Rmk Module/ring/field-finiteness are transitive:

If S is a module/ring/field-finite ext. of R and T is a module/ring/field-finite ext. of S, then T is a module/ring/field-finite ext. of R.

$$\begin{tikzcd} T \arrow[d, dash, "\text{fin}"'] \arrow[dd, dash, dashed, bend left, "\Rightarrow \text{fin}"] \\ S \arrow[d, dash, "\text{fin}"'] \\ R \end{tikzcd}$$

Pf <u>module-finite:</u> S gen. by $a_1, \dots, a_n$ as R-mod

T gen. by $b_1, \dots, b_m$ as S-mod.

$\Rightarrow T$ gen. by $\left\{ a_i b_j \;\middle|\; \begin{matrix} 1 \le i \le n, \\ 1 \le j \le m \end{matrix} \right\}$ as R-mod.

<u>ring-finite:</u> $S = R[a_1, \dots, a_n]$

$T = S[b_1, \dots, b_m]$

$\Rightarrow T = R[a_1, \dots, a_n, b_1, \dots, b_m]$.

<u>field-finite:</u> same ... $\square$

2.6. Integral and algebraic extensions

<u>Def</u> An element a of a ring S is called <u>integral over</u> a subring $R \subseteq S$ if there is a <u>monic</u> polynomial $f(x) \in R[x]$ with $f(a) = 0$.
(leading coeff. $= 1$: $f(x) = x^n + c_{n-1}x^{n-1} + \dots + c_0$)

A ring extension S of R is <u>integral</u> if every $a \in S$ is integral over R.
The <u>integral closure</u> of a ring R in a ring extension S is the set of elements of S that are integral over R.
The ring R is called <u>integrally closed</u> in S if its integral closure in S is R.

<u>Def</u> If $R = K$ is a field, integral is also called <u>algebraic</u>. Numbers that aren't algebraic are transcendental (over K).

<u>Rmk</u> If $R = K$ is a field, one could allow any nonzero polynomial $f(x) \in K[x]$ (divide by the leading coefficient).

Rmk An algebraically closed field K has no algebraic field extensions $L \neq K$.

Ex Any element a of R is integral over R.

Pf Take $f(X) = X - a$. $\square$

Ex $\sqrt[3]{2} \in \mathbb{R}$ is algebraic over $\mathbb{Q}$ and integral over $\mathbb{Z}$.

Pf Take $f(X) = X^3 - 2$. $\square$

Ex $\mathbb{C}$ is an algebraic extension of $\mathbb{R}$.

Pf Let $a \in \mathbb{C}$. Take $f(X) = (X-a)(X-\bar{a})$

$$= X^2 - \underbrace{(a+\bar{a})}_{\in \mathbb{R}}X + \underbrace{a\bar{a}}_{\in \mathbb{R}}.$$

$\square$

Thm $\mathbb{C}$ is not an algebraic ext. of $\mathbb{Q}$.

Thm (Hermite) $\pi \in \mathbb{R}$ is transcendental over $\mathbb{Q}$.

Ex $T \in K(T)$ is transcendental over K for any field K.

Pf If $f(X) \in K[X]$ is a nonzero pol. then $f(T) \in K(T)$ is "the same" nonzero pol. $\square$

Rmk For the same reason, $T \in K[T]$ is not integral over K.

Thm 2.15 A unique factorization domain R (e.g. $R = \mathbb{Z}$, $K[X_1, \dots, X_n]$) is integrally closed in its field of fractions K.

Pf Assume $\frac{p}{q} \in K$ is integral ($p, q \in R$).

W.l.o.g. $\gcd(p, q) = 1$.

Let $f(X) = X^n + c_{n-1} X^{n-1} + \dots + c_0$ with $f\left(\frac{p}{q}\right) = 0$. $\quad (c_i \in R)$

$$\Rightarrow \left(\frac{p}{q}\right)^n + c_{n-1}\left(\frac{p}{q}\right)^{n-1} + \dots + c_0 = 0$$

$$\Rightarrow p^n = -\left(c_{n-1} p^{n-1} q + \dots + c_0 q^n\right)$$

RHS is divisible by q.

If q is divisible by some prime element $t \in R$, then p^n and therefore p is also divisible by t. $\Rightarrow p, q$ aren't coprime. $\lightning$

$\square$

Lemma 2.16 Let R be an integral domain with field of fractions K and let L be a field extension of K. Then, any element $a \in L$ that is algebraic over K can be written as $a = \frac{p}{q}$ with $p \in L$ integral over R and $0 \neq q \in R$.

