MA 3G6 COMMUTATIVE ALGEBRA: INTEGRAL CLOSURE

DIANE MACLAGAN

These notes cover, in a slightly different order, the content of the material on integral closure. They were prepared for a previous year's module. They mostly follow Reid, Chapter 4. Let me know of any typos you notice, no matter how trivial.

Definition 1. Let R be a ring. A ring S is an R-algebra if there is a homomorphism $\phi\colon R \to S$. This makes S into an R-module: for $r \in R$ and $s \in S$ we set $rs = \phi(r)s$. In most applications we can replace R by $\phi(R)$, so can assume that $R \subset S$. We say that an R-algebra S is finite over R if S is a finitely generated R-module.

Example 2. Let $R = \mathbb{Q}$ and $S = \mathbb{Q}(\sqrt{3})$. Then S is finite over R.

Definition 3. Let R be a ring, and let S be an R-algebra. An element $s \in S$ is *integral* over R if there is an monic polynomial $f(y) = y^n + a_1y^{n-1} + \cdots + a_n \in R[y]$ with $f(s) = 0$. If every element of S is integral over R, then we say S is integral over R.

This usage of the word "integral" is unrelated to the "integral" in "integral domain". Avoiding confusion between these two concepts is one of our motivations for using "domain" instead of "integral domain" in commutative algebra.

Example 4.
(1) Let $S = \mathbb{Z}[(1+\sqrt{5})/2]$. Then $\phi = (1+\sqrt{5})/2$ is integral over $\mathbb{Z}$, as $\phi^2 - \phi - 1 = 0$, so ϕ satisfies a monic equation with coefficients in $\mathbb{Z}$. It will follow from the theorem below that S is integral over $\mathbb{Z}$.
(2) Let $S = \mathbb{Z}[(1+\sqrt{3})/2]$. Then S is not integral over $\mathbb{Z}$ because $(1+\sqrt{3})/2$ does not satisfy any monic polynomial with coefficients in $\mathbb{Z}$ (why?!)

Exercise 5.
(1) Show that $\mathbb{C}[x]$ is integral over $\mathbb{C}[x^2]$.
(2) Show that $\mathbb{Z}[1/3]$ is not integral over $\mathbb{Z}$.
(3) Let $R = K[x]$, when K is a field, and let $f \in R$. Let $U = \{f^i : i \geq 0\}$. When is $R[U^{-1}]$ integral over R?

If R is a ring, S is a ring containing R, and $s_1, \ldots, s_m$ are elements of S, then by $R[s_1, \ldots, s_m]$ we mean the smallest subring of S containing R and $s_1, \ldots, s_m$.

Exercise 6. Show that every element of $R[s_1, \ldots, s_m]$ can be written as a polynomial in the s_i with coefficients in R, and this subring contains all such polynomials.

The following proposition uses our corollary to the Cayley-Hamilton theorem to give a relationship between an extension ring being finite and being integral.

Proposition 7. *Let S be an R-algebra, with $R \subset S$. Fix $s \in S$. The following are equivalent:*

1. *s is integral over R;*
2. *The subring $R[s] \subset S$ is finite over R;*
3. *There is an R-subalgebra $R' \subset S$ such that $R[s] \subset R'$ and R' is finite over R.*

Proof.

$1 \implies 2$ If s satisfies a relation $s^n + a_1 s^{n-1} + \cdots + a_n = 0$ with $a_i \in R$, then $R[s]$ is generated by $1, s, s^2, \ldots, s^{n-1}$. Indeed, if $f \in R[s]$ is a polynomial in s of degree at least n, then we can use this relation to lower the degree of the polynomial by one. This shows that every element of $R[s]$ can be written as an R-linear combination of $1, s, \ldots, s^{n-1}$, so $R[s]$ is a finitely generated R-module.

$2 \implies 3$ We can take $R' = R[s]$.

$3 \implies 1$ Consider the R-module homomorphism $\phi\colon R' \to R'$ given by $\phi(r') = sr'$. Since R' is a finitely generated R-module, *phi* satisfies a relation of the form $\phi^n + a_1\phi^{n-1} + \cdots + a_n = 0$ (this follows from the corollary to the Cayley-Hamilton theorem applied to the ideal $I = \langle 1 \rangle = R$). Applying this to 1_R, we get $s^n + a_1 s^{n-1} + \cdots + a_n = 0$, so s is integral over R as required.

