$A \subseteq B$ $\quad$ B finitely generated A-algebra $B = A[b_1, \dots, b_r]$

finite A-algebra : $B = b_1 A + \dots + b_r A$

$b \in B$ integral over A if $\boxed{b^n + a_1 b^{n-1} + \dots + a_n = 0}$, $a_1, \dots, a_n \in A$

Thm. $A \subseteq B$, $b \in B$ $\quad$ $A \subseteq A[b] \subseteq B$. The following are equivalent:

1) b is integral over A;
2) $A[b]$ is a finite A-algebra.
3) $\exists$ C subring of B, containing $A[b]$, $A \subseteq A[b] \subseteq C \subseteq B$ s.t. C is a finite A-algebra.

Pf. 1) $\Rightarrow$ 2) Assume b integral over A: There is a relation.

Claim: $A[b]$ is generated by $1, b, \dots, b^{n-1}$

An A-module $A[b]$ is generated by all powers of b: enough to prove that $b^n, b^{n+1}, \dots, b^k, \dots$ are linear combinations of $1, b, \dots, b^{n-1}$

$$b^n \in A + bA + \dots + b^{n-1}A$$

$$b^{n+1} = b b^n = b(-a_1 b^{n-1} - \dots - a_n) = -a_1 \underbrace{b^n}_{} - \dots - a_n b$$

$$\Rightarrow b^{n+1} \in A + bA + \dots + b^{n-1}A$$

replace w. the lin. combination of previous powers

Then: induction on m to prove that

$$b^{n+m} \in A + bA + \dots + b^{n-1}A$$

Thm. $A \subseteq B$, $b \in B$, $A \subseteq A[b] \subseteq B$. The following are equivalent:

1) b is integral over A;
2) $A[b]$ is a finite A-algebra;
3) $\exists$ C subring of B containing $A[b]$, $A \subseteq A[b] \subseteq C \subseteq B$ s.t. C is a finite A-algebra.

2) $\Rightarrow$ 3) Easy: take $C = A[b]$

3) $\Rightarrow$ 1) $C \subseteq B$ finite A-algebra: $c_1, \dots, c_r$ generators

$C = Ac_1 + \dots + Ac_r$, $A[b] \subseteq C$: $bc_1, \dots, bc_r \in C$

$\forall i$ bc_i is a linear combination of $c_1, \dots, c_r$

$$\begin{cases} bc_1 = m_{11}c_1 + \dots + m_{1r}c_r \\ \vdots \\ bc_r = m_{r1}c_1 + \dots + m_{rr}c_r \end{cases} \qquad m_{ij} \in A$$

$$M = (m_{ij}) \qquad c = \begin{pmatrix} c_1 \\ \vdots \\ c_r \end{pmatrix} \qquad (M - bE_r)c = 0$$

b is an eigenvalue of M, c is an eigenvector

If A is a field, we could deduce $|M - bE_r| = 0$

i.e. the characteristic polyn. $P_M(b) = 0$

$P_M(x)$ is a monic polynomial w. coeff in A

$$b c_i = \sum_{j=1}^{r} m_{ij} c_j \qquad \boxed{(M - bE_r)c = 0}$$

$\mathrm{ad}(M-bE_r)$ adjoint matrix

$$\mathrm{ad}(M-bE_r)(M-bE_r) = \det(M-bE_r)E_r$$

$$\Rightarrow \det(M-bE_r)c = 0 \quad \Rightarrow \forall i \quad \underbrace{\det(M-bE_r)c_i}\, = 0$$

C is a ring containing $A[b] \ni 1$:

1 is a linear combination of $c_1 \dots c_r$, $\alpha_1, \dots, \alpha_r \in A$

$$1 = \alpha_1 c_1 + \dots + \alpha_r c_r \underset{C \text{ is commutative}}{=} c_1\alpha_1 + \dots + c_r\alpha_r \quad / \det(M-bE_r)$$

$$\det(M-bE_r) = \underbrace{\det(M-bE_r)c_1}_{=0}\alpha_1 + \dots + \underbrace{\det(M-E_r)c_r}_{=0}\alpha_r = 0$$

$$\Rightarrow \det(M-bE_r) = 0$$

$P_M(b) = 0$: b is integral over A

Consequences:

