Math 614: Lecture notes

Sep 12, 2007

Note that for any ideal I of R, the subspace $V(I)$ of $\operatorname{Spec}(R)$ is homeomorphic with $\operatorname{Spec}(R/I)$ in such a way that the composition $\operatorname{Spec}(R/I) \to V(I) \to \operatorname{Spec}(R)$ is equal to the map $\operatorname{Spec}(\pi) : \operatorname{Spec}(R/I) \to \operatorname{Spec}(R)$, where $\pi : R \to R/I$ is the natural projection map.

Recall that every nonzero ring has maximal ideals.

Corollary. *If I is a proper ideal of R, there is a maximal ideal of R containing I.*

Proof. Since $R/I \neq 0$, there is a maximal ideal $\mathfrak{n}$ of R/I whose preimage in R is also a maximal ideal, and contains I. □

Corollary. *Let $u \in R$. u is a unit $\iff u \notin \bigcup \Omega(R)$.*

Proof. u is a unit $\iff (u) = R \iff (u)$ is not a proper ideal $\iff (u)$ is not contained in any maximal ideal $\iff u \notin \bigcup \Omega(R)$. □

Also recall that the nilradical $\mathcal{N}(R)$ of R is defined to be the ideal of all nilpotent elements. Define the *radical* $\sqrt{I}$ of an ideal I to be the set of elements whose images in R/I are nilpotent. Recall that $\mathcal{N}(R) = \bigcap \operatorname{Spec}(R)$.

Corollary. *$\sqrt{I} = \bigcap V(I)$.*

Proof. For an element $x \in R$, let $\bar{x} = x + I$ denote the image of x in R/I.

$$x \in \sqrt{I} \iff \bar{x} \in \mathcal{N}(R) \iff \bar{x} \in \bigcap \operatorname{Spec}(R/I) \iff x \in \bigcap V(I)$$

□

Definition. A ring R is *local* if it has exactly one maximal ideal. If $\mathfrak{m}$ is the unique maximal ideal, the field $k = R/\mathfrak{m}$ is called the *residue field* of R. A short way to encode this information is to say that $(R, \mathfrak{m})$ (or $(R, \mathfrak{m}, k)$) *is a local ring.*

R is *semilocal* if $\Omega(R)$ is a finite set.

Warning:

Although these definitions of 'local' and 'semilocal' agree with those found in Atiyah-MacDonald, they disagree with the ones found in Mel Hochster's lecture notes.

Generation, Sum, Intersection, and Product

Fix a ring R. Let S be a subset of an R-module M. Let

$$N := \{\sum_{i=1}^{n} r_i s_i \mid n \in \mathbb{N}^1, r_i \in R, s_i \in S\}$$

By convention, the empty sum $\sum_{n=1}^{0} z_i$ in M is the zero element. Clearly N is a subset of M. In fact it is a submodule of M, since a sum of two sums of the above form is a sum of the above form, and preservation of products with elements of R follows by the distributive law. Moreover, any submodule of M that contains S must contain N, so that N is the smallest submodule of M that contains N. We say that S *generates* N (over R), and we write $N = (S)$. To say that a set generates an ideal is to say that it generates I as a submodule of R.

Let M be an R-module, S a set, and $\{N_s\}_{s \in S}$ be an S-indexed collection of submodules of M. (i.e. N_s is a submodule of M for all $s \in S$)

The *sum* $N = \sum_{s \in S} N_s$ is by definition the submodule of M generated by $\bigcup_{s \in S} N_s$.

The intersection $\bigcap_{s \in S} N_s$ is itself a submodule of M.

The *product* of an ideal I with a module M is the module IM generated by the set $\{im \mid i \in I, m \in M\}$.

We have the *distributive law*: $I \cdot \sum_{s \in S} N_s = \sum_{s \in S}(IN_s)$.

For ideals I, J, we always have $IJ \subseteq I \cap J$, since for any generator $x = ij$, we have $x \in I$ and $x \in J$. Conversely, if $I + J = R$, then $IJ = I \cap J$

Proof. Let $i \in I$, $j \in J$ with $i + j = 1$. Then for any $x \in I \cap J$, we have $x = 1x = (i + j)x = ix + jx$. Since $x \in J$ we have $ix \in IJ$. Since $x \in I$ we have $jx \in JI = IJ$. Hence, $x = ix + jx \in IJ$. □

---

[1] Our convention will always be that $\mathbb{N} = \{0, 1, 2, \dots\}$ is the set of *nonnegative* integers

The property that $I + J = R$ is so important that we give it a name; such a pair of ideals is *comaximal.* The word 'coprime' is also sometimes used, for the following reason:

Proposition. *If $m, n \in \mathbb{Z}$, then $(m) + (n) = \mathbb{Z}$ iff $(m, n) = 1$.*

Proof. The Euclidean algorithm! $\square$

Products of rings:

Let $\{R_s\}_{s \in S}$ be an S-indexed collection of rings, where S is a set. Then define the *product* ring $R = \prod_{x \in S} R_x$ as follows:

As a set, $R := \{(r_x)_{x \in S} \mid r_x \in R_x\}$. Addition and multiplication are given coordinate-wise. The identity element $1_R = (1_{R_x})$. Then for each $y \in S$ there is a projection map $\pi_y : R \to R_y$ given by $\pi_y((r_x)_{x \in S}) := r_y$. Note that for any ring B, to give a map $B \to R$ is equivalent to giving a collection of maps $B \to R_x$, one for each $x \in S$. Indeed, this construction gives S-indexed products in the category of rings, in the sense defined in the Sep 10 lecture.

