4. Lecture 4 – Further operations on ideals + modules

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 $xb \in \mathfrak{a}$. (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 $a \in \mathfrak{a}$. But 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 $x \in (\mathfrak{a} : (b))$.

Example. If $m, n \geq 1$, then $x \in ((m) : (n))$ if and only if $xn \in (m)$, so

$$((m) : (n)) = \{x \mid xn \in (m)\} = \{x \mid m \text{ divides } xn\}.$$

This means that $((m) : (n)) = (k)$, we in particular have that k is the smallest positive integer such that m divides kn. In particular, if n divides m, then $k = m/n$.

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. In an integral domain A, if $a \neq 0$, then $\mathrm{Ann}(a) = (0)$.
In any ring A, the set of zero-divisors is $\bigcup_{a \in A \setminus \{0\}} \mathrm{Ann}(a)$.

4.2. Radicals.

Definition. Let A be a ring, $\mathfrak{a} \subseteq A$ an ideal. The **radical** of $\mathfrak{a}$ is the set of $x \in A$ such that there is an $n \geq 1$ such that $x^n \in \mathfrak{a}$. We denote this by $\mathfrak{r}(\mathfrak{a})$, one occasionally sees $\sqrt{\mathfrak{a}}$.

Example. The radical $\mathfrak{r}((0))$ is exactly the same thing as the nilradical $\mathfrak{N} \subseteq A$, since $x^n \in (0)$ for some $n \Leftrightarrow x^n = 0$ for some $n \Leftrightarrow x \in N$.

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 $\mathfrak{r}(\mathfrak{a}) = \phi^{-1}(\mathfrak{N})$.*

Proof. Let $x \in A$. Then if $x \in \mathfrak{r}(\mathfrak{a})$ we have for some $n \geq 1$ that

$$x^n \in \mathfrak{a} \Leftrightarrow \phi(x^n) = 0 \Leftrightarrow \phi(x)^n = 0 \Rightarrow \phi(x) \in \mathfrak{N}.$$

□

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 $\mathfrak{r}((n))$ if and only if there is an $l \geq 1$ such that $m^l \in (n)$, which is if and only if m^l is divisible by n. If every p_i divides m, then $m^{\max e_i}$ is divisible by n, while if some p_i does not divide m, then no power of m is divisible by n.

Summing up, 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 $p_1 \ldots p_k$, and we thus get

$$\mathfrak{r}((n)) = (p_1 \cdots p_k).^2$$

Example. Consider $\mathbb{Q}[x]$ and the ideal (x^m). Then $f \in \mathfrak{r}((x^m))$ 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 $f \in \mathfrak{r}((x^m))$ if and only if $a_0 = 0$, which is if and only if $f \in (x)$. We've shown

$$\mathfrak{r}((x^m)) = (x).$$

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 $\mathfrak{a}^e$. The **contraction** of $\mathfrak{b}$ is $\phi^{-1}(\mathfrak{b}) \subseteq A$, 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 $\phi(a_1) + \cdots + \phi(a_n)$ with $a_i \in \mathfrak{a}$.

Proposition. *The operation of contraction sends prime ideals to prime ideals.*

Proof. Let $\mathfrak{p} \subset B$ be a prime ideal, and let $\phi\colon A \to B$ be a ring homomorphism. We must show that $\mathfrak{p}^c = \phi^{-1}(\mathfrak{p})$ is a prime ideal. If $a, a' \in A \setminus \phi^{-1}(\mathfrak{p})$, then $\phi(a), \phi(a') \notin \mathfrak{p}$, so $\phi(aa') = \phi(a)\phi(a') \notin \mathfrak{p}$, which means $aa' \notin \phi^{-1}(p)$, and that means $\phi^{-1}(\mathfrak{p})$ is prime. ☐

4.4. **Modules.** Informally, a module is a structure where you can add elements in the module, and multiply module elements by the ring elements.

