Algebraic numbers, algebraic integers

Motivation: diophantine equations

(a) $x^3 - 2y^3 = m$

$(x - y\sqrt[3]{2})(x^2 + xy\sqrt[3]{2} + y^2\sqrt[3]{4})$ $\qquad x - y\sqrt[3]{2} \in \mathbb{Z}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Z}\}$

(b) $x^p + y^p = z^p \quad (p > 2 \text{ prime})$

$(x+y)(x+\zeta_p y)\cdots(x+\zeta_p^{p-1} y)$ $\qquad x + \zeta_p^k y \in \mathbb{Z}[\zeta_p] = \left\{ \sum_{j=0}^{p-2} a_j \zeta_p^j \mid a_j \in \mathbb{Z} \right\}$

$\zeta_p = e^{2\pi i/p}$

Algebraic number theory: studies arithmetic of subrings $A \subset \mathbb{C}$ such that $(A, +)$ is a finitely generated abelian group, $A = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_m$ ($\alpha_i : \mathbb{Z}[i] = \mathbb{Z}\cdot 1 + \mathbb{Z}\cdot i$).

If $(A, +) = \mathbb{Z}\beta_1 \oplus \cdots \oplus \mathbb{Z}\beta_n$ (β_j linearly independent over $\mathbb{Z}$, $n \le m$), then the **fraction field of A** $K = \mathrm{Frac}(A) = \left\{\frac{a}{b} \mid a, b \in A, b \neq 0\right\} \subset \mathbb{C}$ has additive group $(K, +) = \mathbb{Q}\beta_1 \oplus \cdots \oplus \mathbb{Q}\beta_n \Rightarrow [K : \mathbb{Q}] = n$.

Recall: $K \subset L$ fields $\Rightarrow$ the **degree of L over K** is $\underbrace{[L:K]}_{\dim_K(L)}$ = dim of L as a vector space over K

Ex: $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = [\mathbb{C} : \mathbb{R}] = 2$.

Main general results:

(1) The subring $\mathcal{O}_K = \bigcup_{A' \subset K \text{ subring}, (A', +) \text{ finitely generated abelian group}} A'$ $\subset K$ ("the ring of integers of K")

has again additive group of the form $\mathcal{O}_K = \mathbb{Z}\omega_1 \oplus \cdots \oplus \mathbb{Z}\omega_n$ ($\Rightarrow \mathcal{O}_K \supset A$)

Ex: $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$, $\mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i]$, $\mathcal{O}_{\mathbb{Q}(i\sqrt{3})} = \mathbb{Z}[\zeta_3]$.

(2) $|\underbrace{P(A)}_{\text{principal ones}} \setminus \underbrace{I(A)}_{\text{fractional ideals of } A}| < \infty$

(3) (Dirichlet) $A^* \simeq (\text{finite cyclic group}) \times \mathbb{Z}^{r_1 + r_2 - 1}$, $K \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ $(r_1 + 2r_2 = n)$

(4) $\underbrace{I(\mathcal{O}_K) = I_{inv}(\mathcal{O}_K)}$

$\mathcal{O}_K$ is a **Dedekind ring**, has unique factorisation for ($\neq 0$) ideals

(5) One can say something about factorisation of prime numbers p into prime ideals of $\mathcal{O}_K$

Applications: **Kummer:** if $p \nmid \underbrace{|P(\mathbb{Z}[\zeta_p]) \setminus I(\mathbb{Z}[\zeta_p])|}_{\text{the class number } h_{\mathbb{Q}(\zeta_p)}}$, then

$x^p + y^p = z^p$ has no solutions $x, y, z \in \mathbb{Z}$ with $xyz \neq 0$.

Earlier [redacted] methods: worked only if $\underbrace{h_{\mathbb{Q}(\zeta_p)} = 1}_{\mathbb{Z}[\zeta_p] \text{ has unique factorisation}}$ ($\Leftrightarrow p \le 19$).

Key observation:

Prop. 1 If $M = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_m \subset \mathbb{C}$ is a finitely generated subgroup and if $\beta \in \mathbb{C}$ satisfies $\beta M \subset M$, then $\exists\ f(X) = X^n + a_1 X^{n-1} + \cdots + a_n \in \mathbb{Z}[X]$ monic, $f(\beta) = 0$.

Pf: $\beta\alpha_i = \sum_{j=1}^{m} u_{ij}\alpha_j$, $u_{ij} \in \mathbb{Z}$ | **Def:** β is an algebraic integer.

$U = (u_{ij}) \in M_m(\mathbb{Z})$, $\beta \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{pmatrix} = U \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{pmatrix} \Rightarrow \beta$ = eigenvalue of U, $\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{pmatrix} \in \mathbb{C}^m \setminus \{0\}$ eigenvector

$f(X) = \det(X \cdot I_m - U) \in \mathbb{Z}[X]$ monic, $f(\beta) = 0$.

Abstract version: A = integral domain, $K = \mathrm{Frac}(A)$ its fraction field, $L \supset K$ field, $M \subset (L, +)$ additive subgroup

Def. (1) The multiplier ring of M (in L) is $E_L(M) = \{\beta \in L \mid \beta M \subset M\}$

(2) M is an A-module if $\forall \alpha \in A$ $\alpha M \subset M$ ($\Leftrightarrow A \subset E_L(M)$)

(3) ——— " ——— of finite type if $\exists\ m_1, \dots, m_r \in M$ $M = Am_1 + \cdots + Am_r$.

(4) $\beta \in L$ is $\left\{\begin{matrix}\text{integral} \\ \text{algebraic}\end{matrix}\right\}$ over $\left\{\begin{matrix}A \\ K\end{matrix}\right\}$ if $\exists\ f \in \left\{\begin{matrix}A[X] \\ K[X]\end{matrix}\right\}$ monic such that $f(\beta) = 0$

Prop. 2. $A \subset \underbrace{L}_{\text{field}}$, $M \subset L$ A-module of finite type $\Rightarrow$ every $\beta \in E_L(M)$ is integral over A.

Pf: As in Prop. 1.

Prop. 3. B ring, K, L fields, $K \subset B \subset L$, $\dim_K(B) < \infty \Rightarrow B$ = field.

Pf: $B \subset$ field $\Rightarrow B$ domain $\Rightarrow \forall\ \alpha \in B \setminus \{0\}$ multiplication by α: $B \to B$, $x \mapsto \alpha x$ ($\dim_K(B) < \infty$) is an injective K-linear map $\Rightarrow$ it is surjective $\Rightarrow \exists \beta \in B$ $\alpha\beta = 1$.

Cor. If $\underbrace{A}_{\text{domain}} \subset \mathrm{Frac}(A) = K \subset \underbrace{L}_{\text{field}}$, $\alpha_1, \dots, \alpha_n \in L$, then:

$\alpha_1, \dots, \alpha_n$ $\left\{\begin{matrix}\text{integral} \\ \text{algebraic}\end{matrix}\right\}$ over $\left\{\begin{matrix}A \\ K\end{matrix}\right\}$ $\Rightarrow$ $\left\{\begin{matrix} A[\alpha_1, \dots, \alpha_n] = \sum_{0 \le k_i < d_i} A\alpha_1^{k_1} \cdots \alpha_n^{k_n} \\ \text{the smallest subring of } L \text{ containing } A, \alpha_1, \dots, \alpha_n \\ K[\alpha_1, \dots, \alpha_n] = \sum_{0 \le k_i < d_i} K\alpha_1^{k_1} \cdots \alpha_n^{k_n} \end{matrix}\right\}$ is

($\forall i$ $\sum_{j=0}^{d_i} a_{ij}\alpha_i^j = 0$, $a_{id_i} = 1$)

$\forall n \ge d_i$: $\alpha_i^n \in \left\{\begin{matrix} A \cdot 1 + A \cdot \alpha_i + \cdots + A \cdot \alpha_i^{d_i - 1} \\ K \cdot 1 + \cdots + K \cdot \alpha_i^{d_i - 1} \end{matrix}\right\}$ | $\left\{\begin{matrix}\text{an } A\text{-module of finite type} \\ \text{a } K\text{-vector space of } \dim_K < \infty\end{matrix}\right\}$ $\xrightarrow{\text{Prop. 2}}$

$\Rightarrow$ each element of $\left\{\begin{matrix} A[\alpha_1, \dots, \alpha_n] \\ K[\alpha_1, \dots, \alpha_n] \end{matrix}\right\}$ is $\left\{\begin{matrix}\text{integral over } A \\ \text{algebraic over } K\end{matrix}\right\}$ $\xrightarrow{\text{Prop. 3}}$ $K[\alpha_1, \dots, \alpha_n]$ is a field

$= K(\alpha_1, \dots, \alpha_n)$

the smallest subfield of L containing $K, \alpha_1, \dots, \alpha_n$

Cor. $\beta \in L$, $\beta^m + \alpha_1 \beta^{m-1} + \cdots + \alpha_n = 0$, $\alpha_1, \dots, \alpha_n$ $\left\{\begin{array}{l}\text{integral over } A \\ \text{algebraic over } K\end{array}\right\} \Rightarrow$ so is β.

Pf: $\left\{\begin{array}{ll} A[\alpha_1, \dots, \alpha_n, \beta] = \sum_{j=0}^{n-1} A[\alpha_1, \dots, \alpha_n]\beta^j & A\text{-module of finite type} \\ K[\text{---}] = \sum_{j=0}^{n-1} K[\text{---}]\beta^j & K\text{-vs of } \dim_K < \infty \end{array}\right.$

$\beta M \subset M$

Cor. $\{\beta \in L \mid \beta \text{ integral over } A\}$ (the integral closure of A in L) is a subring of L, equal to $\bigcup_{B \subset L \text{ subring}} B$, which is integrally closed.

$(B, +) = A$-module of finite type

Def. A domain A is integrally closed if every $\alpha \in \mathrm{Frac}(A)$ integral over A lies in A.

Prop 4. $A = UFD$ (ex: $A = \mathbb{Z}$) $\Rightarrow A$ is integrally closed.

