in \mathbb{Z}$, the ideal $(a) = (ai)$ of $\mathbb{Z}[i]$ is prime if and only if $a = \pm p$ for a prime number p of the form $4n + 3$. Show also that $(a + bi)$ with $a, b \neq 0$ is a prime ideal if and only if $a^2 + b^2$ is a prime number.

The Eisenstein integers $\mathbb{Z}[\omega]$ with $\omega = e^{2\pi i/3} = \frac{-1+\sqrt{3}i}{2}$ and its subring $\mathbb{Z}[\sqrt{-3}]$ are also good examples to know (note that $\mathbb{Z}[\sqrt{-3}]$ is not a UFD but $\mathbb{Z}[\omega]$ is).

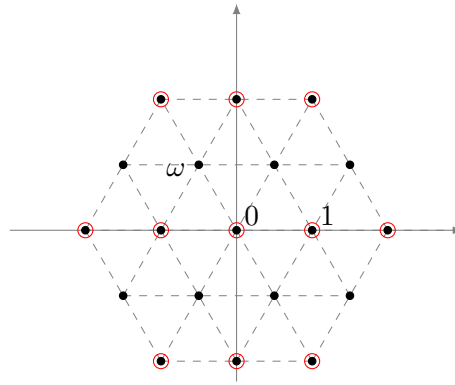


Figure 1: The elements of the ring $\mathbb{Z}[\omega]$, $\omega = e^{2\pi i/3}$. The subring $\mathbb{Z}[\sqrt{-3}]$ is marked red.

< Show that the Eisenstein integers $\mathbb{Z}[\omega]$ with norm $|a + b\omega| = a^2 - ab + b^2$ form a Euclidean domain.

< Show that the ideal $I = (2, 1 + \sqrt{-3})$ is not principal in the ring $\mathbb{Z}[\sqrt{-3}]$. (Use that the norm given by $|a + b\sqrt{-3}| = a^2 + 3b^2$ is multiplicative.)

< Show that the ideal $I = (2, 1 + \sqrt{-3})$ in $\mathbb{Z}[\sqrt{-3}]$ satisfies $I^2 = (2) \cdot I$, hence in $\mathbb{Z}[\sqrt{-3}]$, the ideals do not factor uniquely into prime ideals.