4.4. Ring and field extensions

<u>Def</u> Let R be a ring. A <u>ring extension</u> of R is a ring S containing R as a subring.

<u>Rmk</u> A ring extension of R is also an R-module.

<u>Def</u> Let K be a field. A <u>field extension</u> of K is a field L containing K as a subfield.

<u>Rmk</u> A field ext. of K is also a ring ext. of K and a K-vector space ($=K$-module).

<u>Def</u> Let S be a ring extension of R. The ring extension generated by a subset A of S is the smallest (= inclusion-minimal) subring $R[A]$ of S containing R and A.

<u>Rmk</u> $R[A]$ is the set of sums of products of the form $r \cdot a_1 \cdots a_m$ with $r \in R$ and $a_1, \dots, a_m \in A$.

Rmk Take $A = \{a_1, \dots, a_n\}$.

$R[A]$ is the image of the R-algebra homomorphism

$$\begin{aligned} R[X_1, \dots, X_n] &\longrightarrow S. \\ r \in R &\longmapsto r \\ X_i &\longmapsto a_i \end{aligned}$$

Def Let L be a field extension of K. The field extension generated by a subset A of L is the smallest subfield $K(A)$ of L containing K and A.

Rmk $K(A)$ is the quotient field of the ring extension $K[A]$ generated by A.

Ex $R[X_1, \dots, X_n]$ is a ring extension of R generated by $X_1, \dots, X_n$.

Ex $K(X_1, \dots, X_n)$ is a field extension of K generated by $X_1, \dots, X_n$.

Rmk We now have three notions of being finitely generated:

- fin. generated as a module: $\exists a_1, \dots, a_n$: every el. can be written as a sum of terms ra_i with $r \in R$.
  ((module-) finite)

- fin. generated as a ring extension: $\exists a_1, \dots, a_n$ every el. can be written as a sum of products $r a_1^{e_1} \cdots a_n^{e_n}$ with $r \in R$, $e_i \geq 0$.
  (ring-finite)

- fin. generated as a field extension: $\exists a_1, \dots, a_n$: every el. can be written as the quotient of two such sums
  (field-finite)

Rmk module-finite

$$\Downarrow$$

ring-finite

$$\Downarrow$$

field-finite

However:

<u>Rmk</u> module-finite

$$\not\Uparrow$$

ring-finite

<u>Pf</u> $\mathbb{C}[X]$ is a finitely generated ring ext. of $\mathbb{C}$,

but not a finitely generated $\mathbb{C}$-module

(= $\mathbb{C}$-vector space).

Basis: $1, X, X^2, \ldots$ $\square$.

<u>Rmk</u> ring-finite

$$\not\Uparrow$$

field-finite

<u>Pf</u> $\mathbb{C}(X)$ is a finitely generated field ext. of $\mathbb{C}$,

but not a fin. generated ring ext. of $\mathbb{C}$.

Assume $\mathbb{C}(X) = \mathbb{C}[a_1, \ldots, a_n]$.

Write $a_i(X) = \dfrac{p_i(X)}{q_i(X)}$ with $p_i, q_i \in \mathbb{C}[X]$,

$q_i \neq 0$.

Let $t \in \mathbb{C}$ be <u>not</u> a root of $q_1(X) \cdots q_n(X)$.

By assumption, we can write

$$\mathbb{C}(X) \ni \frac{1}{X-t} = \sum_j c_j \left(\frac{p_1(X)}{q_1(X)} \right)^{e_{1,j}} \cdots \left(\frac{p_n(X)}{q_n(X)} \right)^{e_{n,j}}$$

with $c_j \in K$, $e_{i,j} \geq 0$.

Multiply by $X-t$ and sufficiently large powers of $q_1(X), \ldots, q_n(X)$.

Plug in $X = t$.

$\Rightarrow$ LHS $\neq 0$, RHS $= 0$ $\lightning$ $\square$

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.

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

Pf module-finite: 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 $\left\{ a_i b_j \;\middle|\; \begin{array}{l} 1 \le i \le n, \\ 1 \le j \le m \end{array} \right\}$ as R-mod.

ring-finite: $S = R[a_1, \dots, a_n]$

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

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

field-finite: same ... $\square$

4.5 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 $f(x) \in R[x]$ (leading coeff. $= 1$: $f(x) = x^n + c_{n-1}x^{n-1} + \dots + c_0$) with $f(a) = 0$.

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 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 $f(X) = (X-a)(X-\bar{a})$

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

$\square$

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 4.5.1 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 $f\left(\frac{p}{q}\right) = 0$. $(c_i \in R)$

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

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

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 4.52 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. $\square$