1) if b is integral over A, $A[b]$ is a finite A-module;
if $y \in A[b]$ $\qquad A[y] \subseteq A[b] \subseteq B$

We apply 3) $\Longrightarrow$ y is integral over A.
Every element of $A[b]$ is integral over A :
$A[b]$ is integral extension of A.

2) Transitivity of finiteness:
$A \subseteq B$, M a B-module $\Rightarrow$ M is also an A-module by restriction of the scalars
If M is a finite B-module, and B is a finite algebra over A $\Longrightarrow$ M is also a finite A-module.

Pf. Ass. M is generated as B-module $m_1, \dots, m_r$,
B is gen. as A-module by $b_1, \dots, b_s$ $\Longrightarrow$
$\forall\, m \in M \qquad m = \beta_1 m_1 + \dots + \beta_r m_r,\ \beta_1, \dots, \beta_r \in B$

$$\beta_i = \sum_{j=1}^{s} \alpha_{ij} b_j$$

$\Longrightarrow$ m is a linear combination of $\{b_i m_j\}_{\substack{i=1,\dots,r \\ j=1,\dots,s}}$ with coeff. in A $\Longrightarrow$ M is a finite A-module.

3)

3) $A \subseteq B$ $\quad b_1, \dots, b_n$ all integral over $A \Longrightarrow$
$A[b_1, \dots, b_n]$ is a finite A-module and integral extension of A.

Induction on n: $\quad n = 1$ ✓

Ass. $n > 1$ and that the prop. holds for $n-1$

Notation: $\quad A_r = A[b_1, \dots, b_r] \quad \forall \quad r \geq 1$

$$A_n = \underbrace{A_{n-1}}_{A[b_1 \dots b_{n-1}]}[b_n]$$

b_n integral over $A \Longrightarrow b_n$ is also integral over A_{n-1}

$\Longrightarrow A_n$ integral and finite A_{n-1}-module;

Inductive assumption: A_{n-1} is a finite A-module

$\Longrightarrow A_n$ is a finite A-module

If $b \in A_n$ $\qquad A[b] \subseteq \underbrace{A_n}_{\text{finite } A\text{-mod.}} \subseteq B \Longrightarrow b$ is integral over A

4) Transitivity of integral dependence

$A \subseteq B \subseteq C$ A subring of B subring of C

If B is integral extension of A, and C is integral extension of B $\Longrightarrow$ C is integral extension of A.

Pf $c \in C$: $c^n + b_1 c^{n-1} + \dots + b_n = 0$, $\underbrace{b_1, \dots, b_n \in B}$

$A \subseteq B' := A[b_1, \dots, b_n] \subseteq B$ c is integral over B'

$B'[c]$ is a finite B'-algebra

$A \subset \underset{\text{finite A-algebra}}{\underline{B'}} \subset B'[c] \Longrightarrow B'[c]$ is a finite A-algebra

$\underset{\text{finite A-alg.}}{A[c] \subseteq B'[c]} \subseteq C \overset{(3)}{\Longrightarrow} c$ is integral over A

Normalization Lemma K, $A = K[y_1, \dots, y_n]$ integral domain

$r = \operatorname{tr.d.} Q(A)/K$, $r \le n$

Then $\exists\, z_1, \dots, z_r \in A$, algebraically indep. over K, such that

A is an integral extension of $\underbrace{B := K[z_1, \dots, z_r]}_{\text{a polynomial ring in } r \text{ variables}}$

Proof only for K infinite field.

