MAS439/MAS6320
CHAPTER 5: INTEGRAL EXTENSIONS

EVGENY SHINDER (PARTLY BASED ON NOTES BY JAMES CRANCH)

5.1. **Integral Elements and Integral Extensions.** Let R be a commutative ring. Recall from last semester that an *R-algebra* is a commutative ring S together with a homomorphism $f : R \to S$.

In this section we'll talk about some nice classes of R-algebras.

Recall from the first lecture that, when we have an R-algebra S, then S is also an R-module.

Suppose we have a chain of homomorphisms of commutative rings

$$R \xrightarrow{f} S \xrightarrow{g} T.$$

Then f makes S into an R-algebra, g makes T into an S-algebra, and gf makes T into an R-algebra.

Proposition 5.1. *Suppose given a chain of homomorphisms as above. If S is a finitely-generated R-module, and T is a finitely-generated S-module, then T is also a finitely-generated R-module.*

Proof. If S is a finitely-generated R-module, then there are elements $s_1, \dots, s_m \in S$ such that any element $a \in S$ can be expressed as a sum

$$a = \sum_{1 \le i \le m} a_i s_i.$$

If T is a finitely-generated S-module, then there elements $t_1, \dots, t_n \in T$ such that any element $b \in T$ can be expressed as a sum

$$b = \sum_{1 \le j \le n}^{n} b_j t_j.$$

Now, we will show that the elements $s_i t_j$ (for $1 \le i \le m$ and $1 \le j \le n$) generate T as an R-module.

Indeed, let b be any element of T. We can write

$$b = \sum_{1 \le j \le n} b_j t_j = \sum_{1 \le j \le n} \sum_{1 \le i \le m} (a_{ij} s_i) t_j = \sum_{\substack{1 \le i \le m \\ 1 \le j \le n}} a_{ij}(s_i t_j),$$

for some elements $b_j \in S$ and $a_{ij} \in R$, exactly as needed. □

Now we introduce a definition, extremely useful in algebraic number theory and algebraic geometry alike:

Definition 5.2. *Let S be an R-algebra. An element $x \in S$ is said to be* integral over R *if it satisfies a monic polynomial equation*

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0,$$

where $a_{n-1}, \dots, a_0 \in R$.

Date: March 10, 2016.

Formally, what we really mean by that, of course, is that there are elements $a_{n-1}, \dots, a_0$ of R such that

$$x^n + f(a_{n-1})x^{n-1} + \cdots + f(a_0) = 0,$$

where $f : R \to S$ is the structure map of the S-algebra R. But it's commonplace to not mention the structure map, and I'll usually avoid doing so from now on.

Here are some examples and nonexamples.

Example 5.3. *Given a commutative ring homomorphism $f : R \to S$, any element $r \in R$ is integral over R, because it is a root of the equation $x - r = 0$.*

Exercise 5.4. *The element $1/2 \in \mathbb{Q}$ is not integral over $\mathbb{Z}$.*

Example 5.5. *The element $\sqrt{17} \in \mathbb{R}$ is integral over $\mathbb{Z}$, for example, because it satisfies $x^2 - 17 = 0$.*

Example 5.6. *The golden ratio $\frac{1+\sqrt{5}}{2}$ is integral over $\mathbb{Z}$, because it satisfies $x^2 - x - 1 = 0$.*

Example 5.7. *Any element of $\mathbb{C}$ is integral over $\mathbb{R}$. Indeed, if $x = a + ib$, then $(x - a)^2 = -b^2$ and hence $x^2 - 2ax + a^2 + b^2 = 0$.*

Now we'll see what this has to do with things we were talking about earlier:

Theorem 5.8. *Let S be an R-algebra. The following are equivalent:*

(i) *S is a finitely-generated R-module;*
(ii) *S is generated as an R-algebra by integral elements $x_1, \dots, x_n$;*
(iii) *S is a finitely-generated R-algebra, and every element of S is integral over R.*

Proof. The implication (iii) $\Rightarrow$ (ii) is obvious. We'll prove (ii) $\Rightarrow$ (i) and then (i) $\Rightarrow$ (iii).

In order to prove (ii) $\Rightarrow$ (i), suppose that S is generated as an R-algebra by $x_1, \dots, x_n$ which are roots of monic polynomials of degrees $d_1, \dots, d_n$ respectively.

Then S is generated as an R-module by the monomials $x_1^{a_1} \cdots x_n^{a_n}$. But in fact we don't need the monomials where $a_i \geq d_i$ for any i, since we can use integrality to rewrite these. This means we have a finite set of generators.

Now we must prove (i) $\Rightarrow$ (iii). Note firstly that if S is a finitely-generated R-module then it's certainly a finitely-generated R-algebra: the module generators generate it as an algebra.

Let $x_1, \dots, x_n$ generate S as an R-module, and let s be any element of S; we must show s is a root of a monic polynomial with coefficients in R.

