$y^2 = x^3 + ax + b$ — EC equation for fields K such that $\mathrm{char}(K) \neq 2, 3$

We require that $f(X) = X^3 + aX + b$ has no multiple roots.

$= (X-\alpha_1)(X-\alpha_2)(X-\alpha_3)$ and $\alpha_i \neq \alpha_j$ if $i \neq j$

maybe in some extension field

Analogously to $\mathbb{R}$ and $\mathbb{C}$

$\mathbb{C}$ is $\mathbb{R}$ extended by "i" (a root of x^2+1).

The criterion for $f(X)$ having no multiple roots is simple:

$$4a^3 + 27b^2 \neq 0 \quad ?$$

$4a^3 + 27b^2 \neq 0$ ~~then~~ iff $f(X)$ has no multiple roots.

Let define the discriminant of the polynomial $f(X)$

$$f(X) = (x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n) \in K[X]$$

$\alpha_i \in L$, $i = 1, \ldots, n$

it might be $L = K$ or L = some extension field of K.

by: $\Delta(f) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2$

1) We know that the ~~discriminant~~ determinant of the Vandermonde matrix

$$V = V(x_1, x_2, \ldots, x_n) = \begin{bmatrix} 1 & 1 & \ldots & 1 \\ x_1 & x_2 & \ldots & x_n \\ x_1^2 & x_2^2 & \ldots & x_n^2 \\ \vdots & \vdots & & \vdots \\ x_1^{n-1} & x_2^{n-1} & \ldots & x_n^{n-1} \end{bmatrix}$$

is equal

$$\det V = \prod_{n \geq i > j \geq 1} (x_i - x_j)$$

2) We also know that for $A \in M_{n,n}(L)$ we have

$$\det A^t = \det A$$

3) From Cauchy theorem, for $A, B \in M_{n,n}(L)$

$$\det(A \cdot B) = (\det A) \cdot (\det B)$$

Thus for

$\tilde{V} = V(\alpha_1, \alpha_2, \dots, \alpha_n)$ we have

$$\det(\tilde{V} \cdot \tilde{V}^t) = \det(\tilde{V}) \cdot \det(\tilde{V}^t) =$$

$$= \det(\tilde{V}) \cdot \det(\tilde{V}) = (\det(\tilde{V}))^2$$

$$= \Delta(f)$$

On the other hand

$$\tilde{V} \cdot \tilde{V}^t = \begin{bmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \dots & \alpha_n^2 \\ \vdots & & & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \dots & \alpha_n^{n-1} \end{bmatrix} \cdot \begin{bmatrix} 1 & \alpha_1 & \alpha_1^2 & \dots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \dots & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \dots & \alpha_n^{n-1} \end{bmatrix} =$$

$$= \begin{bmatrix} S_0 & S_1 & S_2 & \dots & S_{n-1} \\ S_1 & S_2 & & \dots & S_n \\ S_2 & & \dots & & \vdots \\ \vdots & & & & \vdots \\ S_{n-1} & S_n & \dots & \dots & S_{2\cdot(n-1)} \end{bmatrix}$$

where $S_i = \sum_{j=1}^{n} \alpha_j^i$

For $n = 3$ we have:

$$\tilde{V} \cdot \tilde{V}^t = \begin{bmatrix} S_0 & S_1 & S_2 \\ S_1 & S_2 & S_3 \\ S_2 & S_3 & S_4 \end{bmatrix}$$

4) If α, β, γ are the roots of $p(x) = A \cdot x^3 + B \cdot x^2 + Cx + D$ then

$(*)$ $\quad p(\alpha) = p(\beta) = p(\gamma) = 0$

hence $\underline{p(\alpha) + p(\beta) + p(\gamma) = 0}$

that means that:

$$\begin{cases} p(X) = AX^3 + BX^2 + CX + D \\ p(\alpha) = A\alpha^3 + B\alpha^2 + C\alpha + D \\ p(\beta) = A\beta^3 + B\cdot\beta^2 + C\beta + D \\ p(\gamma) = A\cdot\gamma^3 + B\cdot\gamma^2 + C\gamma + D \end{cases} +$$

$$AS_3 + BS_2 + CS_1 + DS_0 = 0$$

$S_0 = 3$

Moreover, from (*) we have that:

$$\forall k \geq 0 \quad \alpha^k \cdot p(\alpha) + \beta^k \cdot p(\beta) + \gamma^k p(\gamma) = 0$$

that is:

$$A \cdot S_{3+k} + B \cdot S_{2+k} + C \cdot S_{1+k} + D \cdot S_{0+k} = 0$$

In our case:

$\left\{ X^3 + aX + b \right.$

$A = 1$

$B = 0$

$C = a$

$D = b$

So: $(k=0)$: $\quad S_3 + aS_1 + 3b = 0 \Rightarrow S_3 = -aS_1 - 3b$

On the other hand (from Vieta formula) we know that

$$-(\alpha_1 + \alpha_2 + \alpha_3) = B/A$$

$$A \cdot (X - \alpha_1) \cdot (X - \alpha_2)(X - \alpha_3) =$$
$$= A \cdot X^3 + B \cdot X^2 + CX + D \; / :A$$

$$(X - \alpha_1)(X - \alpha_2)(X - \alpha_3) =$$
$$X^3 + B/A\, X^2 + C/A\, X + D/A$$

$$X^3 + (-\alpha_1 - \alpha_2 - \alpha_3)X^2 + \dots = X^3 + B/A\, X^2 + \dots$$

$$-(\alpha_1 + \alpha_2 + \alpha_3) = B/A$$

$$-S_1 = 0$$

Thus $S_1 = 0$ in our case, and $S_3 = -3b$

$(k=1)$:

$$S_4 + 0 \cdot S_3 + aS_2 + \underbrace{bS_1}_{=0} = 0$$

$$S_4 = -a \cdot S_2$$

$$S_2 = \alpha_1^2+\alpha_2^2+\alpha_3^2 = (\alpha_1+\alpha_2+\alpha_3)^2 - 2(\alpha_1\alpha_2+\alpha_2\alpha_3+\alpha_3\alpha_1)$$

$$(\alpha_1+\alpha_2+\alpha_3)(\alpha_1+\alpha_2+\alpha_3) = \alpha_1^2+\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_1+\alpha_2^2+\boxed{\alpha_2\alpha_3}+\alpha_3\alpha_1+\boxed{\alpha_3\alpha_2}+\alpha_3^2$$

$$S_2 = S_1^2 - 2\,\underbrace{C/A}_{} = 0-2a = -2a$$

from Vieta formulas

$$S_4 = -aS_2 = -a\cdot(-2a) = 2a^2$$

$$\Delta(f) = \begin{vmatrix} 3 & 0 & -2a \\ 0 & -2a & -3b \\ -2a & -3b & 2a^2 \end{vmatrix} = 3\cdot(-1)^{1+1}\cdot\begin{vmatrix} -2a & -3b \\ -3b & 2a^2 \end{vmatrix}$$

$$+(-2a)\cdot(-1)^{1+3}\cdot\begin{vmatrix} 0 & -2a \\ -2a & -3b \end{vmatrix} =$$

$$= 3(-4a^3-9b^2) - (2a)\cdot(-4a^2) = -4a^3-27b^2$$

$$\Delta(f) = -(4a^3+27b^2)$$

$$\Delta(f) = 0 \iff 4a^3+27b^2 = 0$$

$\square$.