Chapter 2: Extension of rings and fields

Defn: $\alpha \in \mathbb{C}$ is call an <u>algebraic number</u> if $\exists\, f(x) \in \mathbb{Q}[x]$ a polynomial, s.t. $f(\alpha)=0$.

Ex: $\sqrt{2}$, $\sqrt{2}+\sqrt{3}$, i,

Fact: The set of all algebraic numbers forms a subfield $\overline{\mathbb{Q}} \subseteq \mathbb{C}$, which is the algebraic closure of $\mathbb{Q}$.

$\mathbb{C} - \overline{\mathbb{Q}}$ = transcendental numbers $\ni \pi, e, \dots$

Roughly speaking, algebraic numbers are most important "numbers" in <u>algebraic number theory</u>.

§1. Elements integral over a ring

<u>Thm 1.1</u>: R: ring, $A \subseteq R$ subring, $x \in R$. TFAE:

(a) $\exists\, a_0, \dots, a_{n-1} \in A$, s.t. $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$,

(b) The ring $A[x]$ is a fin. gen. A-mod

(c) $\exists$ B a subring s.t. $A \subseteq B \subseteq R$, $x \in B$ and B is a fin. gen. A-mod.

Pf: (a) $\Rightarrow$ (b): Clearly $A[x]$ is generated by $\{1, x, \dots, x^{n-1}\}$ since $x^n = -a_{n-1}x^{n-1} - \cdots - a_1 x - a_0$, $x^{n+1} = x \cdot x^n = \cdots$

(b) $\Rightarrow$ (c): let $B = A[x]$.

(c) $\Rightarrow$ (a). Suppose $B = Ay_1 + \cdots + Ay_n$, $x \in B$, B is ring

$\Rightarrow xy_i \in B$. $\Rightarrow xy_i = \sum_{j=1}^{n} a_{ij} y_j$, $\forall i$.

$\Rightarrow \sum_{j=1}^{n} (\delta_{ij} x - a_{ij}) y_j = 0$, $\quad \delta_{ij} = \begin{cases} 0 & i \neq j \\ 1 & i = j. \end{cases}$

Let T = matrix $(\delta_{ij} x - a_{ij})_{1 \le i,j \le n}$,

Recall from lin. alg. generalized Cramer's rule,

for an $n \times n$ matrix M and equation $Ma = b$
where $a = \begin{pmatrix} a_1 \\ a_n \end{pmatrix}$, $b = \begin{pmatrix} b_1 \\ b_n \end{pmatrix}$ column vectors, then have
$\det M \cdot a_i = \det M_i$
where M_i is the matrix by change $\text{col}_i(M)$ to b

Thus, we have $(\det T) \cdot y_i = 0 \quad \forall i$
thus $(\det T) \cdot y = 0, \ \forall y \in B$
$\Rightarrow \det T = 0$ since $1 \in B$
$\det T$ is precisely the desired poly. eqn. $\square$

Defn: R ring, $A \subseteq R$ subring, $x \in R$ is called integral over A if the equivalent conditions in Thm 1.1 are satisfied

Ex: $\mathbb{Z} \subseteq \mathbb{C}$, $\sqrt{2} \in \mathbb{C}$ is integral over $\mathbb{Z}$, since it is root of $x^2 - 2 = 0$
Fact: $\frac{\sqrt{2}}{2}$ is NOT integral over $\mathbb{Z}$. (pf = later).

Prop 1.2 R ring, $A \subseteq R$ subring, $x_1, \dots, x_n \in R$. If x_i is integral over $A[x_1, \dots, x_{i-1}]$ for all i, then $A[x_1, \dots, x_n]$ is a fin. gen. A-mod.

Pf: Recall an A-mod M is fin. gen if $\exists k$, s.t $\exists A^k \twoheadrightarrow M$.
Proof by induction on n. $n = 1$, Thm 1.1 (2)
suppose "case $n-1$" true, then $\exists k$, s.t. $A^k \twoheadrightarrow A[x_1, \dots, x_{n-1}]$,
x_n int over $A[x_1, \dots, x_{n-1}]$, by Thm 1.1 (2), $(A[x_1, \dots, x_{n-1}])^{\oplus k'} \twoheadrightarrow A[x_1, \dots, x_{n-1}, x_n]$
so get $A^{kk'} \twoheadrightarrow A[x_1, \dots, x_{n-1}, x_n]$ $\square$

Cor 1.3: $A \subseteq R$ rings., let $A' = \{x \in R, \ x \text{ int over } A\}$, Then A' is a ring and $A' \supseteq A$.