We now employ the Cayley-Hamilton Theorem from last week, taking $I = R$ so that $IM = M$, and $\phi : M \to M$ to be $m \mapsto sm$. This gives us the monic polynomial we want, with coefficients in R. □

Definition 5.9. *We say that an R-algebra satisfying the conditions of Theorem 5.8 is an* integral extension.

Corollary 5.10. *Let R be a commutative ring, and S an R-algebra. Then sums and products of elements which are integral over R are integral over R.*

Proof. Suppose given two elements $x, y \in S$ which are integral over R. Then consider the subalgebra $T \subset S$ generated as an R-algebra by x and y.

Since it's generated by integral elements x and y, by Theorem 5.8 all its elements are integral over R, but this includes $x + y$ and xy. □

Corollary 5.11. *Let R be a commutative ring, and S an R-algebra. Then the set of integral elements forms a subalgebra of S.*

Proof. This is obvious from Example 5.3 and Corollary 5.10 above. □

We now investigate how integral extensions behave with respect to taking quotient rings. Let $R \xrightarrow{f} S$ be an algebra, and $I \subset R$ be an ideal. In this case the image of $f(I)$ does not have to be an ideal: $f(I) \subset S$ is an abelian subgroup but there is no reason for $f(I)$ to be closed under S-multiplication. For example, if we consider the inclusion homomorphism $\mathbb{Z} \to \mathbb{Q}$, then the image of the ideal (2), that is the set of all even integers, is not an ideal in $\mathbb{Q}$.

The right thing to do is to consider the ideal generated by $f(I)$ in S: $IS = f(I)S$. This consists of sums of elements of the form $i \cdot s$, $i \in I$, $s \in S$.

In other words, IS is the smallest ideal in S which contains $f(I)$.

In this setting we can pass to the quotient rings R/I and S/IS and obtain a homomorphism between them as follows. The homomorphism $R \to S$ defines a composition $R \to S \to S/IS$ which factors to give a ring homomorphism $R/I \to S/IS$ via the rule:

$$r + I \mapsto f(r) + IS,$$

This is well-defined since $f(i) = i \cdot 1 \in IS$.

Lemma 5.12. *If $R \xrightarrow{f} S$ is an integral extension, and $I \subset R$ is an ideal, then the extension $R/I \to S/IS$ is integral.*

Proof. To check that the extension $R/I \to S/IS$ is integral we need to show that S/IS is finitely generated as R/I-module. But this is clear: if $s_1, \ldots, s_r \in S$ generate S as R-module, then the images $s_1 + IS, \ldots, s_r + IS$ generate S/IS, as R-module as well as an R/I-module. □

5.2. **Finite maps of algebraic sets.**

Definition 5.13. *We call a polynomial map of algebraic sets $X \to Y$ finite if the ring homomorphism $k[Y] \to k[X]$ is an integral extension.*

Recall that integral extension simply means that $k[X]$ is a finitely generated $k[Y]$-module. In practice to check that a map is finite we rely on Theorem 5.8: it is sufficient to verify that the $k[Y]$-algebra $k[X]$ is generated by integral elements.

Example 5.14. *Let $\phi : \mathbb{A}^1 \to \mathbb{A}^1$ be a polynomial map defined by $\phi(t) = t^2$. We check that ϕ is a finite map by considering the coordinate rings. Both coordinate rings are $k[t]$, but it will be less confusing if denote the coordinate on the source $\mathbb{A}^1$ by t, and on the target $\mathbb{A}^1$ by u. Then the the map of coordinate rings is:*

$$f : k[u] \to k[t]$$
$$p(u) \mapsto p(\phi(t)) = p(t^2).$$

By considering the top degree term of p we see that f is injective. The image of f consists of polynomials in t^2:

$$\mathrm{Im}(f) = k[t^2] \subset k[t].$$

Hence we are talking about an extension $k[t^2] \subset k[t]$. The key point is that the generator t is integral as it satisfies a monic equation

$$x^2 - t^2 = 0$$

with coefficients in $k[t^2]$. By Theorem 5.8 the above extension is integral, hence the map of algebraic sets ϕ is finite.

Theorem 5.15. *Every finite map $\phi : X \to Y$ has finite fibers, that is for every $y \in Y$ the set $\phi^{-1}(y) = \{x \in X : \phi(x) = y\} \subset X$ is finite.*

Proof. The proof consists of three steps.

Step 1: In this step we identify the fibers algebraically. For every y we construct a ring R^y such that points in $\phi^{-1}(y)$ correspond to maximal ideals in R^y.

For every point $y \in Y$ denote by $m_y \subset k[Y]$ the maximal ideal of functions which vanish at y. Note that by the First Isomorphism Theorem we have $k[Y]/m_y \simeq k$. Similarly, if $x \in X$ we have the corresponding ideal $m_x \subset k[X]$.

