Worksheet: Integral Extensions

Here, S is an R-algebra via a ring map $R \to S$, where R and S are commutative with unity.

Definition. We call an R-algebra S a *finitely generated* R-algebra (or *algebra finite*) if there exist finitely many $s_1, \ldots, s_n \in S$ such that any element of S can be written as a polynomial in the s_i with coefficients in R.

Definition. An R-algebra S is *module finite* over R if S is finitely generated as an R-module.

Definition. An element s of an R-algebra S is *integral* over R if s satisfies a monic polynomial with coefficients in R. We call S an *integral* R-algebra if every element of S is integral over R.

1. **Warm-up.**
   (a) Which is a stronger condition, algebra finite or module finite? Justify your answer.
   (b) Determine, for each algebra below, which of the following properties is satisfied:

   module finite, *algebra finite*, and *integral*.

   i. The $\mathbb{Z}$-algebra of Gaussian integers $\mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z}\}$.
   ii. The $\mathbb{Q}$-algebra $\mathbb{C}$.
   iii. The $\mathbb{R}$-algebra $\mathbb{C}$.
   iv. The $\mathbb{Z}$-algebra $\mathbb{Z}[\{\sqrt{n} : n \in \mathbb{N}\}]$.
   Hint: You can use the theorem stated below for the question of integrality, since you will prove it later on in this worksheet. To address the question of algebra finiteness, suppose that $\mathbb{Z}[\{\sqrt{n} : n \in \mathbb{N}\}]$ is algebra finite over $\mathbb{Z}$. Is there a finite set of algebra generators of the form $\sqrt{p_1}, \ldots, \sqrt{p_k}$, for primes p_i? If so, and p is distinct from the p_i, then $\sqrt{p} \notin \mathbb{Z}[\sqrt{p_1}, \ldots, \sqrt{p_k}] \subseteq \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_k})$. The following lemma might be useful in understanding whether this is possible: If $nn_1 \cdots n_k$ is squarefree, where $n, n_i \in \mathbb{N}$, then $\sqrt{n} \notin \mathbb{Q}(\sqrt{n_1}, \ldots, \sqrt{n_k})$.
   v. The quotient R/I via the natural surjection $R \to R/I$, where I is an ideal of R.
   vi. The inclusion $\mathbb{C}[x] \subseteq \mathbb{C}[x, y]$.
   vii. The localization map $\mathbb{R}[x] \to \mathbb{R}[x]_x := \mathcal{W}^{-1}\mathbb{R}[x]$, with $\mathcal{W} = \{1, x, x^2, \ldots\}$.

Theorem. *An R-algebra is module finite if and only if it is both finitely generated (as an R-algebra) and integral.*

2. **One half of the theorem.** After replacing R with its image in S, convince yourself that in proving the theorem above, we can assume that $R \subseteq S$.
   (a) Prove that an element $s \in S$ is integral over R if and only if $R[s]$–the smallest subring of S containing R and s, or equivalently, the subset of S consisting of all polynomial expressions in s with coefficients in R–is module finite over R.
   (b) Prove that if S is integral and algebra finite over R, then S is module finite over R.

3. **A bit of linear algebra over rings.** Recall that for a positive integer n,

$$R^n = R \oplus R \cdots \oplus R.$$

As when R is a field, we can regard R^n as the set of all column vectors of length n with entries in R. Columns are added componentwise, and the product of an element of R times a column is likewise given by componentwise multiplication.

(a) Explain how an $m \times n$ matrix with entries in R determines an R-linear map $R^n \to R^m$. Furthermore, explain why an arbitrary R-linear map $\phi : R^n \to R^m$ must be given by multiplication by a matrix. How do you describe this matrix in terms of ϕ? To make sure that that this is completely clear, describe the matrix associated to the $\mathbb{Z}[x]$-linear map

$$\mathbb{Z}[x] \oplus \mathbb{Z}[x] \to \mathbb{Z}[x] \oplus \mathbb{Z}[x]$$

given by $(f, g) \mapsto (fx + g, -f + x^2 g)$.

(b) Convince yourself that matrix multiplication makes sense for matrices with entries in R. Similarly, convince yourself that determinants make sense for square matrices with entries in R. Now, suppose that $\phi : R \to S$ is a *ring map*, and given a matrix M with entries in R, let $\phi(M)$ be the matrix with entries in S obtained by applying ϕ component-wise to R. Verify that if M, N are matrices over R whose dimensions are such that the product MN is defined, then $\phi(MN) = \phi(M)\phi(N)$. Similarly, verify that if M is a square matrix over R, then $\det(\phi(M)) = \phi(\det(M))$.