Pf: Suppose $x, y \in A'$, by Prop 1.2, $A[x,y]$ is fin. gen A-mod
$\Rightarrow x+y, x-y, xy \in A'$ by Thm 1.1(3).
$\Rightarrow A'$ is a ring.
$A \subseteq A'$ is obvious, by Thm 1.1(1).

Defn: (1) Let $A \subseteq R$, A' as in Cor 1.3. Then A' is called the integral closure of A in R

(2) Let A be an int domain, $K = \mathrm{Frac} A$, then the integral closure of A in K is called the integral closure of A. △

(3) Let $A \subseteq B$ be rings, say B is integral over A if $\forall x \in B$ is int over A. (i.e, the int clos of A in B is B).

Prop 1.4 (transitivity of integral relation) Let $A \subseteq B \subseteq C$ rings,
If B int over A, C int over B, then C int over A.

Pf: Let $x \in C$, x int over B. $\Rightarrow \exists\ x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0 = 0$
for some $b_i \in B$.
Let $B' = A[b_0, \cdots, b_{n-1}] \subseteq B$, then x int over B'.
b_i int over A, by Prop 1.2, B' is fin. gen A-mod,
$\Rightarrow B'[x]$ is fin. gen. A-mod by Prop 1.2 again
$\Rightarrow x$ int over A, by Thm 1.1(c). □

Prop 1.5 B: int dom; $A \subseteq B$ subring, and B is int over A.
Then B is field $\Leftrightarrow$ A is field.

Pf: "$\Leftarrow$". Suppose A is field. Let $b \in B$, $b \neq 0$, WANT: find b^{-1}.
$A[b]$ is fin. gen A-mod, $\Rightarrow A[b]$ is fin dim A-vec space,
$y \mapsto by$ is A-linear transformation of $A[b]$.

it is ring since $A[b] \subseteq B$ is int domain.
Thus it is bijective. Thus $\exists\ b' \in A[b]$, s.t. $bb' = 1$. i.e. $b' = b^{-1}$.

"$\Rightarrow$" Suppose B field, Let $a \in A - \{0\}$, Then $\exists\ a^{-1} \in B$. WANT: $a^{-1} \in A$.
a^{-1} int over $A \Rightarrow$ $a^{-n} + a_{n-1}a^{-n+1} + \cdots + a_1 a^{-1} + a_0 = 0$, $a_i \in A$,
multiply $a^{n-1} \Rightarrow$ $a^{-1} = -(a_{n-1} + \cdots + a_1 a^{n-2} + a_0 a^{n-1})$

$\Rightarrow a^{-1} \in A$. □

Defn. Int domain A is called integrally closed if it is its own integral closure.

Ex. A: int dom, $K = \mathrm{Frac}\, A$, A' = int closure of $A \subseteq K$.
then A' is int closed. Because by Prop 1.9 (transitivity of int relations), x int over $A' \Rightarrow x$ int over $A \Rightarrow x \in A'$.

Prop. 1.6: PID is int closed.

Pf: Suppose $x \in \mathrm{Frac}\, A$, $x = \frac{a}{b}$ with $(a,b) = 1$, (coprime)
If x int over A, then $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$, $a_i \in A$,

$\Rightarrow a^n + b(a_{n-1}a^{n-1} + \cdots + a_1 ab^{n-2} + a_0 b^{n-1}) = 0$
$\Rightarrow b \mid a^n$, i.e., $b \mid a^{n-1} \cdot a$, but $(a,b) = 1$
$\Rightarrow b \mid a^{n-1}$, iterate process $\Rightarrow b \mid a$
possible only when b is unit $\Rightarrow x \in A$. □

§2. Elements algebraic over a field.

Defn: R: ring, $K \subseteq R$ subfield, $x \in R$ is called algebraic over K if
$\exists\ a_0, \dots a_n \in K$, s.t. $a_n x^n + \cdots + a_1 x + x_0 = 0$

WLOG, can assume $a_n \neq 0$. So divide a_n, get
x alg over $K \iff x$ integral over K.
$\iff K[x]$ is fin. gen K-mod (i.e, fin. dim. vec space)

Defn: $K \subseteq R$ as above, say R is an algebraic extension of K if $\forall\ x \in R$ is alg. over K.