Pf Let $f(X) \in K[X]$ be monic, and $f(a) = 0$.

$$f(X) = X^n + c_{n-1} X^{n-1} + \dots + c_0$$

$$\Rightarrow a^n + c_{n-1} a^{n-1} + \dots + c_0 = 0$$

Clear out denominators:

Pick $0 \neq q \in R$ such that $c_i q \in R$ $\forall i$.

$$\Rightarrow q^n a^n + q c_{n-1} q^{n-1} a^{n-1} + q^2 c_{n-2} q^{n-2} a^{n-2} + \dots + q^n c_0 = 0.$$

$$\Rightarrow (qa)^n + \underbrace{q c_{n-1}}_{\in R} (qa)^{n-1} + \dots + \underbrace{q^n c_0}_{\in R} = 0$$

$\Rightarrow p := qa \in L$ is integral over R. $\square$

Lemma 2.17 Let S be a ring extension of R and let $a \in S$. The following are equivalent:

i) a is integral over R.

ii) The ring extension $R(a)$ of R is module-finite.

iii) There is a ring ext. $a \in S' \subseteq S$ of R which is module-finite.

Pf ii) $\Rightarrow$ iii): clear

i) $\Rightarrow$ ii): Set $f(X) = X^n + c_{n-1}X^{n-1} + \dots + c_0 \in R(X)$ with $f(a) = 0$.

$$\Rightarrow a^n = -(c_{n-1}a^{n-1} + \dots + c_0). \quad (I)$$

Repeatedly applying (I), we can show that any a^e with $e \geq 0$ lies in the R-module generated by $1, a, \dots, a^{n-1}$: Assume a^e is the first counterexample. $\Rightarrow e \geq n$.

$$\underset{(I)}{\Rightarrow} a^e = -(c_{n-1}a^{n-1} + \dots + c_0)a^{e-n}$$

$$= -(c_{n-1}a^{e-1} + \dots + c_0 a^{e-n})$$

apply the induction hypothesis.

$\Rightarrow R[a]$ is gen. by $1, a, \dots, a^{n-1}$.

(Ese $\mathbb{Z}[\sqrt[3]{2}]$ is gen. by $1, \sqrt[3]{2}, \sqrt[3]{2}^2$ as a $\mathbb{Z}$-module.)

iii) $\Rightarrow$ i): Assume S' is generated by $b_1, \dots, b_n \in S'$ as an R-module. W.l.o.g. $1 \in b_1$.

Write $a b_i = r_{i1} b_1 + \dots + r_{in} b_n$ with $r_{ij} \in R$.

$$\Rightarrow \underbrace{\begin{pmatrix} r_{11} & \cdots & r_{1n} \\ \vdots & & \vdots \\ r_{n1} & \cdots & r_{nn} \end{pmatrix}}_{M} \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = a \cdot \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$$

$$\Rightarrow N \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = 0 \text{, where } N = a I_n - M$$

$n \times n$ identity matrix

Let $\tilde{N}$ be the adjugate matrise of N.

$$\Rightarrow \tilde{N} N = \det(N) \cdot I_n$$

$$\Rightarrow 0 = \tilde{N} N \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = \det(N) \cdot \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$$

$$= \det(N) \cdot \begin{pmatrix} 1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$$

$$\Rightarrow \det(N) = 0.$$

But $\det(N) = \det(aI_n - M)$ is a monic polynomial in a of degree n with coefficients in R.

$\Rightarrow a$ is integral over R. $\square$

(Ex $\frac{1}{2} \in \mathbb{Q}$ is not integral over $\mathbb{Z}$

$$\mathbb{Z}[\tfrac{1}{2}] = \left\{ \frac{a}{2^b} \;\middle|\; a \in \mathbb{Z}, b \in \mathbb{Z} \right\}$$

isn't a finitely gen. $\mathbb{Z}$-module.)

Cor 2.18 The integral closure of R in S is a ring (a ring ext. of R).

Pf Let $a, b \in S$ be integral over R.

$\overset{ii}{\Rightarrow}$ The ring ext. $R[a]$ of R is module-finite.
— " — $R[b]$ of R — " —

($R[a]$ gen. by $c_1, \dots, c_n$
$R[b]$ gen. by $d_1, \dots, d_m$)
$\Rightarrow R[a,b]$ gen. by $\{c_i d_j \mid {}^{1 \le i \le n}_{1 \le j \le m}\}$

But $a+b, a \cdot b \in R[a,b] \subseteq S$

$\overset{iii}{\Rightarrow}$ $a+b, a \cdot b$ are integral over R. $\square$

Ex $\sqrt[3]{2} + \sqrt[3]{3}$ is integral over $\mathbb{Z}$.

Cor 2.19 The alg. closure of K in L is a field (a field ext. of K).

Pf Let $0 \neq a \in L$ be algebraic over K.

Let $f(X) = X^n + c_{n-1} X^{n-1} + \dots + c_0 \in K[X]$ with $f(a) = 0$.

$$\Rightarrow a^n + c_{n-1} a^{n-1} + \dots + c_0 = 0$$

$$\Rightarrow 1 + c_{n-1} \frac{1}{a} + \dots + c_0 \left(\frac{1}{a}\right)^n = 0.$$

$\Rightarrow \frac{1}{a}$ is algebraic over K. $\square$

Cor 2.20 Integrality / algebraicity are transitive: If S is an integral ring ext. of R,
and T — " — S,
then T — " — R.

Pf HW. $\square$

Cor 2.21 Let S' be the integral closure of R in S. Then, S' is integrally closed in S.

Pf HW. $\square$