By induction on n

$n = 1$ $A = K[y]$, $Q(A) = K(y)$ $\begin{cases} y \text{ transcendental over } K \\ \text{or} \\ y \text{ algebraic over } K \end{cases}$

y transc. $\Rightarrow$ $r = 1$: take $B = A$

y algebraic $\Rightarrow$ $r = 0$: $A = K[y] = K(y)$

thus an algebraic extension of K of finite degree :

$K = B$ A is an integral extension of K

$n \ge 2$: ass. the thm. is true for algebras with $n-1$ generators over K

$A = K[y_1, \dots, y_n]$ $\quad \varphi : K[x_1, \dots, x_n] \twoheadrightarrow A$ surjective

$F(x_1, \dots, x_n) \longrightarrow F(y_1, \dots, y_n)$

1) $n = r$ $\Rightarrow$ $y_1, \dots, y_n$ are alg. indep., φ is isom.

$A \simeq K[x_1 \dots x_n]$, $B = A$

2) $r < n$: $y_1, \dots, y_n$ are alg. dependent, $\ker\varphi \neq (0)$.

$\exists\, F \neq 0$, $F \in \ker\varphi$ $\quad F(y_1, \dots, y_n) = 0$, $\underset{\overset{\shortparallel}{d}}{\deg F} > 0$

At least one variable occurs in F: ass. x_n occurs in F

If $F(x_1, \dots, x_n)$ is "monic" in x_n, then y_n is integral over $K[y_1, \dots, y_{n-1}]$.

$F = F_0 + F_1 + \dots + \underbrace{F_d}_{\neq 0}$

" F monic in x_n" means " x_n^d appears explicitly in F_d "

$F(x_1, \dots, x_n) = c\, x_n^d + \underbrace{\dots\dots}_{\text{pol. in } x_1, \dots, x_n \text{, s.t. the degree in } x_n \text{ is } < d}$

$0 = F(y_1, \dots, y_n) = \underset{\overset{\shortparallel}{0}\!\!\!\!\!/}{c}\, y_n^d +$ pol. in $y_1, \dots, y_{n-1}, x_n$

invertible in K : multiply c^{-1}

$\Rightarrow$ get a relation of integral dep. for y_n over $K[y_1 \dots y_{n-1}]$

By inductive assumpt. : $\exists\, z_1, \dots, z_r \in K[y_1 \dots y_{n-1}]$ alg. indep. s.t. $K[y_1 \dots y_{n-1}]$ is integral over $K[z_1 \dots z_r]$ $\xRightarrow[\text{of integral dep.}]{\text{transitivity}}$ $A = K[y_1 \dots y_n]$ is integral over $K[z_1 \dots z_r]$

So if $\ker\varphi$ contains some polyn. monic in one the variables $\Rightarrow$ conclude.

Ass. that $\ker\varphi \not\ni$ monic polynomial: "change variables" or "change coordinates".

We look for new generators for $A = k[y_1 \dots y_n]$ s.t. $F(x_1 \dots x_n) \in \ker\varphi$, $\neq 0$ of degree d, is monic w. respect to the new variables. We look for a very simple change of coordinates and precisely:

$$x_1 \longrightarrow x_1 + a_1 x_n$$
$$\vdots$$
$$x_{n-1} \longrightarrow x_{n-1} + a_{n-1} x_n$$
$$x_n \longrightarrow x_n$$

We look for elements $a_1, \dots, a_{n-1} \in A$ s.t. $F(x_1 \dots x_n)$ is monic in $x_1 + a_1 x_n, \dots, x_{n-1} + a_{n-1} x_n, x_n$

$$F(x_1 + a_1 x_n, \dots x_{n-1} + a_{n-1} x_n, x_n) = F_0(\dots) + \dots + \underbrace{F_d(x_1 + a_1 x_n \quad)}$$

The new variables contain linearly x_n

$F_d(x_1 + a_1 x_n, \dots, x_{n-1} + a_{n-1} x_n, x_n)$ is of deg d in x_n, the other have lowest degree