4. **The determinant trick.** Let M be a square matrix over R. As in the case when R is a field, let $\operatorname{adj}(M)$ be the matrix whose (i, j)-th entry is $(-1)^{i+j} \det(M_{ji})$, where M_{ij} is the square matrix obtained from M by omitting its i-th row and j-th column. In other words, $\operatorname{adj}(M)$ is the transpose of the matrix of cofactors of M. Our goal is to prove that

$$M \operatorname{adj}(M) = \operatorname{adj}(M) M = \det(M)\, I \qquad (\heartsuit)$$

where I is the identity matrix of the appropriate size. Note that in this equation, on the left-hand side we are taking multiplication of matrices, while on the right-hand side we are multiplying I by the "scalar" $\det(M) \in R$.

(a) Remind yourself that ($\heartsuit$) holds whenever R is a field. If this fact isn't familiar to you from a linear algebra class, go ahead and prove it–it isn't very hard if you remember how to compute a determinant over a field by expanding across a row or column. If you prove this statement, notice that the proof works over any ring, and skip the remaining parts of this problem. If you decide not to prove it, explain why the fact that ($\heartsuit$) holds for R a field implies that it holds whenever R is a domain, and continue to part (b).

Hint: Every domain sits inside of its fraction field.

(b) Explain why, if ($\heartsuit$) holds for every square matrix over R, and if there exists a surjective *ring map* $\phi : R \to S$, then ($\heartsuit$) also holds for every square matrix over the target ring S.

Hint: Use a result from Problem 1.

(c) Conclude that ($\heartsuit$) is always valid, regardless of the ring R.

Hint: Construct a surjective *ring map* $\theta : D \to R$ with D a domain. This can be done many ways, e.g., with D a polynomial ring over $\mathbb{Z}$ (you may need infinitely many variables).

5. **The other half of the theorem.** Suppose $R \subseteq S$ is an inclusion of rings, and that S is module finite over R. From the Warm-up, we know that S is algebra finite over R, so it remains to prove that S is integral over R. As S is module finite over R, we can fix a set of generators $s_1, \ldots, s_n$ for S as an R-module, and we may as well include 1 in this set, so assume that $s_1 = 1$.

   (a) Multiply each of the generators s_i by s to obtain the element $ss_i \in S$. Explain why there exists elements $a_{ij} \in R$ such that
   $$ss_i = \sum_{j=1}^{n} a_{ij} s_j$$
   for each $i = 1, \ldots, n$. Then, use the elements $a_{ij} \in R$ to define a matrix M with coefficients in R, and so with coefficients in S. Explain why we can rewrite the above system of equations as a single matrix equation over S
   $$sI\mathbf{v} = M\mathbf{v}$$
   where $\mathbf{v} = (s_1, \cdots, s_n)$ and I is the $n \times n$ identity matrix.

   (b) Rewrite this matrix equation in the form $(M - sI)\mathbf{v} = \mathbf{0}$, and use this to prove that as an element of S, $\det(M - sI) = 0$.
   Hint: Multiply by $\mathrm{adj}(M - sI)$, and remember that one of your generators equals 1.

   (c) Conclude that the element $s \in S$ that we fixed satisfies a monic polynomial with coefficients in R. In other words, you have just proved that S is integral over R.

   (d) This process might seem a little abstract, so work through the case that $R = \mathbb{Z}$ and $S = \mathbb{Z}[i]$ and $s = a + ib$ to construct a monic polynomial over $R = \mathbb{Z}$ satisfied by s.

   Lemma. *Let $R \to S \to T$ be ring homomorphisms, under which S is module finite over R with generators $s_1, \ldots, s_m$, and T is module finite over S with generators $t_1, \ldots, t_n$. Then via composition $R \to T$, T is module finite over R with the mn generators $s_i t_j$, $1 \leq i \leq m$, $1 \leq j \leq n$.*

   Theorem. *If S is an R-algebra, then the elements of S integral over R form a subring of S.*

6. **Integral elements form a subring.** First notice that to prove the above theorem, we can again assume $R \subseteq S$.

   (a) Let s, s' be elements of S integral over R. Explain why $R[s]$ is module finite over R, and s' is integral over $R[s]$.

   (b) Explain why (a) implies that $(R[s])[s'] = R[s, s']$ is module finite over $R[s]$.

   (c) Prove the above lemma.

   (d) Use your work so far to conclude that $(R[s])[s'] = R[s, s']$ is module finite over R, so that $s \pm s'$ and ss', which are in $R[s, s']$, are integral over R.

   (e) Which subsets of $\{\text{module finite}, \text{algebra finite}, \text{integral}\}$ are possible for an R-algebra S?
   Hint: You might want to return to the Warm-up, armed with your more powerful theroem(s)!