<u>Lemma</u> 4.5.3 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): Let $f(X) = X^n + c_{n-1} X^{n-1} + \dots + c_0 \in R(X)$ with $f(a) = 0$.

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

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

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

apply the induction hypothesis.

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

(Ex: $\mathbb{Z}[\sqrt[3]{2}]$ 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 matrix 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.)

<u>Cor 4.5.4</u> The integral closure of R in S is a ring (a ring ext. of R).

<u>Pf</u> 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 $\left\{ c_i d_j \;\middle|\; \begin{smallmatrix} 1 \le i \le n \\ 1 \le j \le m \end{smallmatrix} \right\}$

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

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

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

Cor 4.5.5 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 4.5.6 Integrality / algebraicity are transitive: If S is an integral ring ext. of R,
and T — " — S,
then T — " — R.

Pf HW. $\square$

Cor 4.5.7 Let S' be the integral closure of R in S. Then, S' is integrally closed in S.

Pf HW. $\square$

Thm 4.58 Any ring-finite field extension L of a field K is module-finite (= finite-dimensional K-vector space).
($\Rightarrow L$ is an algebraic extension of K).

Pf Let $L = K[a_1, \dots, a_n]$.
Use induction:
$n=1$: $L = K[a_1]$
If a_1 is algebraic, we're done.
If it isn't, then $1, a_1, a_1^2, \dots \in L$ are linearly independent over K.
$\Rightarrow$ The ring homomorphism

$$\begin{aligned} K[X] &\longrightarrow K[a_1] = L \\ X &\longmapsto a_1 \end{aligned}$$

is an isomorphism.
But $K[X]$ isn't a field!
$n-1 \to n$: Note that $L = K(a_1)[a_2, \dots, a_n]$.
$\Rightarrow$ By the induction hypothesis, the field extension $L = K(a_1)[a_2, \dots, a_n]$ of $K(a_1)$ is module-finite.

If a_1 is algebraic over K, then

$K(a_1) = K[a_1]$ is a module-fin. eset. of K.

Since L is a module-fin. eset. of $K(a_1)$,

L is a module-finite eset. of K.

If a_1 isn't algebraic over K:

$$\begin{aligned} K(a_1) &= \text{field of fractions of } K[a_1] \\ &\cong \quad \text{" } \quad \text{of } K[X] \\ &= K(X). \end{aligned}$$

The elements $a_2, \dots, a_n \in L$ are algebraic over $K(a_1) \cong K(X)$.

By Lemma 4.5.2, we can (for $i = 2, \dots, n$) write $a_i = \frac{p_i}{q_i}$ with $p_i \in L$ integral over $K[a_1] \cong K[X]$ and $0 \neq q_i \in K[a_1] \cong K[X]$

Now, proceed as in the proof that the extension $\mathbb{C}(X)$ of $\mathbb{C}$ isn't ring-finite (cf. section 4.4):

The ring $K[a_1] \cong K[X]$ contains ∞ many maximal ideals ($\cong$ monic irreducible polynomials).

$\Rightarrow$ There exists $r \in K[a_1] \cong K[X]$ relatively prime to $q_2, \dots, q_n$.

Since $\frac{1}{r} \in L = K[a_1, \dots, a_n] = K[a_1][a_2, \dots, a_n]$, we can write

$$\frac{1}{r} = \sum_j c_j \, a_2^{e_{2,j}} \cdots a_n^{e_{n,j}} \quad \text{with } c_j \in K[a_1],\ e_{ij} \geq 0.$$

$$\frac{1}{r} = \sum_j c_j \left(\frac{p_2}{q_2}\right)^{e_{2,j}} \cdots \left(\frac{p_n}{q_n}\right)^{e_{n,j}}$$

Multiply by large enough powers of $q_2, \dots, q_n$ to clear out denominators on the RHS.

$\Rightarrow$ Since $c_j \in K[a_1]$ and $p_2, \dots, p_n$ integral over $K[a_1]$, and since the integral closure of $K[a_1]$ in L is a ring, the RHS is then integral.

But $\text{LHS} = \dfrac{q_2^{\cdots} \cdots q_n^{\cdots}}{r} \in K(a_1) \setminus K[a_1]$
$\cong K(X) \setminus K[X]$

isn't integral over $K[a_1] \cong K[X]$ by Thm 4.5.1. $\square$