In particular, if R is a ring and $\{I_s\}_{s \in S}$ are ideals of R, the projection maps $R \to R/I_s$ induce a map $\varphi : R \to \prod_{s \in S} R/I_s$, given by $\varphi(r) = (r + I_s)_{s \in S}$. It is clear that $\ker \varphi = \bigcap_{s \in S} I_s$. Moreover, we have the

Proposition (Chinese Remainder Theorem). *Suppose the ideals $\{I_1, \ldots, I_n\}$ are pairwise comaximal. Then the map $\varphi : R \to \prod_{j=1}^n R/I_j$ is surjective.*

Proof. For each pair i, j with $i \neq j$, choose $u_{ij} \in I_i$ and $v_{ij} \in I_j$ with $u_{ij} + v_{ij} = 1$. For any fixed i, let $e_i := \prod_{1 \leq j \leq n, j \neq i} v_{ij}$. Then if $\pi_j : \prod_{i=1}^n R/I_i \to R/I_j$ are the projection maps, we have $\pi_i(\varphi(e_i)) = 1$ and $\pi_j(\varphi(e_i)) = 0$ whenever $i \neq j$. Hence any element of $\prod_i R/I_i$ is of the form $\sum_{i=1}^n r_i \varphi(e_i) = \varphi(\sum_{i=1}^n r_i e_i)$. $\square$

This implies the classical Chinese Remainder Theorem on integer congruences, first proved in the third or fourth century by Sun Zi.

Colons, Annihilators, and Hom

For ideals I and J, define $(J : I) := \{x \in R \mid Ix \subseteq J\}$. Note that $J : I = J : (I + J)$, so we may restrict our attention to pairs where $J \subseteq I$. Also, $J : I$ is always an ideal.

There are two natural ways to extend this definition to the case of modules:

First, if $N \subseteq M$ is a submodule, $(N :_R M) := (N : M) := \{x \in R \mid rM \subseteq N\}$. This is an ideal of R, and it is immediate that $N : M = 0 : (M/N)$. This latter form of colon ideal has a special name, an *annihilator*. Namely, the *annihilator of* M is $\operatorname{Ann}(M) := \operatorname{Ann}_R M := (0 :_R M)$. In the case of finitely generated modules over Noetherian rings, the annihilator is especially important.

Secondly, if $N \subseteq M$ is a submodule and I is an ideal, define $(N :_M I) := \{z \in M \mid Iz \subseteq N\}$. This is a submodule of M. Similar to the previous case, the *annihilator of* I *in* M is the module $\operatorname{Ann}_M I := (0 :_M I)$.

The following properties are immediate, and should be verified by the reader:

1. $N \subseteq (N :_M I)$, and $\pi(N :_M I) = 0 :_{M/N} I$, where $\pi : M \to M/N$ is the natural surjection.
2. $(N : M)M \subseteq N$ and $I(N :_M I) \subseteq N$.
3. (a) $(N :_M I) :_M J = N :_M IJ = (N :_M J) :_M I$, and
   (b) $(N :_R M) :_R I = N :_R IM = (N :_M I) :_R M$.
4. $(\bigcap_s N_s) : M = \bigcap_s (N_s : M)$, and $(\bigcap_s N_s) :_M I = \bigcap_s (N_s :_M I)$.
5. $N :_R (\sum_s P_s) = \bigcap_s (N :_R P_s)$, and $N :_M (\sum_s I_s) = \bigcap_s (N :_M I_s)$.

Proposition. *Let* M *be an* R*-module and* I *an ideal. Then* $\operatorname{Hom}_R(R/I, M) \cong (0 :_M I)$ *as* R*-modules.*

Proof. Define $z : \operatorname{Hom}_R(R/I, M) \to (0 :_M I)$ via $z(f) = f(\bar{1})$, where $\bar{r}$ is the image of $r \in R$ in R/I. We have $If(\bar{1}) \subseteq f(\bar{I}) = f(0) = 0$, so $z(f) = f(\bar{1}) \in (0 :_M I)$ as required.

z is clearly an R-module map, as $z(rf+g) = (rf+g)(\bar{1}) = rf(\bar{1}) + g(\bar{1}) = rz(f) + z(g)$.

z is injective, for if $z(f) = 0$, then $f(\bar{1}) = 0$, so that for any $\bar{r} \in R/I$, $f(\bar{r}) = rf(\bar{1}) = 0$, whence $f = 0$.

z is surjective. Let $x \in 0 :_M I$, and define $g : R \to M$ by $g(r) := rx$. Then for any $i \in I$, $g(i) = ig(1) = ix = 0$, whence $I \subseteq \ker g$, so that g factors as $g = f \circ \pi$, where $R \xrightarrow{\pi} R/I \xrightarrow{f} M$. Then $z(f) = f(\pi(1)) = g(1) = x$. □