Definition. Let A be a ring. A **module** over A (or "A-module") is an abelian group $(M, +)$ equipped with an operation $A \times M \to M$, denoted

$$(a, m) \mapsto am,$$

satisfying

(1) $1m = m \qquad \forall m \in M.$
(2) $a(bm) = (ab)m \qquad \forall a, b \in A, m \in M$
(3) $(a + b)m = am + bm \qquad \forall a, b \in A, m \in M$
(4) $a(m + n) = am + bn \qquad \forall a \in A, m + n \in M.$

Example. For any ring A, the 0-module has one element 0, and addition and multiplication are trivially defined.

[2] Look up the "abc conjecture" for a natural appearance of this operation in number theory.

Example. Let k be a field. Then a k-module is quite literally the same thing as a k-vector space.

Example. A $\mathbb{Z}$-module is the "same thing" as an abelian group, meaning any abelian group admits a unique structure as a $\mathbb{Z}$-module. To see this, let G be an abelian group. We define a $\mathbb{Z}$-module structure on G by, for $n \in \mathbb{Z}, g \in G$

$$ng = \begin{cases} \overbrace{g + \cdots + g}^{n} & \text{if } n > 0 \\ 0g = 0 \\ ng = \overbrace{(-g) + \cdots + (-g)}^{-n} & \text{if } n < 0. \end{cases}$$

One can check that this is a well-defined $\mathbb{Z}$-module structure. Moreover, this $\mathbb{Z}$-module structure is forced on us by the axioms: If $n > 0$ we must have

$$ng = (1 + \cdots + 1)g = 1g + 1g + \cdots + 1g = \overbrace{g + \cdots + g}^{n},$$

and similar considerations tell us what ng has to be for $n \leq 0$.

Example. Let $\mathfrak{a} \subseteq A$ be an ideal. Then $\mathfrak{a}$ is an A-module in a natural way, since given $x \in A$ and $a \in \mathfrak{a}$, we have $xa \in \mathfrak{a}$, and the operation $(x, a) \mapsto xa$ satisfies the axioms of the definition.

Example. Let $\phi\colon A \to B$ be a homomorphism. Then B has a natural structure of A-module, defined by

$$ab = \phi(a)b \qquad \forall a \in A, b \in B.$$

This generalises the useful fact from field theory that if $\phi\colon k \to k'$ is a homomorphism of fields, then k' is a k-vector space.

Definition. Let M and N be A-modules. A **homomorphism** of A-modules from M to N is a map $\phi\colon M \to N$ such that

$$\phi(m + m') = \phi(m) + \phi(m') \qquad \forall m, m' \in M$$
$$\phi(am) = a\phi(m) \qquad \forall a \in A, m \in M$$

If ϕ is a bijection, we say it is an **isomorphism** of A-modules.

Example. For A-modules M and N, we always have a homomorphism $0\colon M \to N$ given by

$$0(m) = 0 \qquad \forall m \in M.$$

Example. Let k be a field, and let M and N be k-modules. Then a homomorphism $M \to N$ is the same thing as a linear map of vector spaces. So if M and N are finite-dimensional as vector spaces, we can choose bases and represent ϕ by a $(\dim N) \times (\dim M)$-matrix.

Example. A homomorphism of $\mathbb{Z}$-modules is the same thing as a homomorphism of (abelian) groups. This boils down to the fact that given a homomorphism $\phi\colon M \to N$ of abelian groups, the condition

$$\phi(nx) = n\phi(x)$$

is automatically satisfied.

Example. Let $a \in A$, and consider $(a) \subseteq A$ as an A-module. There is a homomorphism of A-modules

$$\phi\colon A \to (a)$$

given by

$$\phi(x) = xa.$$

This is surjective, with kernel equal to $\operatorname{Ann}(a)$.

Definition. Let M and N be A-modules, and let $\operatorname{Hom}_A(M, N)$ be the set of homomorphisms. This set has a structure of an A-module, where for $\phi, \psi \in \operatorname{Hom}_A(M, N)$, $a \in A$ and $m \in M$, we have

$$(\phi + \psi)(m) = \phi(m) + \psi(m)$$
$$(a\phi)(m) = a\phi(m)$$

Example. Let k be a field, and consider the modules k^m, k^n. Then $\operatorname{Hom}_k(k^m, k^n)$ is naturally identified with the set of $(n \times m)$-matrices with entries in k, and the above states that this set has a natural structure of k-module (or k-vector space).