Pf: If $\alpha = \frac{a}{b} \in \mathrm{Frac}(A)$, $\gcd(a,b) = 1$, $\alpha^n + a_1\alpha^{n-1} + \cdots + a_{n-1}\alpha + a_n = 0$

$a_i \in A \Rightarrow$ $a^n + \underbrace{a_1 a^{n-1} b + \cdots + a_{n-1} a b^{n-1}}_{\text{divisible by } b} + a_n b^n = 0$

If $b \notin A^\times$ $\exists \pi \in A$ irreducible $\pi \mid b \Rightarrow \pi \mid a^n \Rightarrow \pi \mid a \Rightarrow \pi \mid \gcd(a,b)$ contrad.

So $b \in A^\times \Rightarrow \alpha \in A$.

Ex: $A = \mathbb{Z}[i\sqrt{3}]$ is not integrally closed: $\xi_3 \notin A$, $\xi_3 \in \mathrm{Frac}(A)$, $\xi_3^2 + \xi_3 + 1 = 0$

Back to number fields:

Def: A number field is a field $K \supset \mathbb{Q}$ such that $[K:\mathbb{Q}] < \infty$.

Its ring of integers is $\mathcal{O}_K = \{\beta \in K \mid \beta \text{ integral over } \mathbb{Z}\}$.

By the above, it is an integrally closed subring of K.

Note: (1) $\alpha \in K \Rightarrow \exists a_i \in \mathbb{Z}, a_0 \neq 0$ $a_0\alpha^n + \cdots + a_n = 0$

$\Rightarrow$ $(a_0\alpha)^n + a_1(a_0\alpha)^{n-1} + \cdots + a_n a_0^{n-1} = 0 \Rightarrow a_0\alpha \in \mathcal{O}_K$.

So, if $[K:\mathbb{Q}] = n$, $\exists\ \alpha_1, \dots, \alpha_n \in \mathcal{O}_K$ such that

$\left(K \neq \mathbb{Q}\alpha_1 \oplus \cdots \oplus \mathbb{Q}\alpha_n \quad (\Rightarrow \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n \subset \mathcal{O}_K)\right)$.

Goal: $\exists \{\alpha_i\}$ such that $\mathcal{O}_K = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n$

an integral basis

Note: Prop. 4, Prop. 1 $\Rightarrow \mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$, $\mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i]$, $\mathcal{O}_{\mathbb{Q}(i\sqrt{3})} = \mathbb{Z}[\xi_3]$.

Algebraic background : Field extensions

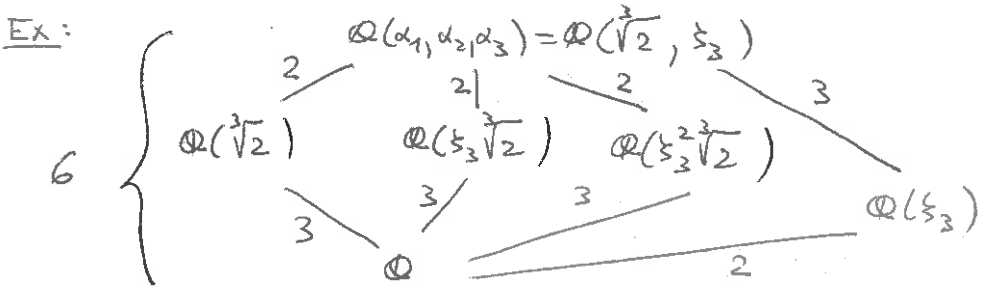
Recall : K field $\Rightarrow$ $\begin{cases} K \supset \mathbb{Q} & \text{"}K \text{ is of characteristic } 0\text{"} \\ K \supset \mathbb{F}_p & \text{" —— " —— } p\text{"} \end{cases}$, p = prime

Prop ("Tower law") $K \subset L \subset M$ fields $\Rightarrow$ $\underline{[M:K] = [M:L][L:K]}$.

Pf : If $(L,+) = \bigoplus_{i\in I} K\alpha_i$, $(M,+) = \bigoplus_{j\in J} L\beta_j \Rightarrow (M,+) = \bigoplus_{(i,j)\in I\times J} K(\alpha_i\beta_j)$

($\{\alpha_i\}_{i\in I}$ basis of $L/K \Rightarrow \{\alpha_i\beta_j\}_{(i,j)\in I\times J}$ basis of M/K) $[L:K]=|I|$, $[M:L]=|J|$, $[M:K]=|I\times J|$
$\{\beta_j\}_{j\in J}$ —" — M/L

Ex :



$x^3-2 = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$
$\alpha_1 = \sqrt[3]{2} \in \mathbb{R}$, $\alpha_2 = \xi_3\alpha_1$, $\alpha_3 = \xi_3^2\alpha_1$

Simple extensions : $K \subset L = K(\alpha)$, α algebraic over K

Ex : $\mathbb{R} \subset \mathbb{C} = \mathbb{R}(i) = \mathbb{R}[i] \simeq \mathbb{R}[X]/(X^2+1)$

$a+bi \longleftrightarrow a+b\overline{X}$

Quotients by ideals : (a) "ring" = commutative ring with 1

(b) **ring morphism** : $f: A \longrightarrow B$, $f(x+y)=f(x)+f(y)$, $f(xy)=f(x)f(y)$, $f(1)=1$

kernel : $\mathrm{Ker}(f) = \{x\in A \mid f(x)=0\} \subset A$ ideal of A

image : $\mathrm{Im}(f) = \{f(x) \mid x\in A\} \subset B$ subring of B

(c) A ring, $I \subset A$ ideal $\rightsquigarrow$ **quotient ring**

A/I = A/(equivalence given by $x \equiv y \pmod I \iff x-y \in I$)

projection $\mathrm{pr}: A \longrightarrow A/I$, $x \longmapsto \overline{x} = x+I$ (the residue class of x modulo I)

$\mathrm{Ker}(\mathrm{pr}) = I$

(d) **Isomorphism thm** : $f: A \longrightarrow B$ ring morphism $\Rightarrow$

ring isomorphism $\overline{f}: A/\mathrm{Ker}(f) \xrightarrow{\sim} \mathrm{Im}(f)$

$\overline{x} = x+\mathrm{Ker}(f) \longmapsto f(x)$

Ex : $A \neq 0$ ring, $g \in A[X]$ **monic** polynomial, $\deg(g) = n \geq 1$

$\Rightarrow$ $A[X]/(g) = A[X]/gA[X] = \{h(X) \pmod g \mid h\in A[X],\ \deg(h) < n\}$

(since any $f(X)\in A[X]$ can be written uniquely as $f = qg+h$, $q,h\in A[X]$, $\deg(h) < \deg(g)$.)

Def. A *principal ideal domain* (PID) is an integral domain A in which every ideal is principal, $I = (a) = aA$ for some $a \in A$.

Prop A Euclidean $\Rightarrow$ A PID ($\varphi: A = \mathbb{Z}$; $K[X]$ (K field)).

Pf: If $\{0\} \neq I \subset A$ ideal, $\varphi: A \to \mathbb{N}$ as in the definition of "A Euclidean", let $b \in I \setminus \{0\}$ with $\varphi(b) = \min\{\varphi(a) \mid a \in I \setminus \{0\}\}$. Then $(b) \subset I$; if $a \in I \setminus \{0\}$ $a = qb + r$, $q, r \in A$, $\varphi(r) < \varphi(b)$

$\Rightarrow r = a - qb \in I$ $\xrightarrow{\text{minimality of } \varphi(b)}$ $r = 0 \Rightarrow a = qb \in (b)$.

Prop: A PID $\Rightarrow$ A UFD
Pf: Later

Back to simple field extensions: $K \subset L$ fields, $\alpha \in L$ algebraic over K

evaluation morphism: $ev_\alpha: K[X] \to L$, $g(X) \mapsto g(\alpha)$ — ring morphism, $ev_\alpha|_K = id$ — "morphism of K-algebras"

$\ker(ev_\alpha) \subsetneq K[X]$ ideal, non-zero ($K[X]$ PID)

$\Rightarrow \ker(ev_\alpha) = (f)$, $f \in K[X] \setminus K$, f monic ($\Rightarrow f$ unique)

Def: f = the *minimal polynomial of α over K*

$n = \deg(f) \geq 1$ = the *degree of α over K*

Properties: (1) $g \in K[X]$ satisfies $g(\alpha) = 0 \iff f \mid g$.

(2) $K[X] \xrightarrow{pr} K[X]/(f) = K \cdot 1 \oplus K \cdot \overline{X} \oplus \cdots \oplus K \cdot \overline{X}^{n-1}$, $\dim_K = n$

$K[X] \xrightarrow{g \mapsto \overline{g}}$ (the quotient map)

(3) $K[X]/(f) \xrightarrow{\overline{ev_\alpha}} \operatorname{Im}(ev_\alpha) = K[\alpha] = K(\alpha) \subset L$

$n = \dim_K < \infty \Rightarrow$ *field*, $[K(\alpha) : K] = n$

$1, \alpha, \ldots \alpha^{n-1}$ basis of $K(\alpha)/K$

(4) $K[X]/(f)$ domain $\Rightarrow f$ *irreducible*.

(5) *Converse:* If $f \in K[X]$ monic, $\deg(f) = n \geq 1$, f irreducible

$\Rightarrow L = K[X]/(f)$ is a domain, $\dim_K(L) = n < \infty \Rightarrow L$ *field*

$\alpha \in \overline{X}$ satisfies $f(\alpha) = \overline{f(X)} = 0 \in L$, $g(\alpha) \neq 0$ if $\deg(g) < n$, $g \in K[X]$

$\Rightarrow f$ = minimal polynomial of α over K

Cor. K field, $f \in K[X] \setminus K \Rightarrow \exists$ field $K_1 \supset K$, $\alpha_1 \in K_1$ $f(\alpha_1) = 0$

Pf: take $f_1 \mid f$ irred., $K_1 = K[X]/(f_1) \ni \overline{X} = \alpha_1$ $f_1(\alpha_1) = 0$.

