CA LECTURE 20

SCRIBE: MATTHEW WRIGHT

A mixed bag of facts today, building up to a discussion of DVR's and Dedekind domains on Wednesday

Lemma: if I is comaxl with each of $J_1, \dots J_n$ then I is comaxl with $J_1 \dots J_n$.

Proof: otherwise let P be prime such that $I + J_1 \dots J_n \subseteq P$. Then $I \subseteq P$ and $J_i \subseteq P$ for some i, so $R = I + J_i \subseteq P$, contradiction.

Theorem (Chinese Remainder theorem): Let $I_1, \dots I_n$ be pairwise comaxl. Then $I_1 \cap \dots I_n = I_1 \dots I_n$ and the map $r + I_1 \dots I_n \mapsto (r + I_1, \dots r + I_n)$ sets up an IM between $R/I_1 \dots I_n$ and the direct product of the R/I_j.

Proof: by induction $I_2 \dots I_n = I_2 \cap \dots I_n$ and by the last result I_1 is comaxl with this ideal. We say last time that if I and J are comaxl then $I \cap J = IJ$ so putting it all together

$$I_1 \cap \dots I_n = I_1 \cap (I_2 \dots I_n) = I_1 \dots I_n.$$

Now consider the map $r \mapsto (r + I_1, \dots r + I_n)$. Clearly its a HM with kernel $I_1 \cap \dots I_n = I_1 \dots I_n$. So it suffices to show irs surjective, for which by linearity its enough to show that for every i the point $(0 + r_1, \dots 1 + I_i, \dots 0 + I_n)$ is in the image. But this is easy: I_i is comaximal with $\prod_{j \neq i} I_j$ and so we may find b such that $b + I_i = 1 + I_i$ while $b + I_j = 0 + I_j$ for $j \neq i$.

Now for another application of Nakayama. The idea is that we can sometimes reduce the problem of finding a generating set for a module/ideal to a problem about finding a spanning set for a VS (which is a better deal because we have all the tools of linear algebra available).

Theorem: Let R be local, M the unique maxl ideal and N a fg R-module. Then N/MN is a (finite diml) VS over the field R/M. If $x_i \in N$ for $1 \leq i \leq k$ and the cosets $x_i + MN$ form a spanning set for N/MN then the x_i generate N as an R-module.

Proof: Let $\bar{N}$ be the submodule generated by the x_i. Verify that $N = \bar{N} + MN$ and thus that $N/\bar{N} = M(N/\bar{N})$. Now use Nakayama on the fg module $N/\bar{N}$ to see $N/\bar{N} = 0$, hence $N = \bar{N}$.

It will be convenient to know some facts about Artin local rings (actually any Artin ring is a finite product of Artin local rings but we do not need this).

Recall that last time we analysed N'ian local rings and showed that if M is the unique maxl ideal of such a ring and $M^n = 0$ then the ring is Artinian.

Lemma: let R be an N'ian local ring and let M be the unique maxl ideal. Then for all n, R/M^n is an Artin local ring.

Proof: R/M^n is easily seen to be a N'ian local ring with unique maxl ideal M/M^n. Now $(M/M^n)^n = 0$ and we may appeal to the analysis from last time.

Theorem: Let R be an Artin local ring with maximal ideal M, and let $k = R/M$. Then TFAE:

(1) Every ideal is principal.
(2) M is principal.

(3) The dimension of M/M^2 as a k-VS is at most one.

Proof: clearly 1 implies 2 and 2 implies 3. 3 implies 2 because R is N'ian, hence M is a fg R-module, and so by the last theorem if $x + M^2$ spans M/M^2 then x generates M.

We are left to show that if M is principal all ideals are principal. Let $M = (x)$. Since we are in an Artin ring M is the only prime ideal, in particular M is the nilradical and so $x^n = 0$ for all large n.

Let I be any ideal with $I \neq 0, R$. Then $I \subseteq M = (x)$ but $I \nsubseteq (x^n) = 0$ for n large so we may find r with $I \subseteq (x^r)$ and $I \nsubseteq (x^{r+1})$. Let $y \in I$ with $y \notin (x^{r+1})$, so $y = bx^r$ where $b \notin (x)$. Since $(x) = M$ we see that b is a unit hence $x^r = b^{-1}y \in I$ and so $I = (x^r)$.

Note: in fact we showed that under these circumstances every ideal $I \neq 0, R$ is a power of the maximal ideal. This will be useful a bit later in the treatment of DVRs.

Now we start to discuss another important class of rings, the *discrete valuation rings*. This is a subclass of the more general *valuation rings* but we defer the general discussion.

If K is a field then a *discrete valuation* on K is a surjection v from K to $\mathbb{Z} \cup \{\infty\}$ such that $v(ab) = v(a) + v(b)$, $v(a+b) \geq \min\{v(a), v(b)\}$. We adopt the conventions $n + \infty = \infty + \infty = \infty$ and $n < \infty$ for all $n \in \mathbb{Z}$.

Example (p-adic valn): $K = \mathbb{Q}$ and $v_p(q)$ is the unique n such that $q = p^n r/s$ where r, s are integers not divisible by p.

The *valuation ring* is the set of $a \in K$ such that $v(a) \geq 0$. It is easy to see that a is a unit in this ring iff $v(a) = 0$. Also easily the set $\{a : v(a) > 0\}$ forms an ideal and so the valuation ring is a local ring.

Let I be a nonzero ideal of the valn ring and let $a \in I$ be nonzero with $v(a) = k$ minimal. Then for all nonzero b with $v(b) \geq k$, $v(ba^{-1}) = v(b) - v(a) \geq 0$ and so easily $I = (a) = \{b : v(b) \geq k\}$. So immediately the valuation ring is a Noetherian PID. What is more if t is such that $v(t) = 1$ then every nonzero ideal is (t^k) for some $k \geq 0$.