□

Theorem 8. *Let S be an R-algebra, with $R \subset S$.*

1. *Let S' be a ring containing S such that S' finite over S. If S is an R-algebra that is finite over R, then S' is finite over R.*
2. *If $s_1, \ldots, s_m \in S$ are integral over R, then $R[s_1, \ldots, s_m]$ is finite over R, and thus every $f \in R[s_1, \ldots, s_m]$ is integral over R.*
3. *If $R \subset S \subset S'$, S' is integral over S, and S is integral over R, then S' is integral over R.*

(4) *The subset* $\tilde{R} = \{s \in S : s \text{ is integral over} R\} \subset S$ *is a subring of* S*. If* $s \in S$ *is integral over* $\tilde{R}$*, then* $s \in \tilde{R}$ *(so* $\tilde{\tilde{R}} = \tilde{R}$*).*

Proof. (1) If $s_1, \ldots, s_m$ generate S as an R-module, and $s'_1, \ldots, s'_n$ generate S' as an S-module, then $\{s'_i s_j : 1 \leq i \leq m, 1 \leq j \leq n\}$ generate S' as an R-module. Indeed, if $s \in S'$, then $s = \sum_{i=1}^n a_i s'_i$ for $a_i \in S$. We can write $a_i = \sum_{j=1}^m r_{ij} s_j$ for some $r_{ij} \in R$, so $s = \sum_{i=1}^n a_i s'_i = \sum_{i=1}^n (\sum_{j=1}^m r_{ij} s_j) s'_i = \sum_{i=1}^n \sum_{j=1}^m r_{ij}(s'_i s_j)$.

(2) The proof is by induction on m. The base case is $m = 1$, when Proposition 7 implies that $R[s_1]$ is finite over R. The induction step uses the previous part, since $R[s_1, \ldots, s_m] = R[s_1, \ldots, s_{m-1}][s_m]$. This shows that $R[s_1, \ldots, s_m]$ is finite over R. Thus any $f \in R[s_1, \ldots, s_m]$ satisfies the hypotheses of part 3 of Proposition 7, and so is integral over R.

(3) Let $s' \in S'$. Then s' satisfies a relation $s'^n + b_1 s'^{n-1} + \cdots + b_n = 0$, where all the b_i are integral over R. Thus $R[b_1, \ldots, b_n]$ is finite over R, and $R[b_1, \ldots, b_n, s']$ is finite over $R[b_1, \ldots, b_n]$, so $R[b_1, \ldots, b_n, s']$ is finite over R by the first part. Thus s' satisfies the hypotheses of part 3 of Proposition 7, and so is integral over R. Since s' was arbitrary, S' is integral over R.

(4) For the first part we need to show that $\tilde{R}$ is closed under inverses, addition and multiplication. Consider $s_1, s_2 \in \tilde{R}$. Then s_1, s_2 are integral over R, so $R[s_1, s_2]$ is finite over R, and thus by the second part $-s_1$, $s_1 + s_2$ and $s_1 s_2$ are integral over R. The second part follows from the previous part of the proposition. □

Exercise 9. We have $\sqrt{2}$ and $\sqrt{3}$ both integral over $\mathbb{Z}$. Show directly that $\sqrt{2}+\sqrt{3}$ is integral over $\mathbb{Z}$ by giving the monic equation it satisfies. Repeat this with 2 and 3 replaced by your favourite smallish positive squarefree integers, and square roots replaced by larger roots. Note how much easier (thanks to the corollary of the Cayley-Hamilton theorem!) the proof of the last part of the theorem was than your computations.

Definition 10. Let R, S be rings with $R \subset S$. The subring $\tilde{R} = \{s \in S : s \text{ is integral over} R\}$ of S is the *integral closure* of R in S. If $\tilde{R} = R$, then R is *integrally closed in* S. If R is a domain, and R is integrally closed in its field of fractions, then we say that R is integrally closed, or *normal*.

Example 11. (1) Consider $\mathbb{Z} \subset \mathbb{Q}(\sqrt{3})$. Then the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{3})$ is $\mathbb{Z}[\sqrt{3}]$.

(2) The subring $\mathbb{Z}[\sqrt{5}]$ is not integrally closed in $\mathbb{Q}(\sqrt{5})$, because $(1+\sqrt{5})/2$ is integral over $\mathbb{Z}$, and thus over $\mathbb{Z}[\sqrt{5}]$. Thus $\mathbb{Z}[\sqrt{5}]$ is not normal.

Definition 12. A *number field* is a finite field extension of $\mathbb{Q}$ (i.e., a field K containing $\mathbb{Q}$ that is a finite $\mathbb{Q}$-module. The *ring of integers* O_K of a number field K is the integral closure of $\mathbb{Z}$ in K. This is a fundamental object in algebraic number theory.

Exercise 13. Let n be a squarefree integer (no divisible by m^2 for any integer m), and let $K = \mathbb{Q}(\sqrt{n})$. Let $\alpha = (1+\sqrt{n})/2$ if $n \equiv 1 \mod 4$, and $\alpha = \sqrt{n}$ if $n \equiv 2$ or $3 \mod 4$ (the case $n \equiv 0 \mod 4$ is ruled out by the squarefree hypothesis). Show that the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{n})$ is $\mathbb{Z}[\alpha]$.