Lem: If L is a field, $K \subseteq L$ subfield, s.t. $[L:K] < \infty$, then L is alg. over K.

Pf: Apply Thm 1.1.(c). (Unless otherwise specified, the reference is within the current chapter, i.e, This is Chapter 2, Thm 1.1(c).)

Prop 2.1 $K \subseteq L \subseteq M$ three fields, if L is alg over K, M is alg over L, then M is alg over K. Furthermore $[M:K] = [M:L] \cdot [L:K]$

Pf: M/K alg $\iff M/K$ int $\Leftarrow$ use transitivity of integral relation.
If $\{l_i\}_{i \in I}$ a basis of L as K-mod ($\iff K$-vec. space)
$\{m_j\}_{j \in J}$ —— $M - L$ ——
then easy to check $\{l_i m_j\}_{i \times j \in I \times J}$ is basis of M over K. □

R ring, $K \subseteq R$ subfield, $x \in R$. Let $K[T]$: polynomial ring.
Let $\varphi: K[T] \to R$ be the ring homomorphism defn by $T \mapsto x$.
Then x is alg over $K \iff \ker \varphi \neq \{0\}$
If $\ker \varphi \neq (0)$, since $K[T]$ is PID $\Rightarrow \ker \varphi = (f(T))$ for some $f(T) \in K[T]$.

Defn: x is alg over K, let $\mathrm{Irr}(x, K) :=$ the unique monic polynomial in the ideal $(f(T))$. Call it the minimal polynomial of x over K.

Easy fact. $\mathrm{Irr}(\alpha, K)$ is the unique monic poly with least degree s.t. α is a root.

Ex: $\mathrm{Irr}(\sqrt{2}, \mathbb{Q}) = T^2 - 2$, $\mathrm{Irr}(i, \mathbb{R}) = T^2 + 1$.

$\mathrm{Irr}(\sqrt{2}, \mathbb{C}) = T - \sqrt{2}$

Suppose R: int domain, $\alpha \in R$.

Lem 2.2. α alg over K, then $K[\alpha]$ is a field, and $\mathrm{Irr}(\alpha, K)$ is an irreducible polynomial

Pf $\mathrm{Irr}(\alpha, K)$ irred $\Leftrightarrow \ker\varphi = (f(T))$ is prime ideal

Indeed, if $g(T), h(T) \in K[T]$, $g(T)h(T) \in \ker\varphi$,

then $g(\alpha)h(\alpha) = 0 \Leftrightarrow g(\alpha) = 0$ or $h(\alpha) = 0 \Leftrightarrow g$ or $h \in \ker\varphi$.

($\Leftrightarrow$: R is int dom.)

FACT: in a PID a nonzero prime ideal is a maximal ideal.

Pf of fact: $0 \subsetneq (\alpha) \subsetneq A$, (α) prime. If not max, then $(\alpha) \subsetneq (\beta)$, $\Rightarrow \alpha = \beta\gamma$, but $\beta\gamma \in (\alpha) \Rightarrow \gamma \in (\alpha)$ since $\beta \notin (\alpha)$

$\Rightarrow \gamma = \alpha\theta \Rightarrow \alpha = \beta\alpha\theta \Rightarrow \beta\theta = 1 \Rightarrow (\beta) = A$, contradiction □

Now, $K[\alpha] \simeq K[T]/\ker\varphi$ is a field bec. $\ker\varphi$ is a max ideal. □.

Rmk. The condition that R is int dom is almost always satisfied in our later application. Indeed, we mostly consider the case R is a field.

(Rmk: $\mathbb{C} \subseteq \mathbb{C}[x]/x^2$, then $\mathrm{Irr}(x, \mathbb{C}) = T^2$!)

Thm 2.3. K field, then $\exists$ some field E, s.t. all $f(T) \in K[T]$ can be factored as $f(T) = \prod_{i=1}^{n} (T - \alpha_i)$ for some $\alpha_i \in E$.

Defn. Call such E an algebraically closed extension of K. The minimal such E is called an algebraic closure, denoted as $\bar{K}$.

