DEFINITION: Let $\phi : A \to R$ be a ring homomorphism. We say that ϕ is **integral** or that R is **integral over** A if every element of R is integral over A.

THEOREM: A homomorphism $\phi : A \to R$ is module-finite if and only if it is algebra-finite and integral. In particular, every module-finite extension is integral.

COROLLARY 1: An algebra generated (as an algebra) by integral elements is integral.

COROLLARY 2: If $R \subseteq S$ is integral, and x is integral over S, then x is integral over R.

PROPOSITION: Let $R \subseteq S$ be an integral extension of domains. Then R is a field if and only if S is a field.

DEFINITION: Let A be a ring, and R be an A-algebra. The **integral closure** of A in R is the set of elements in R that are integral over A.

(1) Proof of Theorem:
- **(a)** Very briefly explain why, to prove that module-finite implies integral in general, it suffices to show the claim for an inclusion $A \subseteq R$.
- **(b)** Take a module generating set $\{1, r_2, \dots, r_n\}$ for R as an A-module, and write it as a row vector $v = \begin{bmatrix} 1 & r_2 & \cdots & r_n \end{bmatrix}$. Let $x \in R$. Explain why there is a matrix $M \in \mathrm{Mat}_{n\times n}(A)$ such that $vM = xv$.
- **(c)** Apply a TRICK to obtain a monic polynomial over A that x satisfies.
- **(d)** Combine the previous parts with results from last time to complete the proof of the Theorem.

- **(a)** You can replace A by $\phi(A)$ for both.
- **(b)** $xr_i \in R$ for each i, so each xr_i is an A-linear combination of $1, r_2, \dots, r_n$. We can write these linear combinations using matrix multiplication.
- **(c)** The eigenvector trick implies that $\det(M - x\mathbb{1}_n)$ kills v; since 1 is an entry of v, $\det(M - x\mathbb{1}_n) = 0$, so x is a root of the polynomial $\det(M - X\mathbb{1}_n) = 0$, which is monic.
- **(d)** The previous part shows that module-finite implies integral. We already saw that module-finite implies algebra-finite. Also, if $R = A[r_1, \dots, r_m]$ and R is integral over A, then each r_i is integral over R. We saw last time that R as above is module-finite over A.

(2) Let $R = \mathbb{C}[X, X^{1/2}, X^{1/3}, \dots] \subseteq \overline{\mathbb{C}(X)}$, where $X^{1/n}$ is an nth root of X. Is $\mathbb{C}[X] \subseteq R$ integral[1]? Is it module-finite? Is it algebra-finite?

Each algebra generator $X^{1/n}$ satisfies a polynomial $T^n - X = 0$, so is integral over $\mathbb{C}[X]$. By the Corollary, R is integral over $\mathbb{C}[X]$. It is not algebra-finite or module-finite. The argument is similar to examples we have done before: if it was, it would be generated by a finite subset of $\{X^{1/n}\}$, but there would then be a largest denominator on the powers of X.

(3) Proof of Corollary 1: Let R be an A-algebra.
- **(a)** If $x, y \in R$ are integral over A, explain why $A[x, y] \subseteq R$ is integral over A. Now explain why $x \pm y$ and xy are integral over A.

[1]You might find the Corollary helpful.

(b) Deduce that the integral closure of A in R is a ring, and moreover an A-subalgebra of R.
(c) Now let S be a set of integral elements. Apply (b) to the ring $R = A[S]$ in place of R. Complete the proof of the Corollary.

> **(a)** $A[x, y]$ is module-finite over A, and $x \pm y$ and $xy \in A[x, y]$.
> **(b)** This follows from (a) plus the fact that every element of A is obviously integral over A.
> **(c)** The integral closure of A in $A[S]$ is a subalgebra of A that contains S, so by definition of generators must be all of $A[S]$. Thus $A[S]$ is integral over A.

(4) Proof of Proposition:
  (a) First, assume that S is a field, and let $r \in R$ be nonzero. Explain why r has an inverse in S.
  (b) Take an integral equation for $r^{-1} \in S$ over R, and solve for r^{-1} in terms of things in R. Deduce that R must also be a field.
  (c) Now, assume that R is a field, and that S is a domain, and let $s \in S$ be nonzero. Explain why $R[s]$ is a finite-dimensional vector space.
  (d) Explain why the multiplication by s map from $R[s]$ to itself is surjective. Deduce that S must also be a field.

> (a) Because S is a field.
> (b) Take $(r^{-1})^n + r_1(r^{-1})^{n-1} + \cdots + r_n = 0$. Multiplying through, $r^{-1} = -r_1 - r_2 r - \cdots - r_n r^{n-1} \in R$.
> (c) $R[s]$ is module-finite over R; for a field, this means finite-dimensional.
> (d) Since s is nonzero, and S is a domain, multiplication by s is injective. But this is an R-linear map from $R[s]$ to itself, and since $R[s]$ is a finite-dimensional vector space, this is also surjective. That means that $1 = ss'$ for some s', so s is a unit. Thus, S is also a field.

(5) Prove Corollary 2.

> Let $R \subseteq S$ be integral and x be integral over S. Let $x^n + s_1 x^{n-1} + \cdots + s_n = 0$ with $s_i \in S$. Then x is integral over $R[s_1, \ldots, s_n]$, so $R[s_1, \ldots, s_n, x]$ is module-finite over $R[s_1, \ldots, s_n]$. But $R[s_1, \ldots, s_n]$ is module-finite over R, so $R[s_1, \ldots, s_n, x]$ is module-finite over R, and hence integral over R. In particular, x is integral over R.

(6) Let $A = \mathbb{C}[X, Y]$ be a polynomial ring, and $R = \dfrac{\mathbb{C}[X, Y, U, V]}{(U^2 - UX + 3X^3, V^2 - 7Y)}$. Find an equation of integral dependence for $U + V$ over A.