Cor. — " — $\Rightarrow \exists$ field $L \supset K$, $f = c\prod_{i=1}^{n}(X - \alpha_i)$, $\alpha_i \in L$, $c \in K^*$

Pf: Induction on n.

The Chinese Remainder Thm (CRT). A = ring, $I, J \subset A$ ideals such that $I+J = A = (1)$. Then $IJ = I \cap J$ and

$$A/(I \cap J) \longrightarrow A/I \times A/J$$
$$x \pmod{I \cap J} \longmapsto (x \pmod I,\ x \pmod J)$$

is a ring isomorphism. [Note: $\forall k \geq 1$ $(1) = (I+J)^{2k} \subset I^k + J^k \Rightarrow I^k + J^k = (1)$]

Pf: $f: A \longrightarrow A/I \times A/J$, $f(x) = (x \pmod I,\ x \pmod J)$ has $\ker(f) = I \cap J$.
$\exists\ i \in I,\ j \in J$ $i+j = 1 \Rightarrow \forall a, b \in A$ $f(bi + aj) = (a \pmod I,\ b \pmod J) \Rightarrow f$ surjective
$IJ \subset I \cap J$ always. If $a \in I \cap J \Rightarrow a = ai + aj \in IJ + IJ = IJ$

Cor. If $I_1, \dots, I_n \subset A$ ideals such that $I_i + I_j = A$ $\forall i \neq j \Rightarrow$

$I_1 \cdots I_n = I_1 \cap \cdots \cap I_n$ and $A/(I_1 \cap \cdots \cap I_n) \xrightarrow{\sim} A/I_1 \times \cdots \times A/I_n$

Ex: (1) $A = K[X]$, K field, $g_1, \dots, g_n$ distinct monic irreducible polynomials $\in K[X] \setminus K$, $r_i \geq 1$, $f = g_1^{r_1} \cdots g_n^{r_n}$
$I_i = (g_i^{r_i})$, $I_1 \cdots I_n = (f)$ $\quad \left(\sum r_i \deg(g_i) = \deg(f)\right)$

$$K[X]/(f) \xrightarrow{\sim} \prod_{i=1}^n K[X]/(g_i^{r_i})$$

(2) If $r_1 = \cdots = r_n = 1$, then $K[X]/(f) \xrightarrow{\sim} \prod_{i=1}^n \underbrace{K[X]/(g_i)}_{L_i = \text{field}}$, $[L_i : K] = \deg(g_i)$

(3) If $r_1 = \cdots = r_n = 1$, $g_i = X - \alpha_i$ $\quad (\alpha_i \in K$ distinct$)$

$\overline{ev_{\alpha_i}}$: $K[X]/(X-\alpha_i) \xrightarrow{\sim} K$, $\overline{h}(X) \longmapsto h(\alpha_i)$

$$K[X]/\prod_{i=1}^n (X-\alpha_i) \xrightarrow{\sim} \prod_{i=1}^n K$$
$$\overline{h(X)} \longmapsto (h(\alpha_1), \dots, h(\alpha_n))$$
$$\overline{\frac{1}{f'(\alpha_i)} \frac{f(X)}{X-\alpha_i}} \longleftrightarrow e_i = (0, \dots, 1, 0, \dots, 0)$$
$$\overline{\sum_{i=1}^n \frac{a_i}{f'(\alpha_i)} \frac{f(X)}{X-\alpha_i}} \longleftrightarrow (a_1, \dots, a_n)$$

Lagrange interpolation

Separable polynomials: for $f = \sum_{i=0}^n a_i X^i \in K[X] \setminus K$ let $f' = \sum_{i=1}^n \underbrace{i a_i}_{a_i + \cdots + a_i \ (i \text{ times})} X^{i-1} \in K[X]$

Exercise: (1) f has distinct roots (in some field $L \supset K$) $\Leftrightarrow \gcd(f, f') = 1$ (in $K[X]$)

(2) If f is irreducible, then: $\gcd(f, f') = 1 \Leftrightarrow f' \neq 0 \Leftrightarrow$ always if $K \supset \mathbb{Q}$,
if $f(X) \neq g(X^p)$ if $K \supset \mathbb{F}_p$.

Finite fields: F field, $|F| < \infty \Leftrightarrow F \supset \mathbb{F}_p$, $[F : \mathbb{F}_p] = n < \infty \Rightarrow |F| = p^n \Rightarrow$

$\forall \alpha \in F^*$ $\alpha^{p^n - 1} = 1 \Rightarrow \forall \alpha \in F$ $\alpha^{p^n} - \alpha = 0$. $\quad (*)$

F^* cyclic (of order $p^n - 1$) $\Rightarrow$ for any generator α of F^*, $F = \mathbb{F}_p(\alpha) \simeq \mathbb{F}_p[X]/(f)$,
f minimal polynomial of α over $\mathbb{F}_p \overset{(*)}{\Rightarrow} f \mid \underbrace{(X^{p^n} - X)}_{g}$ in $\mathbb{F}_p[X]$ $\quad (\deg(f) = n,\ f \text{ irred.})$
$g' = -1 \in \mathbb{F}_p[X] \Rightarrow g$ has p^n distinct roots $\Rightarrow$ $F = \{\text{the roots of } X^{p^n} - X \text{ (in some big } L \supset \mathbb{F}_p)\}$

$\Rightarrow$ **F is unique.** field $\Rightarrow$ **F exists.**

Notation: $F = \mathbb{F}_{p^n}$

Algorithmic aspects

(1) **Computing the inverse**: if $0 \neq \beta \in L = K[X]/(f) = K(\alpha)$, $f(\alpha)=0$ (f = minimal polynomial of α over K, $n = [L:K] = \deg(f) \geq 2$), then $\exists!\ g \in K[X]$, $\deg(g) < n$, $g(\alpha) = \beta$. As f is irreducible in $K[X]$, $\gcd(f,g) = 1 \overset{\text{Euclid's algorithm}}{\Longrightarrow} \exists\ a, b \in K[X]$ $a(X) f(X) + b(X) g(X) = 1$

$\Rightarrow b(\alpha) g(\alpha) = 1$, $b(\alpha) = \beta^{-1}$.

---

(2) **Berlekamp's algorithm**: **factorisation of polynomials in $\mathbb{F}_q[X]$**, $q = p^n$

For every ring $A \supset \mathbb{F}_q$ the Frobenius map $\underline{\varphi_q : a \longmapsto a^q = a^{p^n}}$ is a ring morphism $\varphi_q : A \longrightarrow A$, $\varphi \circ \cdots \circ \varphi$ n times, $\varphi(a) = a^p$ since $(a+b)^p = a^p + b^p$ in a ring containing $\mathbb{F}_p$. As $\alpha^q = \alpha\ \forall \alpha \in \mathbb{F}_q$, the maps φ_q and $\varphi_q - id : a \longmapsto a^q - a$ are $\mathbb{F}_q$-linear.

Special case: $f = f_1 \cdots f_r$, $f_i \in \mathbb{F}_q[X]$ distinct (monic) irreducible polynomials,

$$A = \mathbb{F}_q[X]/(f) \xrightarrow{\sim} \prod_{i=1}^{r} \underbrace{\mathbb{F}_q[X]/(f_i)}_{\text{field } \mathbb{F}_{q^{d_i}}}, \quad d_i = \deg(f_i)$$

$$\operatorname{Ker}\left(A \xrightarrow{\varphi_q - id} A\right) = A^{\varphi_q = id} \xrightarrow{\sim} \prod_{i=1}^{r} \underbrace{\{\alpha \in \mathbb{F}_{q^{d_i}} \mid \alpha^q = \alpha\}}_{\mathbb{F}_q} = \prod_{i=1}^{r} \mathbb{F}_q \Rightarrow \boxed{\dim_{\mathbb{F}_q}\left(A^{\varphi_q = id}\right) = r}$$

In particular, a separable polynomial $f \in \mathbb{F}_q[X] \setminus \mathbb{F}_q$ is irreducible $\Longleftrightarrow$

$\Longleftrightarrow r = 1 \Longleftrightarrow \dim_{\mathbb{F}_q} \operatorname{Ker}\left(\mathbb{F}_q[X]/(f) \xrightarrow{\varphi_q - id} \mathbb{F}_q[X]/(f)\right)$.

Factorisation algorithm: given $f \in \mathbb{F}_q[X] \setminus \mathbb{F}_q$ such that $\gcd(f, f') = 1$,

a) write down the matrix M of $\varphi_q - id : \mathbb{F}_q[X]/(f) \longrightarrow \mathbb{F}_q[X]/(f)$ in the basis $1, \overline{X}, \ldots, \overline{X}^{d-1}$ ($d = \deg(f)$).

b) compute $\operatorname{Ker}(M) = \left\{ \begin{pmatrix} a_0 \\ \vdots \\ a_{d-1} \end{pmatrix} \in \mathbb{F}_q^d \;\middle|\; M \begin{pmatrix} a_0 \\ \vdots \\ a_{d-1} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \right\} \subset \mathbb{F}_q^d \left(\operatorname{Ker}(M) \supset \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \right)$.

(c) If $\dim_{\mathbb{F}_q}(M) = 1 \Longrightarrow f$ irreducible.