Ex: $K = \mathbb{R}$, then $\bar{K} = \mathbb{C}$.

Pf: We only prove the following fact: given a single fixed $g(T) \in K[T]$, can find a finite extension $K' = K_g$ of K, s.t. $g(T) = \prod_{i=1}^{m} (T - \alpha_i)$, for $\alpha_i \in K'$

then we can "let" $\overline{K} := \bigcup_{g \in K[T]} K'_g$ (some set theory, Zorn lemma needed to make this rigorous.)

To prove the above, it suffices to prove when $g(T)$ is irreducible polynomial. Let $K'' = K[Y]/g(Y)$, which is a field. $g(T)$ considered as a poly in $K''[T]$, has a root $\overline{Y}$. $\Rightarrow g(T) = (T - \overline{Y})h(T)$ for some $h(T) \in K''[T]$. We can iterate the argument with $h(T)$ to find the desired K'. □

Lem 2.4: K: field, char $k = 0$. $f(T) \in K[T]$ monic, irred. Suppose $f(T) = \prod_{i=1}^{n} (T - x_i)$ in $\overline{K}$, then x_i are distinct.

Pf: If not, suppose $x_1 = x_2$.
Note $f(T) \in (\mathrm{Irr}(x_1, K))$ $\Rightarrow \mathrm{Irr}(x_1, K) = f(T)\, g(T)$
$\Rightarrow \mathrm{Irr}(x_1, K) = f(T)$.
$x_1 = x_2 \Rightarrow x_1$ is a root of $f'(T)$ (the derivative)
$\Rightarrow f(T) \mid f'(T)$.
which is impossible, since $\deg f'(T) = n - 1$ □

(Thm of primitive element) finite
Thm 2.5: $K \subseteq K'$ field extension, char $= 0$, then $\exists$ some $\alpha \in K'$, s.t. $K' = K[\alpha]$.
(all such α a primitive element of the ext K'/K)
Ex: $K = \mathbb{Q}$, $K' = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, then can take $\alpha = \sqrt{2} + \sqrt{3}$

Pf: If $[K' : K] = 2$, can take any $\alpha \in K' \setminus K$.
By induction, reduces to the case $K' = K[\alpha, \beta]$.
WANT some γ, s.t. $K' = K[\gamma]$.
Claim: can find some $\lambda \in K$, s.t. $K' = K[\alpha + \lambda\beta] = K[\gamma]$ (in fact, ∞-many such λ)
For above to be true, it suffices that $\beta \in K[\gamma]$

$\Leftrightarrow m(T) = \mathrm{Irr}(\beta, K[\gamma])$ has deg 1.

Let $f(T) = \mathrm{Irr}(\alpha, K)$, $g(T) = \mathrm{Irr}(\beta, K)$,
let $h(T) := f(\gamma - \lambda T) \in K[\gamma][T]$, and $h(\beta) = 0$.
Recall $w(T) \in K[\gamma][T]$, $w(\beta) = 0$
$\Rightarrow w(T) \mid h(T)$
also, $g(T) \in K[T] \subseteq K[\gamma][T]$, $g(\beta) = 0$
$\Rightarrow w(T) \mid g(T)$
Thus, it suffices if $\mathrm{GCD}(h(T), g(T))$ has deg ≤ 1, considered as elements in $K[\gamma][T]$.
which, $\Leftarrow$ $h(T), g(T)$ has only one common root β.
suppose otherwise, $h(\beta') = 0, g(\beta') = 0$, $\beta' \neq \beta$.

then $f(\gamma - \lambda\beta') = 0 \Rightarrow \alpha' = \gamma - \lambda\beta'$ is a root of $f(T)$

$$\alpha' = \alpha + \lambda\beta - \lambda\beta' \Rightarrow \lambda = \frac{\alpha' - \alpha}{\beta - \beta'}$$

So, the only possible "bad" λ are those that can be expressed as above with α, α' roots of $f(T)$ and β, β' roots of $g(T)$,
$\Rightarrow$ only fin. many such "bad" λ.
Thus can take any other λ. □

Ex. $K' = \mathbb{Q}[\sqrt{5}, \sqrt{7}]$
$f(T) = T^2 - 5$, $g(T) = T^2 - 7$

$$\text{bad } \lambda = \frac{\pm(\sqrt{5} - (-\sqrt{5}))}{\pm(\sqrt{7} - (-\sqrt{7}))} = \pm\left(\frac{\sqrt{5}}{\sqrt{7}}\right)$$

thus can take $\alpha = \sqrt{5} + \lambda\sqrt{7}$ for any $\lambda \neq \pm\frac{\sqrt{5}}{\sqrt{7}}$ or 0.

