CA LECTURE 16

SCRIBE: GEORGE SCHAEFFER

Start with some generalities: suppose that R is a ring, I is an ideal of R and M is an R-module. Then IM is the least submodule of M containing all products am with $a \in I$ and $m \in M$, or more explicitly IM consists of all finite sums $\sum_i a_i m_i$ where $a_i \in I$ and $m_i \in M$. It's easy to see that if we set $(r + I)m = m + IM$ then M/IM is an R/I-module.

Now we briefly discuss fg R-modules. Suppose that M is fg and is generated by $m_1, \dots m_n$. Let ϕ be an R-linear map and write

$$\phi(m_j) = \sum_{i=1}^{n} a_{ij} m_i,$$

where we note that there may be many choices for the a_{ij} . We can see $A = (a_{ij})$ as an $n \times n$ matrix which represents ϕ.

Fact (the "Cayley-Hamilton theorem"): if p is the determinant of the matrix $xI - A$ then $p \in R[x]$ is monic and $p(\phi) = 0$, to be more explicit if $p = \sum_{i=0}^{n} a_i x^i$ then for all $m \in M$ we have $\sum_{i=0}^{n} a_i \phi^i(m) = 0$.

Proof: Computation which we omit. Maybe sketch later.

We only use the corollary: if M is fg, I is an ideal, and ϕ is a linear map from M to M with $im(\phi) \subseteq IM$, then there is $p = x^n + \sum_{i<n} a_i x^i$ such that $a_i \in I$ and $p(\phi) = 0$.

A very important corollary is

Nakayama's lemma: if I is contained in the Jacobson radical of R, M is fg and $M = IM$ then $M = 0$.

Proof of Nakayama: let $\phi = id_M$ then $im(\phi) = M \subseteq IM = M$, so we get that there is $a \in I$ such that $(1 + a)m = 0$ for all m. Since a is in the Jacobson radical, $1 + a$ is a unit and so $m = 0$ for all $m \in M$ that is $M = 0$.

Now we discuss integrality: this is a generalisation of algebraicity in field theory but is somewhat less well-behaved (in particular the notion of the algberaic closure of a field has no exact parallel).

If A and B are rings with $A \leq B$ and $b \in B$, we say b is *integral over* A iff $p(b) = 0$ for some monic $p \in A[x]$.

We need the notion of a *faithful* module: M is faithful iff $Ann(M) = 0$ where $Ann(M)$ is the ideal of R given by

$$Ann(M) = \{r \in R : \forall m \in M \; rm = 0\}$$

The following characterisations are very useful:

Theorem 1. *Let $A \leq B$ and $b \in B$.*

(1) *b is integral over A.*
(2) *$A[b]$ is module finite over A.*
(3) *There is a subring B' of B such that $A[b] \subseteq B'$ and B' is module finite over A.*

(4) *There is a faithful $A[b]$-module M which is fg as an A-module.*

Proof. To show 1 implies 2, suppose that b is integral over A. We have an equation $b^n = \sum_{i<n} a_i b^i$ with $a_i \in A$ and by an easy induction all powers of b lie in the A-submodule generated by $\{b^j : j < n\}$.

To show 2 implies 3 let $B' = A[b]$. To show 3 implies 4 let $M = B'$ (note: if $R \leq S$ then S is always a faithful R-module, because if $r \in Ann(S)$ then $r = r1 = 0$)

Finally we show 4 implies 1. Consider the map $\phi : m \mapsto bm$, this is A-linear and so there is monic $p \in A[x]$ with $p(\phi) = 0$. This is equivalent to saying that $p(b)m = 0$ for all $m \in M$, and by faithfulness we have $p(b) = 0$. □

Remark: If k and l are fields with $k \leq l$ then $b \in l$ is algebraic over k iff it is integral over k.

Definition 1. *Let $A \leq B$.*

(1) *The* integral closure of A in B *is the set of $b \in B$ which are integral over A.*
(2) *B is integral over A iff all $b \in B$ are integral over A, that is the integral closure of A in B is B.*
(3) *A is* integrally closed in B *iff all elements which are integral over A are in A, that is the integral closure of A in B is A.*

Theorem 2. *Let A and B be rings with $A \leq B$. The integral closure of A in B is a subring of B.*

Proof. Let b_1 and b_2 be integral over A. Immediately from the definition b_2 is integral over $A[b_1]$, so $A[b_1]$ is module finite over A and also $A[b_1, b_2]$ is module finite over $A[b_1]$. By an old argument (just multiply the generating sets) we see that $A[b_1, b_2]$ is module finite over A, so that by clause 3 in the characterisation of integrality above all elements of $A[b_1, b_2]$ are integral over A. In particular $b_1 + b_2$ and $b_1 b_2$ are integral over A. □

Theorem 3. *Let A, B, C be rings with $A \leq B \leq C$. If B is integral over A and C is integral over B then C is integral over A.*

Proof. Let $c \in C$ and let $f \in B[x]$ be monic with $f(c) = 0$. Let $b_1, \dots b_m$ be the coefficients of f. Arguing as in the last proof $B' = A[b_1, \dots b_m]$ is module finite over A, and since $f \in B'[x]$ we see that c is integral over B' so that $B'[c]$ is module finite over B'. Hence $B'[c]$ is module finite over A, thus (clause3 in the equivalence again) c is integral over A. □