(d) If not, then $a = \begin{pmatrix} a_0 \\ \vdots \\ a_{d-1} \end{pmatrix} \in \operatorname{Ker}(M) \setminus \mathbb{F}_q \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ gives $h(X) = a_0 + a_1 X + \cdots + a_{d-1} X^{d-1} \in \mathbb{F}_q[X]$ ($\deg(h) < d$)

such that $f \mid (h^q - h) = \prod_{b \in \mathbb{F}_q} (h - b)$

(e) $\gcd(\underbrace{h-b}_{\deg < \deg(f)}, h-b') = 1$ if $b \neq b' \Longrightarrow$ non-trivial factorisation in $\mathbb{F}_q[X]$ $f = \prod_{b \in \mathbb{F}_q} \gcd(f, h-b)$

---

(3) **Factorisation of polynomials in $\mathbb{Z}[X]$**: Berlekamp's algorithm for reductions (mod p) for several primes p + Chinese Remainder Theorem

Irreducibility criteria

Def: let A = UFD, $K = \mathrm{Frac}(A)$ (ex: $A=\mathbb{Z}$, $K=\mathbb{Q}$). The content of $f \in A[X]\setminus\{0\}$ is the $\gcd(\text{coefficients of } f) = ct(f) \in (A\setminus\{0\})/A^*$.
The content of $g \in K[X]\setminus\{0\}$ is $ct(ag)/a \in (K\setminus\{0\})/A^* = K^*/A^*$, for any $a \in A\setminus\{0\}$ such that $ag \in A[X]$.

Lemma (Gauss). $f, g \in K[X]\setminus\{0\} \Rightarrow \boxed{ct(fg) = ct(f)\,ct(g)}$

Pf. Replace f, g by $f/ct(f)$, $g/ct(g)$; then $f, g \in A[X]\setminus\{0\}$, $ct(f)=ct(g)=1$.
Write $f = \sum a_i X^i$, $g = \sum b_j X^j$, $fg = \sum c_k X^k$, $c_k = \sum_{i+j=k} a_i b_j$. If $\pi \in A$ irreducible
$\Rightarrow \exists\, i_0 = \min\{i \mid \pi \nmid a_i\}$, $\exists\, j_0 = \min\{j \mid \pi \nmid b_j\}$

$$c_{\underbrace{i_0+j_0}_{k}} = \underbrace{a_{i_0} b_{j_0}}_{\pi \nmid a_{i_0} b_{i_0}} + \underbrace{\sum_{i<i_0} a_i b_{k-i} + \sum_{j<j_0} a_{k-j} b_j}_{\text{divisible by } \pi} \Rightarrow \pi \nmid c_k \Rightarrow \pi \nmid ct(fg) \Rightarrow ct(fg) = 1.$$

Note: $ct(f) \in A \iff f \in A[X]\setminus\{0\}$

Cor. If A = UFD, $K = \mathrm{Frac}(A)$, $f \in A[X]$, $f = gh$, $g, h \in K[X]\setminus K$
$\Rightarrow \exists\, g_1, h_1 \in A[X]\setminus A$ $\quad f = g_1 h_1$

Pf: Take $g_1 = g/ct(g)$, $h_1 = h\,ct(g)$; $ct(g_1) = 1 \Rightarrow g_1 \in A[X]$,
$ct(h_1) = ct(f/g)\,ct(g) = ct(f) \in A \Rightarrow h_1 \in A[X]$.

Thm (Eisenstein's irreducibility criterion). If A = UFD, $\pi \in A$ irreducible,
$f = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \in A[X]$, $\forall i = 0, \dots, n-1$ $\pi \mid a_i$, $\pi^2 \nmid a_0$
$\Rightarrow f \neq gh$, $g, h \in A[X]\setminus A$. [Works if A = any domain, P = prime ideal of A, $a_0, \dots, a_{n-1} \in P$, $a_0 \notin P^2$.]

Pf: If $f = gh$, can assume g, h monic, $\deg(g) = r < n$, $\deg(h) = n-r < n$.
$\overline{f} = \overline{gh} = f \pmod{\pi} = X^n \in \underbrace{(A/\pi A)}_{\text{domain}}[X] \subset \underbrace{\mathrm{Frac}(A/\pi A)}_{\text{UFD}}[X] \Rightarrow \overline{g} = X^r$, $\overline{h} = X^{n-r}$

$g = X^r + b_{r-1}X^{r-1} + \cdots + b_0$, $h = X^{n-r} + c_{n-r-1}X^{n-r-1} + \cdots + c_0$, $\forall i,j$ $\pi \mid b_i, c_j$
$\Rightarrow \pi^2 \mid \underbrace{b_0 c_0}_{a_0}$ — contradiction.

Cor: If A = UFD, $\pi \in A$ irreducible, $f = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ ($n \geq 1$), $\forall i$ $\pi \mid a_i$, $\pi^2 \nmid a_0$
("f is an Eisenstein polynomial with respect to π")
$\Rightarrow$ f is irreducible in $K[X]$ $\quad (K = \mathrm{Frac}(A))$.

Ex: $A = \mathbb{Z}$, $K = \mathbb{Q}$, $\pi = p$ prime, $f = X^n - a$, $a \in \mathbb{Z}$, $p \mid a$, $p^2 \nmid a$.

Rmk: Gauss's lemma implies that [A UFD $\Rightarrow A[X]$ UFD, hence $A[X_1, \dots, X_n]$ UFD $\forall n \geq 1$]

The regular representation, trace, norm

Assume: $A \subset B$ rings, B = free A-module of rank $= n < \infty$

$(B \neq Ab_1 \oplus \cdots \oplus Ab_n = \{b = \sum_{i=1}^{n} a_i b_i \mid a_i \in A$ uniquely determined by $b\}$

($b_1, \dots, b_n$: basis of B over A)

Def. The regular representation $M : B \longrightarrow M_n(A)$ with respect to the basis $\{b_i\}$ attaches to $b \in B$ the matrix $M(b) \in M_n(A)$ given by $b(b_1, \dots, b_n) = (b_1, \dots, b_n) M(b)$

Ex: $\Delta \in \mathbb{Q}$, $\sqrt{\Delta} \notin \mathbb{Q}$, $A = \mathbb{Q}$, $B = \mathbb{Q}(\sqrt{\Delta})$, $b_1 = 1$, $b_2 = \sqrt{\Delta}$, $b = u + v\sqrt{\Delta}$, $u, v \in \mathbb{Q}$

$(u+v\sqrt{\Delta})(1, \sqrt{\Delta}) = (u+v\sqrt{\Delta}, v\Delta + u\sqrt{\Delta}) = (1, \sqrt{\Delta}) \begin{pmatrix} u & \Delta v \\ v & u \end{pmatrix}$, $\boxed{M(u+v\sqrt{\Delta}) = \begin{pmatrix} u & \Delta v \\ v & u \end{pmatrix}}$

Properties: (1) $M(b+b') = M(b) + M(b')$, $M(bb') = M(b)M(b')$, $\forall a \in A$ $M(a) = a \cdot I_n$

$\Rightarrow$ M is a morphism of A-algebras

(2) $\operatorname{Ker}(M) = 0$ (if $bb_i = 0$ $\forall i$ $\longrightarrow$ $\forall b' \in B$ $bb' = 0 \Longrightarrow b \cdot 1 = 0$)

$\Rightarrow$ $M : B \hookrightarrow M_n(A)$ is injective

Change of basis: $(b_1, \dots, b_n) = (b'_1, \dots, b'_n) g$, $g \in GL_n(A)$

$b(b'_1, \dots, b'_n) = (b'_1, \dots, b'_n) M'(b) \Longrightarrow M'(b) = g\, M(b)\, g^{-1}$

Def. the characteristic polynomial $P_{B/A,b}(X) = \det(X \cdot I_n - M(b)) \in A[X]$ (monic)

($b \in B$) the trace $\operatorname{Tr}_{B/A}(b) = \operatorname{Tr}(M(b)) \in A$ (do not depend on $\{b_i\}$)

the norm $N_{B/A}(b) = \det(M(b)) \in A$

Properties: (1) $P_{B/A,b}(b) = 0$ $\left(\overset{\operatorname{Ker}(M)=0}{\Longleftarrow} M(P_{B/A,b}(b)) = P_{B/A,b}(M(b)) = 0\right)$

Cayley–Hamilton

Exercise. The Cayley–Hamilton Thm is usually proved for matrices over a field (say, over $\mathbb{C}$). Why does it imply the corresponding statement for matrices over an arbitrary ring?

---

(2) $b = a \in A \Longrightarrow P_{B/A,a}(X) = (X-a)^2$, $\operatorname{Tr}_{B/A}(a) = na$, $N_{B/A}(a) = a^n$

($M(a) = a \cdot I_n$)

---

(3) $\operatorname{Tr}_{B/A}(b+b') = \operatorname{Tr}_{B/A}(b) + \operatorname{Tr}_{B/A}(b')$, $N_{B/A}(bb') = N_{B/A}(b)\, N_{B/A}(b')$

($\Longrightarrow N_{B/A}(B^*) \subset A^*$)

---

(4) If $f = X^n + a_1 X^{n-1} + \cdots + a_n \in A[X]$ (monic), $B = A[X]/(f)$, $\{b_i\} = \{1, \overline{X}, \dots, \overline{X}^{n-1}\}$

$\Rightarrow$ $M(\overline{X}) = \begin{pmatrix} 0 & & & -a_n \\ 1 & 0 & & \vdots \\ & 1 & \ddots & \vdots \\ & & 1 & -a_1 \end{pmatrix}$, $P_{B/A,\overline{X}}(T) = \det(T \cdot I_n - M(\overline{X})) = f(T)$

---

(5) $A \subset B \subset C$ (B free over A, C free over B (of finite rank))

$\Rightarrow$ $\operatorname{Tr}_{C/A} = \operatorname{Tr}_{B/A} \circ \operatorname{Tr}_{C/B}$ (easy); $N_{C/A} = N_{B/A} \circ N_{C/B}$ (exercise)

Prop. (Characteristic polynomial and the minimal polynomial)
$K \subset L$ fields, $[L:K] < \infty$, $\alpha \in L$, $f \in K[X]$ the minimal polynomial of α over K $\Longrightarrow$ $\boxed{P_{L/K,\alpha}(X) = f(X)^{[L:K(\alpha)]}}$

Pf: $n = [L:K] = \underbrace{[L:K(\alpha)]}_{m}\,\underbrace{[K(\alpha):K]}_{d}$ $\qquad d = \deg(f)$, $\quad f = X^d + a_1 X^{d-1} + \cdots + a_d \in K[X]$

$1, \alpha, \ldots, \alpha^{d-1}$ basis of $K(\alpha)/K$
$\beta_1, \ldots, \beta_m$ —— " —— $L/K(\alpha)$
$\Big\} \Longrightarrow \{\alpha^i \beta_j\}_{0 \le i < d,\ 1 \le j \le m}$ basis of L/K

In this basis $M(\alpha) = \begin{pmatrix} M & & \\ & \ddots & \\ & & M \end{pmatrix}$ } m blocks, $M \in M_d(K)$ the matrix of multiplication by α in the basis $\{\alpha^i\}$

M = as in (4) above $\Longrightarrow \det(X \cdot I_d - M) = f \Longrightarrow \det(X \cdot I_n - M(\alpha)) = f^m$.