No.

Date

Defn: $K \subseteq L$, $K \subseteq L'$ fields, a K-isomorphism is an isomorphism $\varphi: L \to L'$ such that $\varphi(a) = a$, $\forall a \in K$.
And we say L and L' are conjugate over K.

Defn: $K \subseteq L$, $K \subseteq L'$ fields, $x \in L$, $x' \in L'$, say x, x' are conjugate over K, if $\exists$ K-isom $\varphi: K(x) \to K(x')$ s.t. $\varphi(x) = x'$.

Lem 2.6 Notation as above, then x, x' are K-conj $\Leftrightarrow$ $\mathrm{Irr}(x, K) = \mathrm{Irr}(x', K)$.
Pf: "$\Rightarrow$", $K[T]/(\mathrm{Irr}(x, K)) \simeq K[x] \simeq K(x') \simeq K[T]/(\mathrm{Irr}(x', K))$

"$\Leftarrow$" easy $\square$

Thm 2.7: $K \subseteq K'$ field ext, $\mathrm{char} = 0$, $[K' : K] = n$, then $\exists$ precisely n K-isom of K' into $\overline{K}$.
Pf: Indeed, let $K' = K[\alpha]$ by primitive element thm,
let $\mathrm{Irr}(\alpha, K) = f(T) = \prod_{i=1}^{n} (T - x_i)$, $x_i \in \overline{K}$, (distinct by Lem 2.4)
The n K-isom are defn by
$\varphi_i: K' \to \overline{K}$, $\varphi_i(\alpha) = x_i$.
easy to check they are the only one by Lem 2.6. $\square$

§3. Integers in quadratic fields

Defn: $K/\mathbb{Q}$, s.t $[K:\mathbb{Q}]=2$ is called a quadratic field.

Prop 3.1. Any quad field is of form $K=\mathbb{Q}(\sqrt{d})$ for some $d\in\mathbb{Z}$ squarefree.

Pf: Take any $x\in K\setminus\mathbb{Q}$, then $\mathbb{Q}\subsetneq\mathbb{Q}(x)\subseteq K$

$[K:\mathbb{Q}]=2=[\mathbb{Q}(x):\mathbb{Q}][K:\mathbb{Q}(x)] \Rightarrow \mathbb{Q}(x)=K$

Suppose $\mathrm{Irr}(x,\mathbb{Q})=x^2+bx+c$, $b,c\in\mathbb{Q}$

$\Rightarrow x=\frac{1}{2}(-b\pm\sqrt{b^2-4c})$

$\Rightarrow \mathbb{Q}(x)=\mathbb{Q}(\sqrt{b^2-4c})=\mathbb{Q}(\sqrt{\frac{u}{v}})$ for $\frac{u}{v}\in\mathbb{Q}$, $(u,v)=1$

$=\mathbb{Q}(\sqrt{\frac{uv}{v^2}})=\mathbb{Q}(\sqrt{uv})$ □.

Defn: For $K=\mathbb{Q}(\sqrt{d})$ d squarefree, call it { real quad field if $d>0$; imaginary quad field if $d<0$

$x\in K\Rightarrow x=a+b\sqrt{d}$, $a,b\in\mathbb{Q}$, its conjugate in $\bar{\mathbb{Q}}$ is $a-b\sqrt{d}$

(recall there are two $\mathbb{Q}$-isom of K into $\bar{\mathbb{Q}}$.

$id: K\to\bar{\mathbb{Q}}$, $\sqrt{d}\mapsto\sqrt{d}$

$\sigma:$ $\sqrt{d}\mapsto-\sqrt{d}$.)

Let $A:=\{x\in K \mid x \text{ integral over } \mathbb{Z}\}$ called ring of integers.

