CLASS 14, MARCH 8TH: INTEGRAL RING EXTENSIONS

Today we will shift toward a study of containments of rings $R \subseteq S$. As with all of our objects so far, a notion of finiteness is important and useful for actually acquiring results. Our notion of interest in turns out will be exactly the one that defines algebraic extensions.

Definition 14.1. If R is a ring, A is called an R**-algebra** if A is itself a ring and there exists a ring homomorphism $R \to A$.

A is a **finite** R-algebra if it is a finitely generated R-module.

$a \in A$ is said to be **integral over** R if there exists a monic polynomial $p(x) \in R[x]$ such that

$$p(a) = a^n + r_1 a^{n-1} + \ldots + r_{n-1}a + r_n = 0$$

A is said to be **integral** over R if every element is integral.

Note that for an R-algebra A, we can consider the image of R under the homomorphism. Call it R'. Then we are merely considering $R' \subseteq A$, which is an extension of rings.

Example 14.2.

- $\mathbb{Z}[\frac{1}{m}]$ is not integral over $\mathbb{Z}$ for $m > 1$. We can check this easily by noting
$$\frac{1}{m^n} + a_1\frac{1}{m^{n-1}} + \ldots + a_n = \frac{1 + m(a_1 + \ldots + m^{n-1}a_n)}{m^n}$$
The numerator of this fraction is $\equiv 1 \pmod m$, therefore can not be 0. This procedure generalizes to R any UFD, with algebra $A = R[f]$ where $f \in Frac(R) \setminus R$.
- $K[x^n] \subseteq K[x]$ is an integral extension.
- $\mathbb{Z} \subseteq \mathbb{Z}[\tau]$, where $\tau = \frac{1+\sqrt{5}}{2}$ is the golden ratio. Then τ satisfies $\tau^2 - \tau - 1 = 0$. Therefore τ is an integral element. On the otherhand, if $\tau = \frac{1+\sqrt{3}}{2}$, then τ satisfies $\tau^2 - \tau - \frac{1}{2}$. This makes it non-integral upon further inspection.
- $\mathbb{Q} \subseteq \bar{\mathbb{Q}}$ is an example of an integral extension which is not finite.

Now we will work through a comparison of the integral and finite extensions. This is typically realized through the following proposition:

Proposition 14.3. *If A is an R-algebra, and $a \in A$, then TFAE:*

(a) *a is integral over R.*
(b) *The subring $R'[a]$ is a finite R'-algebra.*
(c) *There exists $B \subseteq A$ an R'-subalgebra containing a such that B is a finite R'-algebra.*

Proof. $(a) \Rightarrow (b)$: Note $R'[a]$ is generated as an R'-module by $1, a, a^2, \ldots$. a being integral ensures that

$$a^n + r_1 a^{n-1} + \ldots + r_n = 0$$

which is to say $a^n \in \langle 1, a, \ldots, a^{n-1}\rangle$. This implies that $a^m \in \langle 1, a, \ldots, a^{n-1}\rangle$ for all $m \geq n$. As a result,,

$$R'[a] = \langle 1, a, \ldots, a^{n-1}\rangle$$

$(b) \Rightarrow (c)$: Let $B = R'[a]$.

$(c) \Rightarrow (a)$: Consider $B \xrightarrow{\cdot a} B$. Note that this is an R-module homomorphism. Since B is assumed finite as an R- (or R'-)module. By the determinant trick, we get a relation of the form

$$(\cdot a)^n + r_1(\cdot a)^{n-1} + \ldots + r_{n-1}(\cdot a) + r_n$$

Applying this function to $1 \in B$, we get the desired relation on a. $\square$

Next up, we see a set of so-called 'tower laws'. These regard how these properties hold up under 2 (or a finite number of) successive extensions.

Proposition 14.4.
(a) *If $A \subseteq B \subseteq C$ are extensions of rings, and C over B is a finite extension, and B over A is a finite extension, then C over A is a finite extension.*
(b) *If $A \subseteq B \subseteq C$ are extensions of rings, and C over B is an integral extension, and B over A is an integral extension, then C over A is an integral extension.*
(c) *If A is an R-algebra, and $a_1, \ldots, a_n$ are integral over R, then $R[a_1, \ldots, a_n]$ is a finite R-algebra.*
(d) *The subset $\tilde{R} \subseteq A$ given by*

$$\tilde{R} = \{a \in A \mid a \text{ is integral over } R\}$$

forms a subring of A. If $a \in A$ is integral over $\tilde{R}$, then it is integral over R, thus in $\tilde{R}$.

Proof. (a): Let $B = \langle b_1, \ldots, b_n \rangle$ as an A-module, and $C = \langle c_1, \ldots, c_m \rangle$ as a B-module. Then for $c \in C$,

$$c = \sum_{j=1}^{m} b_j c_j$$

for some $b_j \in B$. As a result, we can conclude that $b_j = \sum_{i=1}^{n} a_{ij} b_i$ for $a_{ij} \in A$. Thus

$$c = \sum_{j=1}^{m} \left(\sum_{i=1}^{n} a_{ij} b_i \right) c_j = \sum_{j=1}^{m} \sum_{i=1}^{n} a_{ij} (b_i c_j)$$

which is to say $b_i c_j$ form a finite generating set for C over A.

(c): This follows by induction using Proposition 14.3 (b).

(b): We can use (c) and (a) to show this. If $c^n + b_1 c^{n-1} + \ldots + b_n = 0$, then we note that this is a relation in $A[b_1, \ldots, b_n]$. As a result, we can conclude by (a) that

$$A[b_1, \ldots, b_n][c] = A[b_1, \ldots, b_n, c]$$

is a finite A algebra by (c). Therefore, c is integral over A by Proposition 14.3 (c), and thus C is integral over A.

(d): The claim that it is a subring follows by consideration of the finite algebra $R[\alpha, \beta]$ for $\alpha, \beta \in A$. Note in contains $\alpha + \beta$ and $\alpha \cdot \beta$. From (b) we acquire the second assertion. $\square$