Prop (Integral closure and the characteristic/minimal polynomials).
A = integrally closed domain (ex: $A = \mathbb{Z}$), $K = \mathrm{Frac}(A)$ (ex: $K = \mathbb{Q}$),
$L \supset K$ field, $[L:K] < \infty$, $\alpha \in L$ ($\Rightarrow$ algebraic over K). It is equivalent:
(1) α is integral over A $\Longleftrightarrow$ (2) $P_{L/K,\alpha}(X) \in A[X]$ $\Longleftrightarrow$ (3) $f(X) \in A[X]$ (the minimal pol. of α over K)

Pf: (3) $\Longrightarrow$ (2) (since $P = f^m$), (2) $\Longrightarrow$ (1) (since $P(\alpha) = 0$, P monic)
(1) $\Longrightarrow$ (3): if α integral over $A \Rightarrow \exists\, g \in A[X]$ monic, $g(\alpha) = 0$; $\exists$ field $M \supset L$
$f(X) = \prod_{i=1}^{d} (X - \alpha_i)$, $\alpha_1 = \alpha$, $\forall i\ \alpha_i \in M$. As $g(\alpha) = 0 \Rightarrow f \mid g$ in $K[X] \Rightarrow$
$\forall i\ \ g(\alpha_i) = 0 \Rightarrow$ each α_i is integral over A
(Each coefficient of f) $\in \mathbb{Z}[\alpha_1, \ldots, \alpha_d] \cap K \subset$ (integral closure of A in K) $= A$.

Cor1. If α is integral over A (and A integrally closed) $\Rightarrow \mathrm{Tr}_{L/K}(\alpha),\ N_{L/K}(\alpha) \in A$

Cor2 If $[L:\mathbb{Q}] < \infty$, then $\mathcal{O}_L = \{\alpha \in L \mid P_{L/\mathbb{Q},\alpha}(X) \in \mathbb{Z}[X]\}$ $\quad (A = \mathbb{Z},\ K = \mathbb{Q})$.

Ex.: $[L:\mathbb{Q}] = 2$ (quadratic field) $\exists!\ d \in \mathbb{Z} \setminus \{0,1\}$ square-free $L = \mathbb{Q}(\sqrt{d})$
$\alpha = u + v\sqrt{d} \in L$, $u, v \in \mathbb{Q}$. So: $P_{L/\mathbb{Q},\alpha}(X) = \det\left(X \cdot I_2 - \begin{pmatrix} u & dv \\ v & u \end{pmatrix}\right) = X^2 - \underbrace{2u}_{\mathrm{Tr}(\alpha)} X + \underbrace{(u^2 - dv^2)}_{N(\alpha)}$
$\alpha \in \mathcal{O}_L \Longleftrightarrow 2u,\ u^2 - dv^2 \in \mathbb{Z} \Longleftrightarrow$
$\begin{cases} u \in \mathbb{Z},\ dv^2 \in \mathbb{Z} \Longleftrightarrow u, v^2 \in \mathbb{Z} \Longleftrightarrow u, v \in \mathbb{Z} \\ u \in \mathbb{Z} + \frac{1}{2}\ (\Rightarrow u^2 \in \mathbb{Z} + \frac{1}{4}),\ 4dv^2 \in (4\mathbb{Z}+1) \Longleftrightarrow 2u \in 2\mathbb{Z}+1 \\ \qquad\qquad\qquad\qquad\qquad\qquad (2v)^2 \in 2\mathbb{Z}+1 \\ \qquad\qquad\qquad\qquad\qquad\qquad d \in 4\mathbb{Z}+1 \end{cases}$

Conclusion: $\mathcal{O}_L = \begin{cases} \mathbb{Z} \cdot 1 + \mathbb{Z} \cdot \frac{1+\sqrt{d}}{2}, & d \equiv 1 \pmod 4 \\ \mathbb{Z} \cdot 1 + \mathbb{Z} \cdot \sqrt{d}, & d \equiv 2, 3 \pmod 4 \end{cases}$

Cor3. If α is integral over A (and A integrally closed) $\Longrightarrow \alpha \mid N_{L/K}(\alpha)$ in $A[\alpha]$

Pf: $0 = P_{L/K,\alpha}(\alpha) = \underbrace{\alpha^n + a_1 \alpha^{n-1} + \cdots + a_{n-1}\alpha}_{\cdot \alpha \beta,\ \beta \in A[\alpha]} + (-1)^n N_{L/K}(\alpha)$.

Discriminants

Discriminant of a monic polynomial: R = any ring (commutative), $n \geq 1$;

the symmetric group S_n acts on the polynomial ring $R[x_1, \dots, x_n]$ by $(\tau * f)(x_1, \dots, x_n) = f(x_{\tau(1)}, \dots, x_{\tau(n)})$ (for any permutation τ of $\{1, 2, \dots, n\}$).

The ring of **symmetric polynomials** $R[x_1, \dots, x_n]^{S_n} = \{f \mid \tau * f = f \ \forall \tau \in S_n\}$ is equal to $R[\sigma_1, \dots, \sigma_n]$, where $\sigma_k = \sum_{1 \leq i_1 < \dots < i_k \leq n} x_{i_1} \cdots x_{i_k}$ are the **elementary symmetric functions**. They satisfy

$$f(T) = (T - x_1) \cdots (T - x_n) = T^n - \sigma_1 T^{n-1} + \sigma_2 T^{n-2} - \cdots + (-1)^n \sigma_n = T^n + a_1 T^{n-1} + \cdots + a_n.$$

($n \geq 2$) The polynomial $\Delta = \prod_{1 \leq i < j \leq n} (x_i - x_j) \in \mathbb{Z}[x_1, \dots, x_n]$ satisfies

$$\forall \tau \in S_n \quad \tau(\Delta) = \underbrace{\operatorname{sgn}(\tau)}_{\pm 1} \Delta$$

the sign of the permutation τ

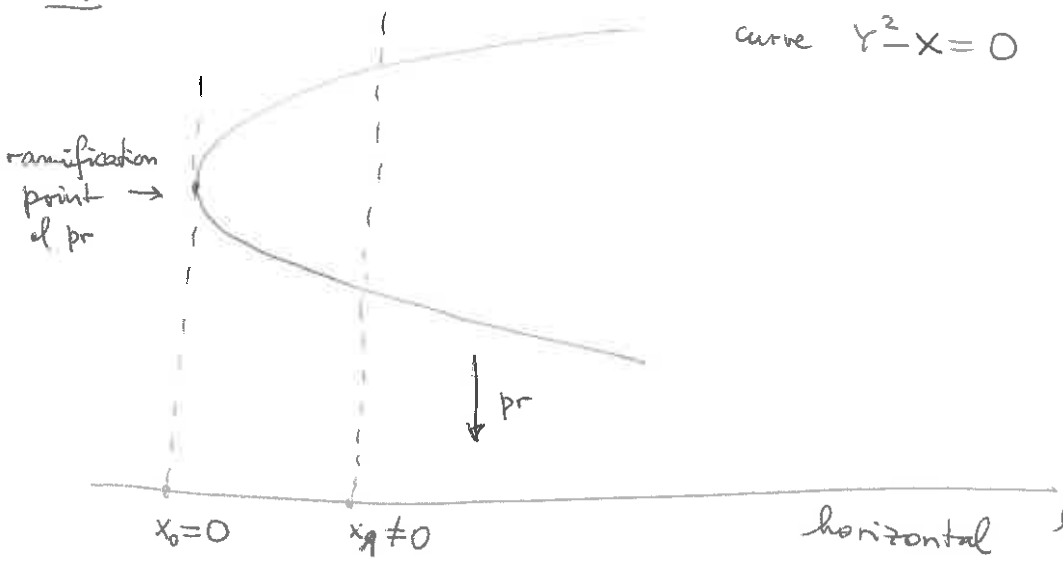
$\Rightarrow \exists!$ $\operatorname{disc}(f) \in \mathbb{Z}[a_1, \dots, a_n]$ ($a_k = (-1)^k \sigma_k$) equal to Δ^2.

Ex: ($n = 2$) $\operatorname{disc}(T^2 + a_1 T + a_2) = (x_1 - x_2)^2 = (x_1 + x_2)^2 - 4 x_1 x_2 = \sigma_1^2 - 4\sigma_2 = a_1^2 - 4a_2$

Why do we care about discriminants?

$\operatorname{disc}(f) \neq 0 \iff f$ has distinct roots ($f \in K[T]$, K field)

Ex:



$$\operatorname{disc}(Y^2 - x_i) = 4x_i \begin{cases} = 0 & i = 0 \\ \neq 0 & i = 1 \end{cases}$$

The trace form and the general discriminants

Given: $A \subset B$ rings, B = free A-module of rank $n < \infty$

Fix a basis of B over A: $(B,+) = Ab_1 \oplus \cdots \oplus Ab_n$

Def (1) the **trace form** of B over A is $T: B \times B \longrightarrow A$, $(x,y) \longmapsto Tr_{B/A}(xy)$

T is A-bilinear and symmetric

(2) The **matrix of T** in the basis $\{b_i\}$ is $M = {}^tM = (Tr_{B/A}(b_i b_j))_{1 \le i,j \le n} \in M_n(A)$

If we identify $B \xrightarrow{\sim} A^n$, $x = \sum_{i=1}^n x_i b_i \longmapsto x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$, then $T(x,y) = {}^t x M y$

(3) The **discriminant** of the form T in the basis $\{b_i\}$ is

$D_B(b_1, \cdots, b_n) = \det(M) \in A$.