Thm 3.2. $K=\mathbb{Q}(\sqrt{d})$ d sqfree (thus $d\not\equiv 0 \pmod 4$)

(a) if $d\equiv 2,3 \pmod 4$, then $A=\{a+b\sqrt{d} \mid a,b\in\mathbb{Z}\}$

(b) if $d\equiv 1 \pmod 4$, then $A=\{\frac{1}{2}(u+v\sqrt{d}) \mid u,v\in\mathbb{Z},\ 2\mid u-v\}$

Pf: $x\in A\Leftrightarrow \mathrm{Irr}(x,\mathbb{Q})\in\mathbb{Z}[T]$, since $\mathrm{Irr}(x,\mathbb{Q})=\mathrm{Irr}(\sigma(x),\mathbb{Q})$, $x\in A\Leftrightarrow\sigma(x)\in A$.

A is a ring. $\Rightarrow x+\sigma(x)$, $x\cdot\sigma(x)\in A$. Let $x=a+b\sqrt{d}\in A$,

then $2a\in\mathbb{Q}$, $a^2-db^2\in\mathbb{Q}$ are also integral over $\mathbb{Z}$.

$\mathbb{Z}$ PID $\Rightarrow\mathbb{Z}$ int closed $\Rightarrow 2a\in\mathbb{Z}$, $a^2-db^2\in\mathbb{Z}$

$\Rightarrow 4a^2-4db^2\in\mathbb{Z} \Rightarrow 4db^2\in\mathbb{Z} \Rightarrow 4b^2\in\mathbb{Z} \Rightarrow 2b\in\mathbb{Z}$

↑ bec d sqfree

Let $a = u/2$, $b = v/2 \Rightarrow a^2 - dv^2 \in 4\mathbb{Z}$ ⊛

note $t \in \mathbb{Z}$, then $t^2 \equiv 0, 1 \pmod 4$

$\Rightarrow$ if $d \equiv 2, 3 \pmod 4$, ⊛ possible only when $2 \mid u$, $2 \mid v$.

if $d \equiv 1 \pmod 4$ ⊛ possible only when $2 \mid u - v$, i.e. u, v same parity

Thus, in case (a), $A \subseteq \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$

(b) $A \subseteq \{\frac{1}{2}(u + v\sqrt{d}) \mid u, v \in \mathbb{Z},\ 2 \mid u - v\}$.

In (a), easy to see "$\supseteq$", since $\sqrt{d} \in A$

(b) also can check "$\supseteq$", i.e. can check $\frac{1+\sqrt{d}}{2} \in A$, since $\left(\frac{1+\sqrt{d}}{2}\right)^2 - 1\left(\frac{1+\sqrt{d}}{2}\right) - \frac{d-1}{4} = 0$

□,

Now, in (a), $A = \mathbb{Z} \oplus \mathbb{Z}\sqrt{d}$

(b) $A = \mathbb{Z} \oplus \mathbb{Z}\left(\frac{1+\sqrt{d}}{2}\right)$

No

Date

§4. Norms and traces.

Defn A: ring, $M = A^{\oplus n}$, $u: M \to M$, A-linear endomorphism,

By Lin. alg, can define trace, determinant, characteristic polynomial of u

Indeed, pick any basis of M, and let $U = (u_{ij})_{n\times n}$ be the $n\times n$ matrix corresp to u.

Then $\mathrm{Tr}(u) = \mathrm{tr}(U) = \sum_{i=1}^{n} u_{ii}$

$\det(u) = \det(U)$

$\mathrm{char.poly}(u) = \det(T\cdot I_n - U) \in A[T]$

By lin. alg, the above defn is indep of choice of basis.

Recall: $\mathrm{Tr}(u+u') = \mathrm{Tr}(u) + \mathrm{Tr}(u')$

$\det(uu') = \det(u)\det(u')$

$\det(T\cdot I_n - u) = T^n - \mathrm{Tr}(u)\cdot T^{n-1} + \cdots + (-1)^n \det(u)$

Now, let $A \subseteq B$ rings, s.t. $B = A^n$ as A-mod. (e.g. field ext of deg n)

Defn For $x \in B$, let $\mathrm{Tr}_{B/A}(x)$, $N_{B/A}(x)$, $\mathrm{char.poly}_{B/A}(x)$ to be the trace, determinant, char. poly of the A-linear morphism: $m_x: B \to B$, $b \mapsto bx$.

