§1 Motivating Example $k = \mathbb{Q}$, $n \geq 1$

(or k any w/ $\mathrm{char}\, k \nmid n$)

1) $k(\zeta_n)/k$ is abelian, $\mathrm{Gal} \xhookrightarrow{i} (\mathbb{Z}/n\mathbb{Z})^\times$.

$\sigma(\zeta_n) = \zeta_n^{i(\sigma)}$

2) Assume $k(\zeta_n) = k$, $a \in k^\times$.

Then $k(\sqrt[n]{a})/k$ abelian and

choice of ζ_n.

$\mathrm{Gal} \hookrightarrow \mathbb{Z}/n\mathbb{Z}$

$\sigma \longmapsto \sigma(\sqrt[n]{a})/\sqrt[n]{a} \in \langle \zeta_n \rangle \xrightarrow{\sim} \mathbb{Z}/n\mathbb{Z}$.

Both extensions naturally arise from

$\mathbb{G}_m = \mathrm{Spec}\, k[T, T^{-1}]$ multiplicative group $/k$.

Multiplication $\mathbb{G}_m \times \mathbb{G}_m \longrightarrow \mathbb{G}_m$

$T \otimes T \longmapsto T$

Torsion $\mu_n := \mathbb{G}_m[n] \longrightarrow \mathrm{Spec}\, k[T]$

$\mathrm{Spec}\, k[T]/T^n - 1 \quad \| \quad \downarrow \quad \square \quad \downarrow [n] \; T \longmapsto T^n$

$\mathrm{Spec}\, k \xrightarrow{e} \mathrm{Spec}\, k[T]$

$1 \longmapsto T$

In 1) Write $\mu_n = \coprod_{i \in I} \operatorname{Spec} K_i$ (μ_n is an étale group scheme of char $\nmid n$)

Then $k(\xi_n)$ = Composite of all $\tau(K_i)$ in $\bar{k}$,

$\tau : K_i \longrightarrow \bar{k}$ any embedding

In 2) Write $[n]^{-1}(a) = \coprod_{i \in I} \operatorname{Spec} K_i$

$$\begin{array}{ccc} [n]^{-1}(a) & \longrightarrow & \mathbb{G}_m \\ \downarrow & \square & \downarrow [n] \\ \operatorname{Spec} k & \xrightarrow{a} & \mathbb{G}_m \end{array}$$

Then Composite of all $\tau(K_i)$ in $\bar{k}$

$= k(\xi_n, \sqrt[n]{a})$.

§2 Adaption to ECs

E/k EC, $\operatorname{char} k \nmid n$

$\bar{k}/k$ choice of alg cl.

$K :=$ Composite $\operatorname{Im}(x^*) \subseteq \bar{k}$
$x \in E[n](\bar{k})$

(Write $E[n] = \operatorname{Spec} A$.

$x \longmapsto x^* : A \longrightarrow \bar{k}$, then take image)

Note $E[n](K) \simeq (\mathbb{Z}/n\mathbb{Z})^{\oplus 2}$ just like $\mu_n(k(\zeta_n)) \simeq \mathbb{Z}/n$.

$L :=$ Composite $\operatorname{Im}(x^*) \subseteq \bar{k}$.
$a \in E(K)$, $x \in [n]^{-1}(a)(\bar{k})$

Prop 1) K is a finite Galois extension

$$\operatorname{Gal}(K/k) \hookrightarrow GL_2(\mathbb{Z}/n\mathbb{Z})$$

2) L/K is a (possibly infinite) abelian ext of K,

$$\operatorname{Gal}(L/K) \hookrightarrow \operatorname{Hom}(E(k), E[n](k))$$

Proof 1) K Galois because $\forall\, \sigma : \bar{k} \longrightarrow \bar{k}$

and $x^* \in E[n](\bar{k})$, $\sigma(x) \longleftrightarrow (\sigma \circ x^*) \in E[n](\bar{k})$

Moreover, $[n] : E \longrightarrow E$ is étale, so any residue field

$\kappa(x_0)$, $x_0 \in E[n]$, is separable over k

$\Rightarrow$ K is $\mathrm{Gal}(\bar{k}/k)$-stable composite of separable extensions, hence Galois.

Let $x, y \in E[n](K)$ be $\mathbb{Z}/n$-basis.

Then $\sigma \longmapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ if

$$\sigma(x) = ax + by, \quad \sigma(y) = cx + dy$$

defines a group homomorphism

$$\mathrm{Gal}(K|k) \xrightarrow{i} GL_2(\mathbb{Z}/n\mathbb{Z}).$$

Claim In fact, $K = k(\mathrm{Im}(x^*), \mathrm{Im}(y^*))$, so i is injective.

Proof Any $P \in E[n](\bar{k})$ is a linear combination

$$P = ax + by \qquad a, b \in \mathbb{Z}/n.$$

This means $P^* : A \longrightarrow \bar{k}$ is a composition

$$A \xrightarrow{m^*} A \underset{k}{\otimes} A \xrightarrow{[a]^* \otimes [b]^*} A \underset{k}{\otimes} A \xrightarrow{x^* \cdot y^*} \bar{k}$$

So $\mathrm{Im}(p^*) \subseteq \mathrm{Im}(x^*)\,\mathrm{Im}(y^*)$. $\square$ (Claim & Part 1).

2) L/K Galois for same reason as before

Define $\mathrm{Gal}(L/K) \longrightarrow \mathrm{Hom}(E(K), E[n](K))$

$$\sigma \longmapsto \left[P \longmapsto Q^{\sigma} - Q \right]$$

where $Q \in E(\bar{k})$, $n \cdot Q = P$.

Well-defined: If also $n \cdot \tilde{Q} = P$, then

$$n(Q - \tilde{Q}) = O, \text{ so } \sigma(Q - \tilde{Q}) = Q - \tilde{Q}.$$

Linear in P Given $P_1 = nQ_1$, $P_2 = n \cdot Q_2$,

then $P_1 + P_2 = n(Q_1 + Q_2)$.

Now apply defn.

Linear in σ Assume $nQ = P$.

Then $\sigma_1 \sigma_2 (Q) - Q$

$$= \sigma_1 \underbrace{\left(\sigma_2(Q) - Q \right)}_{\in E[n](K)} + \sigma_1(Q) - Q$$

$$= \sigma_2(Q) - Q + \sigma_1(Q) - Q.$$

Injective $\delta \longmapsto O \longrightarrow \delta(Q) = Q$

$\forall\, Q \in [n]^{-1} E(k)$.

□ Prop.