(4) **Change of basis**: $(b_1, \cdots, b_n) = (b'_1, \cdots, b'_n)g$, $g \in GL_n(A)$

$M = {}^t g M' g$, $\det(M) = \det(M') \underbrace{\det(g)^2}_{\in A^{*2}}$

(5) the **discriminant of B over A**: $\underbrace{D(\text{any basis of } B \text{ over } A)}_{D_{B/A}} \in A/A^{*2}$

Ex: $A = \mathbb{Z}$, $\mathbb{Z}^* = \{\pm 1\}$, $\mathbb{Z}^{*2} = \{1\} \Longrightarrow D_{B/\mathbb{Z}} \in \mathbb{Z}$ well-defined.

Def. If $A = K$ field, $B \supset K$ ring (commutative), $\dim_K(B) = n < \infty$, we say that

B/K is **separable** $\Longleftrightarrow$ $D_{B/K} \neq 0$

$\Longleftrightarrow$ $T: B \times B \longrightarrow K$ is **non-degenerate**:

$\forall\, x \in B - \{0\}$ $\exists\, y \in B$ $Tr_{B/A}(xy) \neq 0$

If $B = L \supset K$ field, $\Longleftrightarrow$ $Tr_{L/K}(L) \neq \{0\}$

[if $Tr_{L/K}(\alpha) \neq 0$, then $Tr_{L/K}(x \cdot (x^{-1}\alpha)) \neq 0$]

Note: If $\mathbb{Q} \subset K \subset L$ fields, $[L:K] < \infty \Longrightarrow$ **L/K separable**

(since $Tr_{L/K}(1) = [L:K] \cdot 1 \neq 0 \in \mathbb{Q} \subset K$)

Thm. If $L \supset \mathbb{Q}$ field, $[L:\mathbb{Q}] = n < \infty \Longrightarrow (\mathcal{O}_L, +) \simeq \mathbb{Z}^n$.

Pf. $\exists$ basis $L = \mathbb{Q}b_1 \oplus \cdots \oplus \mathbb{Q}b_n$ with $b_i \in \mathcal{O}_L$; $M = (Tr_{L/\mathbb{Q}}(b_i b_j)) \in M_n(\mathbb{Z})$,

$d = \det(M) \neq 0$ $(d \in \mathbb{Z})$; $\forall\, b \in \mathcal{O}_L$ $b = \sum_{i=1}^n \lambda_i b_i$, $\lambda_i \in \mathbb{Q}$, $Tr_{L/\mathbb{Q}}(b b_j) = \sum_i M_{ij} \lambda_i \in \mathbb{Z}$

$M \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} \in \mathbb{Z}^n \xrightarrow[\text{rule}]{\text{Cramer's}} \det(M) \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} \in \mathbb{Z}^n \Longrightarrow \forall i\ \lambda_i \in d^{-1}\mathbb{Z}$. So

$\bigoplus_1^n \mathbb{Z} b_i \supset \mathcal{O}_k \supset \bigoplus_1^n \mathbb{Z} \frac{b_i}{d}$ $\Longrightarrow$ $\mathcal{O}_L \simeq \mathbb{Z}^n$.

$$\boxed{\operatorname{disc}(f) = D(1, \alpha, \dots, \alpha^{n-1})}$$

Back to regular representation: (1) If $B = A (= A b_1$ for any $b_1 \in A^*)$, then $M : A \longrightarrow M_1(A) = A$ is the identity map, $M(a) = a$.

(2) If $B = A \times A \times \cdots \times A$ (n times) $= \bigoplus_{i=1}^{n} A e_i$, $e_i = (0, \dots, \underbrace{1}_{i\text{-th place}}, 0, \dots, 0)$, then $M(a_1, \dots, a_n) = \begin{pmatrix} a_1 & & \\ & \ddots & \\ & & a_n \end{pmatrix}$

Back to separable monic polynomials:

(3) K = field, $f \in K[X]$ monic, $\deg(f) = n \geq 1$, f has n distinct roots $\alpha_1, \dots, \alpha_n \in \underbrace{K'}_{\text{field}} > K$

We can consider the regular representation M for the pairs $K \subset K[X]/(f)$ and $K' \subset K'[X]/(f)$ with respect to the basis $1, \overline{X}, \dots, \overline{X}^{n-1}$

Lagrange interpolation: $f(X) = \prod_{i=1}^{n} (X - \alpha_i)$

$$K'[X]/(f) \xrightarrow{\sim} \prod_{i=1}^{n} K'[X]/(X-\alpha_i) \xrightarrow{(\mathrm{ev}_{\alpha_i})} \prod_{i=1}^{n} K'$$

$$\overline{h(X)} \longmapsto (h(\alpha_1), \dots, h(\alpha_n))$$

$$\frac{1}{f'(\alpha_i)} \frac{f(X)}{X - \alpha_i} \longmapsto e_i = (0, \dots, 1, \dots, 0)$$

If $g \in GL_n(K')$ is the base change matrix between the bases $\{\overline{X}^{i-1}\}_{1 \leq i \leq n}$ and $\left\{ \frac{1}{f'(\alpha_i)} \frac{f(X)}{X - \alpha_i} \right\}_{1 \leq i \leq n}$, then

$$\forall h \in K[X] \qquad g\, M(\overline{h(X)})\, g^{-1} = \begin{pmatrix} h(\alpha_1) & & \\ & \ddots & \\ & & h(\alpha_n) \end{pmatrix}, \text{ by (2).}$$

(4) $\forall h \in K[X]$ $\quad P_{K[X]/(f),\, \overline{h(X)}}(T) = \prod_{i=1}^{n} (T - h(\alpha_i))$, $\quad \operatorname{Tr}_{(K[X]/f)/K}(\overline{h(X)}) = \sum_{i=1}^{n} h(\alpha_i)$,

(5) $N_{(K[X]/(f))/K}(\overline{f'(X)}) = \prod_{i=1}^{n} f'(\alpha_i) = \prod_{i=1}^{n} \prod_{j \neq i} (\alpha_i - \alpha_j) =$ $\boxed{N_{(K[X]/(f))/K}(\overline{h(X)}) = \prod_{i=1}^{n} h(\alpha_i)}$.

$$= (-1)^{1+2+\cdots+(n-1)} \prod_{i<j} (\alpha_i - \alpha_j)^2 = (-1)^{n(n-1)/2} \operatorname{disc}(f)$$

Ex: $n = 3$, $f(X) = X^3 + aX + b$, $f'(X) = 3X^2 + a$; basis $1, \overline{X}, \overline{X}^2$ of $K[X]/(f)$,

$\overline{X}^3 + a\overline{X} + b = 0$, $(1, \overline{X}, \overline{X}^2) M(3\overline{X}^2 + a) = (3\overline{X}^2 + a,\ \underbrace{3\overline{X}^3 + a\overline{X}}_{-2a\overline{X} - 3b},\ \underbrace{3\overline{X}^4 + a\overline{X}^2}_{-2a\overline{X}^2 - 3b\overline{X}})$

$$M(3\overline{X}^2 + a) = \begin{pmatrix} a & -3b & 0 \\ 0 & -2a & -3b \\ 3 & 0 & -2a \end{pmatrix}$$

$(-1)^{3-2/2} \operatorname{disc}(f) = \det = 4a^3 + 27b^2 \Longrightarrow \operatorname{disc}(X^3 + aX + b) = -4a^3 - 27b^2$

Exercice: Compute $\operatorname{disc}(X^n + aX + b)$ $(n \geq 2)$

(6) The matrix entries of $M = \left(\operatorname{Tr}_{(K[X]/(f))/K} (\overline{X}^i \overline{X}^j) \right)_{1 \leq i,j \leq n}$ ($\det(M) = D(1, \overline{X}, \dots, \overline{X}^{n-1})$) are $M_{ij} \overset{(4)}{=} \sum_{k=1}^{n} \alpha_k^{i+j} = \sum_{k=1}^{n} N_{ik} N_{jk}$, $N_{ik} = \alpha_k^i$, $N = (N_{ij}) \in M_n(K')$

$\Rightarrow M = N\, {}^t N$, $\det(M) = \det(N)^2$

But $\det(N) = \pm \prod_{i<j} (\alpha_i - \alpha_j)$ (Vandermonde's determinant)

$$\Rightarrow \boxed{D(1, \overline{X}, \dots, \overline{X}^{n-1}) = \operatorname{disc}(f)}$$

Prop. Let A be any ring (commutative), $f \in A[X]$ monic, $\deg(f) = n \geq 2$, $B = A[X]/(f) \ni \alpha = \overline{X}$ ($\Rightarrow f(\alpha) = 0$). Then:

$$N_{B/A}(f'(\alpha)) = (-1)^{n(n-1)/2} \operatorname{disc}(f), \quad D(1, \alpha, \dots, \alpha^{n-1}) = \operatorname{disc}(f).$$

Pf. It is sufficient to establish these polynomial identities in the universal case, when $f(X) = \prod_{i=1}^{n}(X - x_i)$, $x_1, \dots, x_n$ independent variables, $A = \mathbb{Z}[x_1, \dots, x_n]^{S_n} = \mathbb{Z}[a_1, \dots, a_n] \subset K = \operatorname{Frac}(A) = \mathbb{Q}(x_1, \dots, x_n)$ (field of rational functions), in which case we app. (5), (6). [redacted].

Determining $\mathcal{O}_L$ ($[L:\mathbb{Q}] < \infty$)

Prop: If $\mathbb{Z} \subset B_1 \subset B_2$ are rings such that $(B_i, +) \simeq \mathbb{Z}^n$, then $(B_2 : B_1) < \infty$ and

$$\boxed{D_{B_1/\mathbb{Z}} = (B_2 : B_1)^2 D_{B_2/\mathbb{Z}}}$$

Cor. If $D_{B_1/\mathbb{Z}} \in \mathbb{Z}_{>0}$ and is square-free, then $B_1 = B_2$.