We need to translate the condition $\phi(y) = x$ into algebraic language:

Lemma 5.16. *Let $\phi : X \to Y$ be a polynomial map of algebraic sets, let $x \in X$, $y \in Y$ be points, and let $m_x \subset k[X]$, $m_y \subset k[Y]$ the corresponding maximal ideals. Let $f : k[Y] \to k[X]$ be the k-algebra homomorphism corresponding to ϕ. Then we have*

$$\phi(x) = y \iff m_x \supset m_y k[X].$$

Recall that the ideal $m_y k[X]$ is the same thing as $f(m_y)k[X]$: the smallest ideal of $k[X]$ which contains $f(m_y)$.

Proof of the Lemma. Recall how $f : k[Y] \to k[X]$ is constructed from $\phi : X \to Y$: if $h \in k[Y]$ is a polynomial function, then $f(h) = h \circ \phi \in k[X]$, that is $f(h)(x) = h(\phi(x))$.

If $\phi(x) = y$, then for every $h \in k[X]$ if $h \in m_y$, then $f(h) = h \circ \phi \in m_x$, since $f(h)(x) = h(\phi(x)) = h(y) = 0$. This shows that $f(m_y) \subset m_x$, and since m_x is an ideal, this implies that $f(m_y)k[Y] \subset m_x$.

Now if $\phi(x) = y' \neq y$, then we can find a function $h \in k[Y]$ such that $h(y) = 0$, $h(y') \neq 0$. In this case $f(h) \notin m_x$ since $f(h)(x) = h(\phi(x)) = h(y') \neq 0$. Thus $f(m_y)k[X] \not\subset m_x$. □

We continue proving the Theorem. From the Lemma it follows that points in $\phi^{-1}(y)$ are in bijection with maximal ideals in the ring $R^y := k[X]/(m_y k[Y])$.

Step 2: In this step we show that R^y is an Artinian ring for every $y \in Y$. Since the extension $k[Y] \to k[X]$ is integral, by Lemma 5.12, for every $y \in Y$ the extension

$$k[Y]/m_y \to k[X]/(m_y k[X]) = R^y.$$

is integral. On the other hand $k[Y]/m_y$ is isomorphic to k, thus R^y is an integral extension of k, i.e. a finite-dimensional as k-vector space. We deduce that R^y is an Artinian k-module, hence an Artinian ring.

Step 3: In this final step we show that fibers of ϕ are finite. Assume that there are infinitely many points $x_1, x_2, \ldots$ in X contained in a fiber $\phi^{-1}(y)$. For every n consider an ideal $I_n = I(\{x_1, x_2, \ldots, x_n\}) \subset k[X]$ of functions vanishing at the n points. This is a strictly decreasing chain:

$$I_1 \supset I_2 \supset \ldots$$

Since by assumption all the points x_j are contained in the fiber $\phi^{-1}(y)$, every one of the ideals I_n contains the ideal $m_y k[X]$ (like in Step 1). This yields an infinite strictly descending chain of ideals in $k[X]/(m_y k[X]) = R^y$:

$$\overline{I_1} \supset \overline{I_2} \supset \ldots$$

contradicting to the fact that R^y is Artinian. This shows that all fibers are in fact finite. □

Example 5.17. *Let us compute the fibers of the finite polynomial map $\phi(t) = t^2$ from Example 5.14. For every $a \in \mathbb{A}^1$ the fiber is*

$$\phi^{-1}(a) = \begin{cases} \{\pm\sqrt{a}\}, & a \neq 0 \\ \{0\}, & a = 0 \end{cases}$$

which are evidently finite sets. To demonstrate the proof of Theorem 5.15 we consider the rings R^a, $a \in \mathbb{A}^1$:

$$R^a = k[X]/(m_y k[X]) = k[t]/(t-a) = k[u]/(t^2-a).$$

Maximal ideals in $k[t]/(u^2-a)$ correspond to maximal ideals in $k[t]$ that contain t^2-a, i.e. divisors of the polynomial $t^2 - a = (t-\sqrt{a})(t+\sqrt{a})$.

If $a = 0$, then we have $k[t]/(t^2)$, which is a local ring with the maximal ideal $(\bar{t})$ corresponding to $0 \in \phi^{-1}(0)$. If $a \neq 0$, then there are two maximal ideals $(\bar{t}-\sqrt{a}), (\bar{t}+\sqrt{a}) \subset k[t]/(t^2-a)$, corresponding to the two elements $\pm\sqrt{a} \in \phi^{-1}(a)$.

Remark 5.18. *One can prove that any finite map $\phi : X \to Y$ is surjective. Thus finite maps are analogous to finite coverings in topology, the difference is that so-called ramification is allowed: some points have fewer preimages than a general point. In the Example 5.14 all fibers have two preimages except for the fiber over $0 \in \mathbb{A}^1$ which has one.*