We remove the subscripts "B/A" if no confusion arises

Ex $A = \mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) = B$, take A-basis of B: $\{1, \sqrt{2}\}$.

for $x = \sqrt{2}$, $m_x: B \to B \rightsquigarrow \sqrt{2}\begin{pmatrix}1\\ \sqrt{2}\end{pmatrix} = \begin{pmatrix}0 & 1\\ 2 & 0\end{pmatrix}\begin{pmatrix}1\\ \sqrt{2}\end{pmatrix}$

$\Rightarrow \mathrm{Tr}(\sqrt{2}) = 0$, $N(\sqrt{2}) = -2$, $\mathrm{char\ poly}(\sqrt{2}) = T^2 - 2$.

Note. take $x = a \in A$, then $m_a \rightsquigarrow \begin{pmatrix}a & 0\\ 0 & a\end{pmatrix}$. $\Rightarrow \mathrm{Tr}(a) = na$, $N(a) = a^n$.

$[L:K]=n$.

Prop 4.1 $K \subseteq L$ fields, char $=0$, $x \in L$, $\mathrm{Irr}(x,K) = \prod_{i=1}^{m}(T-x_i)$ in $\bar{K}[x]$.
(note $K \subseteq K[x] \subseteq L$, thus $m \mid n$)
Then $\mathrm{Tr}_{L/K}(x) = \frac{n}{m}(x_1 + \cdots + x_m)$,

$$N_{L/K}(x) = (x_1 \cdot \cdots \cdot x_m)^{\frac{n}{m}}$$

$$\text{Char poly}(x) = (\mathrm{Irr}(x,K))^{n/m} = \left(\prod_{i=1}^{m}(T-x_i)\right)^{n/m}.$$

Pf: **Special case** $n=m$, i.e, $L=K[x]$, i.e, x is a primitive elt.
Denote $F(T) = \mathrm{Irr}(x,K) = T^n + a_{n-1}T^{n-1} + \cdots + a_1 T + a_0$
As a K-mod, $L = K[x] = \langle 1, x, \cdots, x^{n-1}\rangle_K$
the matrix of m_x w.r.t basis $\{1, x \cdots x^{n-1}\}$ is

$$m_x(1, x, \cdots, x^{n-1}) = (1, x, \cdots, x^{n-1}) \begin{pmatrix} 0 & & & -a_0 \\ 1 & 0 & & -a_1 \\ 0 & 1 & & \vdots \\ & & 0 & \\ 0 & 0 & 1 & -a_{n-1} \end{pmatrix} \in M$$
$$= (x, x^2, \cdots, x^n)$$

$$T \cdot I_n - M = \begin{pmatrix} T & & & a_0 \\ -1 & T & 0 & a_1 \\ & -1 & & \vdots \\ & & T & a_{n-2} \\ 0 & & -1 & T + a_{n-1} \end{pmatrix} \begin{matrix} \text{row}_1 \\ + T \cdot \text{row}_2 \\ + \\ + T^{n-1} \cdot \text{row}_n \end{matrix} \rightsquigarrow \begin{pmatrix} 0 & 0 & \cdots & 0 & F(T) \\ -1 & T & & & a_1 \\ & -1 & & & \\ & & \ddots & & \\ & & & T & \\ & & & -1 & T + a_{n-1} \end{pmatrix}$$

$\Rightarrow \text{charpoly}(x) = \det(T \cdot I_n - M) = (-1)^{n-1} \cdot F(T) \cdot (-1)^{n-1} = F(T)$

$\Rightarrow \mathrm{Tr}(x) = \sum x_i$, $N(x) = \prod x_i$

General case $[L:K(x)] = \frac{n}{m} = r$. Suppose $L = \langle z_1, \cdots, z_r\rangle_{K(x)}$. Since $K(x) = \langle 1, \cdots, x^{m-1}\rangle_K$
then $L = \langle z_1, xz_1, \cdots, x^{m-1}z_1, z_2, xz_2, \cdots x^{m-1}z_2, \cdots, z_r, xz_r, \cdots, x^{m-1}z_r\rangle_K$
check m_x w.r.t basis of L above is $\begin{pmatrix} M & & 0 \\ & M & \\ 0 & & M \end{pmatrix}$, then easy to conclude

□