Pf of Prop: Thm on elementary divisors $\Rightarrow \exists$ bases

$(B_2, +) = \mathbb{Z} b_1 \oplus \cdots \oplus \mathbb{Z} b_n$, $(B_1, +) = \mathbb{Z} \underbrace{d_1 b_1}_{b_1'} \oplus \cdots \oplus \mathbb{Z} \underbrace{d_n b_n}_{b_n'}$ $\quad d_i \in \mathbb{Z}_{>0}$, $(B_2 : B_1) = d_1 \cdots d_n$

$\forall b \in B_1$

$$g = \begin{pmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_n \end{pmatrix}$$

$$\begin{array}{ccc} B_1 & \xrightarrow{M} & M_n(A) \ni M' \\ \cap & & \downarrow \quad \downarrow \\ B_2 & \xrightarrow{M} & M_n(A) \ni g M' g^{-1} \end{array}$$

in the basis $\{b_i'\}$

— " — $\{b_i\}$

$$\Rightarrow \operatorname{Tr}_{B_1/\mathbb{Z}}(b) = \operatorname{Tr}_{B_2/\mathbb{Z}}(b)$$

$$D_{B_1/\mathbb{Z}} = \det\Big(\underbrace{\operatorname{Tr}_{B_1/\mathbb{Z}}(d_i b_i, d_j b_j)}_{d_i d_j \operatorname{Tr}_{B_2/\mathbb{Z}}(b_i, b_j)} \Big) = \underbrace{(d_1 \cdots d_n)^2}_{(B_2 : B_1)^2} \underbrace{\det(\operatorname{Tr}_{B_2/\mathbb{Z}}(b_i, b_j))}_{D_{B_2/\mathbb{Z}}}$$

Special case: if $L \supset \mathbb{Q}$ field, $[L:\mathbb{Q}] = n < \infty$, $(\mathcal{O}_L, +) \simeq \mathbb{Z}^n$

$D_L = D_{\mathcal{O}_L/\mathbb{Z}} \in \mathbb{Z}_{\neq 0}$. So if $B \subset \mathcal{O}_L$ subring, $(\mathcal{O}_L : B) < \infty \Rightarrow$ $\boxed{D_{B/\mathbb{Z}} = (\mathcal{O}_L : B)^2 D_L}$

Examples: (1) If $\alpha \in \mathcal{O}_L$, $L = \mathbb{Q}(\alpha) \Rightarrow B = \mathbb{Z}[\alpha] \subset \mathcal{O}_L$, $(\mathcal{O}_L : \mathbb{Z}[\alpha]) < \infty$,

$D_{\mathbb{Z}[\alpha]/\mathbb{Z}} = \operatorname{disc}(f)$, $f \in \mathbb{Z}[X]$ the minimal polynomial of α over $\mathbb{Q}$

$$\Rightarrow \quad \boxed{\operatorname{disc}(f) = (\mathcal{O}_L : \mathbb{Z}[\alpha])^2 D_L} \quad (\in \mathbb{Z}_{\neq 0})$$

Cor: If $\operatorname{disc}(f)$ is square-free $\Rightarrow \mathcal{O}_L = \mathbb{Z}[\alpha]$, $D_L = \operatorname{disc}(f)$.

(2) $f(X) = X^3 \pm X + 1$ irreducible over $\mathbb{Q}$ (exercise)

$$\operatorname{disc}(f) = -4(\pm 1)^3 - 27 \cdot 1^2 = \begin{cases} -31 \\ -23 \end{cases}$$

So: if $\alpha^3 \pm \alpha + 1 = 0$, $L = \mathbb{Q}(\alpha) \Rightarrow \mathcal{O}_L = \mathbb{Z}[\alpha]$, $D_L = \begin{cases} -31 \\ -23 \end{cases}$.

What if $B \subset \mathcal{O}_L$, $D_{B/\mathbb{Z}} \neq$ square-free?

Recall: (1) A = ring, $I \subset A$ ideal, the **radical of I** is the ideal $\sqrt{I} = \{a \in A \mid \exists n \geq 1 \; a^n \in I\}$

(2) the **nilradical of A** is $\mathrm{Nil}(A) = \sqrt{(0)} = \{a \in A \mid \exists n \geq 0 \; a^n = 0\}$; $\mathrm{Nil}(A/I) = \sqrt{I}/I$.

(3) the **reduced ring** attached to A is $A^{red} = A/\mathrm{Nil}(A)$ ($\Rightarrow \mathrm{Nil}(A^{red}) = 0$)

Ex: $\mathrm{Nil}(\mathbb{Z}/12\mathbb{Z}) = 6\mathbb{Z}/12\mathbb{Z}$, $\mathrm{Nil}(\mathbb{C}[X]/(X^3 - X^2)) = (X(X-1))$

Situation: $L \supset \mathbb{Q}$ field, $[L:\mathbb{Q}] = n < \infty$, $B \subset \mathcal{O}_L$, $(\mathcal{O}_L : B) < \infty$

($\Leftrightarrow$ $B \subset L$ subring, $(B,+) \simeq \mathbb{Z}^n$), p prime, $p^2 \mid D_{B/\mathbb{Z}} = (\mathcal{O}_L : B)^2 D_L$

Question: does $p \mid (\mathcal{O}_L : B)$? ($\Leftrightarrow$ is there $x \in B$, $\frac{x}{p} \in \mathcal{O}_L$, $\frac{x}{p} \notin B$?)

Prop. Consider

$$\begin{array}{ccc} \mathrm{Nil}(B/pB) & \subset & B/pB \\ \uparrow & & \uparrow \mathrm{pr} \\ N = \mathrm{pr}^{-1}(\mathrm{Nil}(B/pB)) & \subset & B \end{array} \qquad \text{(ideal in } B \text{ containing } pB\text{)}$$

and the ring morphism $m : B/pB \longrightarrow \mathrm{End}_{B/pB}(N/pN)$ ← {B/pB-linear maps from N/pN to N/pN}

$$\begin{array}{ccc} \downarrow & & \downarrow \\ y & \longmapsto & (n \longmapsto yn) \end{array}$$

Then: $\boxed{\mathrm{Ker}(m) = (B \cap p\mathcal{O}_L)/pB}$

Cor. (1) $\mathrm{Ker}(m) = 0 \Leftrightarrow B \cap p\mathcal{O}_L = pB \Leftrightarrow p \nmid (\mathcal{O}_L : B)$.

(2) If $x \in B$, $m(\underbrace{x \pmod{pB}}_{\neq 0 \in B/pB}) = 0 \Rightarrow \frac{x}{p} \in \mathcal{O}_L$, $\frac{x}{p} \notin B$

Ex (Eisenstein case): $L = \mathbb{Q}(\alpha) = \mathbb{Q}[X]/(f)$, $f = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{Z}[X]$,

p prime, $\forall i$ $p \mid a_i$, $p^2 \nmid a_0$, $B = \mathbb{Z}[\alpha] = \mathbb{Z}[X]/(f) = \mathbb{Z}[X]/f\mathbb{Z}[X] = \bigoplus_{i=0}^{n-1} \mathbb{Z} \cdot \overline{X}^i$

$B/pB = \mathbb{F}_p[X]/(X^n) \supset \mathrm{Nil}(B/pB) = X\mathbb{F}_p[X]/X^n\mathbb{F}_p[X]$

$N = \underbrace{\mathbb{Z} \cdot p}_{\beta_1} \oplus \bigoplus_{i=1}^{n-1} \underbrace{\mathbb{Z} \cdot \overline{X}^i}_{\beta_{i+1}}$, $N/pN = \bigoplus_{i=1}^{n} \mathbb{F}_p \cdot \beta_i$, $B/pB = \bigoplus_{i=1}^{n} \mathbb{F}_p \cdot \overline{X}^{i-1}$

$m : B/pB \longrightarrow \mathrm{End}_{B/pB}(N/pN)$ (multiplication map)

$y \longmapsto (n \longmapsto yn)$

Claim: $\mathrm{Ker}(m) = 0$

Pf: $\mathrm{Ker}(m) =$ ideal in $\mathbb{F}_p[X]/(X^n) \Rightarrow \mathrm{Ker}(m) = (\overline{X}^i)$ $(1 \leq i \leq n)$

$(\overline{X}) \supset (\overline{X}^2) \supset \cdots \supset (\overline{X}^{n-1}) \supset (\overline{X}^n) = (0)$. It is enough to show that $m(\overline{X}^{n-1}) \overset{?}{\neq} 0$.

Let $c = a_0/p \pmod p \in \mathbb{F}_p^*$. Then: $\overline{X}^{n-2} \underbrace{\beta_2}_{\overline{X}} = \overline{X}^{n-1} = \beta_n \in N/pN$

$$\overline{X}^{n-1}\beta_2 = \overline{X}\beta_n = \overline{X}^n = \underbrace{-a_{n-1}\overline{X}^{n-1} - \cdots}_{\in pN} - a_0 \pmod{pN} = -c\beta_1 \neq 0 \in N/pN \Rightarrow \mathrm{Ker}(m) = 0.$$

Therefore $p \nmid (\mathcal{O}_L : \mathbb{Z}[\alpha])$ in the Eisenstein case.

Exercise: (1) Let $a \in \mathbb{Z}_{>1}$ be square-free, $L = \mathbb{Q}(\sqrt[3]{a})$. Show that

$$\mathcal{O}_L = \begin{cases} \mathbb{Z}\cdot 1 \oplus \mathbb{Z}\cdot \sqrt[3]{a} \oplus \mathbb{Z}\sqrt[3]{a^2} & \text{if } a \not\equiv \pm 1 \pmod 9 \\ \mathbb{Z}\cdot 1 \oplus \mathbb{Z}\sqrt[3]{a} \oplus \mathbb{Z}\,\dfrac{1 \pm \sqrt[3]{a} + \sqrt[3]{a^2}}{3} & \text{if } a \equiv \pm 1 \pmod 9 \end{cases}$$

(2) If $b \in \mathbb{Z}_{\geq 1}$ is square-free and $\gcd(a,b)=1$, $L' = \mathbb{Q}(\sqrt[3]{ab^2})$, then:

$$\mathcal{O}_{L'} = \begin{cases} \mathbb{Z}\cdot 1 \oplus \mathbb{Z}\cdot \sqrt[3]{ab^2} \oplus \mathbb{Z}\cdot \sqrt[3]{a^2 b} & \text{if } a^{\#} \not\equiv \pm b \pmod 9 \\ \mathbb{Z}\cdot 1 \oplus \mathbb{Z}\cdot \sqrt[3]{ab^2} \oplus \mathbb{Z}\cdot \dfrac{1 + u\sqrt[3]{ab^2} + v\sqrt[3]{a^2 b}}{3} & \text{if } u,v \in \{\pm 1\},\ \begin{matrix} a \equiv u \\ b \equiv v \end{matrix} \pmod 3 \\ & a \equiv \pm b \pmod 9 \quad (v = \pm u) \end{cases}$$

Pf of Prop. We want to show that $\ker(m) \overset{?}{=} (\mathcal{B} \cap p\mathcal{O}_L)/p\mathcal{B}$.

$p\mathcal{B} \subset N \subset \mathcal{B} \Rightarrow N$ = finitely generated abelian group $\Rightarrow \frac{x}{p} \in L$ is an algebraic integer $\Rightarrow \frac{x}{p} \in \mathcal{O}_L$

$(\subseteq)$: if $x \in \mathcal{B}$, $m(x \pmod{p\mathcal{B}}) = 0 \Rightarrow xN \subset pN \Rightarrow \frac{x}{p} N \subset N$

$(\supseteq)$: set $\mathcal{B}' = \{x \in \mathcal{O}_L \mid xN \subset N\} = \{x \in L \mid xN \subset N\}$, $\mathcal{B}'' = \mathcal{O}_L \cap p^{-1}\mathcal{B}$.

If $x \in \mathcal{B} \cap p\mathcal{O}_L \Rightarrow \frac{x}{p} \in \mathcal{B}'' \overset{\text{Lemma below}}{=\!=} \mathcal{B}' \Rightarrow xN \subset pN \Rightarrow m(x \pmod{p\mathcal{B}}) = 0$.

Lemma. $\mathcal{B}' = \mathcal{B}''$.

Pf: $(\subseteq)$ if $x \in \mathcal{B}' \overset{p \in N}{\Longrightarrow} px \in N \subset \mathcal{B} \Rightarrow x \in \mathcal{B}''$.

$(\supseteq)$ if $x \in \mathcal{B}'' \Rightarrow x \in \mathcal{O}_L$, $px \in \mathcal{B}$. Fix $y \in N$; we must show that $xy \in N$.

$\exists m \geq 1$ $y^m \in p\mathcal{B} \Rightarrow xy^m \in px\mathcal{B} \subset \mathcal{B} \Rightarrow \forall k \geq 1$ $y^m (xy^m)^k = x^k y^{m+mk} \in p\mathcal{B}$

$\Rightarrow \forall k = 0, 1, \dots, n-1$ $x^k y^{mn} \in p\mathcal{B}$.

$x \in \mathcal{O}_L \Rightarrow x^n + a_1 x^{n-1} + \cdots + a_n = 0$, $a_i \in \mathbb{Z} \subset \mathcal{B} \Rightarrow \forall k \geq 0$ $x^k \in \mathbb{Z}\cdot 1 + \mathbb{Z}\cdot x + \cdots + \mathbb{Z}\cdot x^{n-1}$ $\Rightarrow \forall k \geq 0$ $x^k y^{mn} \in p\mathcal{B}$

Take $k = mn$: $(xy)^{mn} \in p\mathcal{B} \Rightarrow xy \in N$, as required.

Computing $\operatorname{disc}(f)$ directly

The symmetric polynomials $s_k = x_1^k + \cdots + x_n^k$ satisfy Newton's recursive formulas $s_k - \sigma_1 s_{k-1} + \cdots + (-1)^{k-1}\sigma_{k-1} s_1 + (-1)^k k\sigma_k = 0$ $(k \geq 1)$ (exercise!)

and

$$\operatorname{disc}(f) = D(1, \overline{x}, \dots, \overline{x}^{n-1}) = \begin{vmatrix} s_0 & s_1 & \cdots & s_{n-1} \\ s_1 & s_2 & \cdots & s_n \\ \vdots & & \ddots & \vdots \\ s_{n-1} & s_n & \cdots & s_{2n-2} \end{vmatrix}$$

Exercise: let A = ring, $d \in A$, $B = A[X]/(X^n - d) \ni \overline{X} = \alpha$

$B = \{ \beta = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \mid a_i \in A \}$ $\quad \alpha^n = d$

(1) Write down explicitly the matrix $M(\beta) \in M_n(A)$ in the basis $\{1, \alpha, \ldots, \alpha^{n-1}\}$ of B over A, the trace $Tr_{B/A}(\beta)$ and the matrix $(Tr_{B/A}(\alpha^i \alpha^j))$ computing the discriminant $D(1, \alpha, \ldots, \alpha^{n-1})$.

(2) For $n = 2, 3$ write down explicitly the full characteristic polynomial $P_{B/A, \beta}(T)$ and $N_{B/A}(\beta)$.

Discriminant of a quadratic field

If $[K : \mathbb{Q}] = 2 \Rightarrow \exists\, d \in \mathbb{Z} \setminus \{0, 1\}$ square-free (unique) $K = \mathbb{Q}(\sqrt{d})$,

$\mathcal{O}_K = \mathbb{Z}[\alpha]$, $\alpha = \begin{cases} \sqrt{d} & d \not\equiv 1 \pmod 4 \\ \frac{1+\sqrt{d}}{2} & d \equiv 1 \pmod 4 \end{cases}$. Set $D = \begin{cases} 4d & d \not\equiv 1 \pmod 4 \\ d & d \equiv 1 \pmod 4 \end{cases}$

D = fundamental discriminant, $K = \mathbb{Q}(\sqrt{D})$

$f(X)$ = the minimal polynomial of α over $\mathbb{Q} = \left\{ \begin{matrix} X^2 - d \\ X^2 - X + \frac{1-d}{4} \end{matrix} \right\} \Rightarrow$

$$D_K = D_{\mathcal{O}_K/\mathbb{Z}} = D_{\mathbb{Z}[\alpha]/\mathbb{Z}} = \operatorname{disc}(f) = \left\{ \begin{matrix} 4d \\ d \end{matrix} \right\} = D$$

$\mathcal{O}_K = \mathbb{Z}\left[\frac{D+\sqrt{D}}{2}\right] = \mathcal{O}_D$ in the language of the chapter on binary quadratic forms

Exercise (Orthogonal similitude groups of binary quadratic forms)

Let $f = ax^2 + bxy + cy^2 \in \mathrm{Quad}_{\mathrm{prim}}(\Delta)$, $\sqrt{\Delta} \notin \mathbb{Z}$. For any ring $A \supset \mathbb{Z}$ consider $GO(f)(A) = \{ U \in GL_2(A) \mid \exists\, \nu(U) \in A^* \quad fU = \nu(U) f \}$. Writing $f\binom{x}{y} = \frac{N(\alpha_1 x + \alpha_2 y)}{(\mathcal{O}_\Delta : I)}$ ($I = \mathbb{Z}\alpha_1 \oplus \mathbb{Z}\alpha_2$ invertible fractional $\mathcal{O}_\Delta$-ideal), the goal is to give an explicit description of $GO(f)(A)$ for $A = \mathbb{Q}, \mathbb{Z}$ in terms of the regular representation $M : K = \mathbb{Q}(\sqrt{\Delta}) \hookrightarrow M_2(\mathbb{Q})$ with respect to the basis α_1, α_2: $\beta(\alpha_1, \alpha_2) = (\alpha_1, \alpha_2) M(\beta)$.

(1) the image of $M : K^* \hookrightarrow GL_2(\mathbb{Q})$ lies in $GO(f)(\mathbb{Q})$ and the composite morphism $K^* \xrightarrow{M} GO(f)(\mathbb{Q}) \xrightarrow{\nu} \mathbb{Q}^*$ is given by the norm $N = N_{K/\mathbb{Q}}$.

(2) The matrix $V \in GL_2(\mathbb{Q})$ given by $(\alpha_1, \alpha_2) V = (\alpha_1', \alpha_2')$ lies in $GO(f)(\mathbb{Q})$ (but not in $M(K^*)$) and satisfies $V^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $\det(V) = -1$, $\nu(V) = 1$.

(3) $\forall\, \beta \in K^* \qquad V^{-1} M(\beta) V = M(\beta')$

(4) $GO(f)(\mathbb{Q}) = \underbrace{M(K^*)}_{\text{"a non-split Cartan subgroup of } GL_2(\mathbb{Q})\text{"}} \sqcup \underbrace{\frac{M(K^*)V}{V M(K^*)}}$ } "the normaliser of a non-split Cartan subgroup of $GL_2(\mathbb{Q})$"

(5) $V \in M_2(\mathbb{Z}) \iff I = I'$

(6) $M^{-1}(M_2(\mathbb{Z})) = \mathcal{O}_\Delta$

(7) If $I \neq I'$, then $GO(f)(\mathbb{Z}) = M(\mathcal{O}_\Delta^*)$

(8) If $I = I'$, then $GO(f)(\mathbb{Z}) = M(\mathcal{O}_\Delta^*) \sqcup \underbrace{\frac{M(\mathcal{O}_\Delta^*)V}{V M(\mathcal{O}_\Delta^*)}}$

Exercise. What happens if $\sqrt{\Delta} \in \mathbb{Z}$? [Hint: f is equivalent to $\sqrt{\Delta}xy$]
