Defn | F-field. An abelian extn of F is a galois extn E/F s.t. $\mathrm{Gal}(E/F)$ abelian

E.g. |

1) $F(\sqrt{a})/F$ is ab $\quad$ Gal $= \mathbb{Z}/2$
2) if $\mu_n \subset F \Rightarrow F(a^{1/n})/F$ is ab, gal $\subset \mathbb{Z}/n$
3) $F(\mu_n)/F$ is ab, gal $\subseteq (\mathbb{Z}/n)^\times$
4) If f is irred cubic poly s.t. $\mathrm{disc}(f) = \square$
$\Rightarrow$ its splitting field is a $\mathbb{Z}/3$ extn

Fact | Say $E_1, E_2 \subset K$ are ab extn of F w/ K/F gal.
Then E_1E_2 (composition) is an abelian extn of F $\subseteq \mathrm{Gal}(E_1/F) \times \mathrm{Gal}(E_2/F)$

$\Rightarrow \exists$ unique max'l abelian extn of F contained in K by taking comp.

Taking $K = \overline{F} \Rightarrow \exists$ max'l ab extn of F.

$$\left.\begin{array}{c} K \\ \Big| \\ E \\ \Big| \\ F \end{array}\right. \quad \begin{array}{l} \}\,[G,G] \\ \\ \}\,G_{ab} = G/[G,G] \end{array} \qquad \text{gal w/ gp } G$$

E = max ab extn of F in K

can do $K = \overline{F}$

$\mathrm{Gal}(F^{ab}/F) = (G_F)_{ab}$

$$\left.\begin{array}{c} \overline{F} \\ \Big| \\ F^{ab} \\ \Big| \\ F \end{array}\right\} G_F$$

Class Field theory $\to$ abelian extensions of number fields $\to$ fin extn of $\mathbb{Q}$.
$\hookrightarrow$ wanna grab $(G_{\mathbb{Q}})_{ab}$

Kronecker Weber Tm | $\mathbb{Q}^{ab} = \bigcup_{n \geq 1} \mathbb{Q}(\mu_n)$ $\to$ Chain by divisib.

Cor | If $E|\mathbb{Q}$ is a finite ab extn
$\Rightarrow E \subset \mathbb{Q}(\mu_n)$ for some n

E.g | $\mathbb{Q}(\sqrt{5})$ is contained in some $\mathbb{Q}(\mu_n)$

Cor | $\mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^\times$ so gal gp of union is inv lim

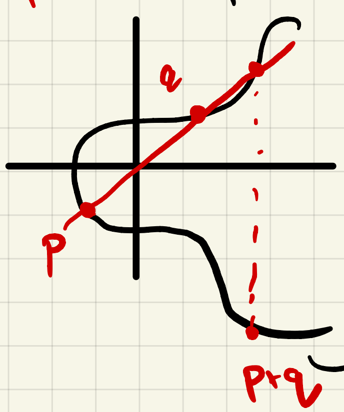
$$\mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q}) = (G_{\mathbb{Q}})_{ab} = \hat{\mathbb{Z}}^\times = \prod_p \mathbb{Z}_p^\times$$

If K is some number field then
$$K^{ab} \supset \bigcup_{n\geq 1} K(\mu_n)$$
if $K \neq \mathbb{Q}$ then it will be bigger

Kronecker's Jugentraum |
Find explicit generators of K^{ab} ⇝ unsolved in general

(any field K).

Def | An elliptic curve over K is an eqn $y^2 = x^3 + ax + b$ — distinct root in $\bar{K}$ ⟶ disc $\neq 0$



→ grp law.
⇝ requiring pt at ∞ ⟶ identity

$$E(K) = \{(x,y)\in K^2 \mid y^2 = x^3+ax+b\} \cup \{\infty\}$$

⟶ above pic gives $E(K)$ struct of ab grp.

If $k = \mathbb{C}$

typically, the map $E(\mathbb{C})\setminus\{\infty\} \longrightarrow \mathbb{C}$ is 2 – 1 (unless $x^3+ax+b = 0$)

$(x,y) \longmapsto x$

So $E(\mathbb{C}) \cong S^1 \times S^1$ as top grp.

$\cong \mathbb{C}/\Lambda \qquad \Lambda \cong \mathbb{Z}^2$ disc lattice in $\mathbb{C}$

Rmks | given Λ $\exists!$ $\wp : \mathbb{C} \longrightarrow \mathbb{C}$ meromorphic

1) • $\wp$ has poles at Λ, no other poles → order 2

• $\wp(z+\lambda) = \wp(z)$ $\forall z \in \mathbb{C}, \lambda \in \Lambda$

↳ $\wp$ is doubly polar

$$\wp(z) = \frac{1}{z^2} + \sum_{\lambda \neq 0} \left[\frac{1}{(z+\lambda)^2} - \frac{1}{\lambda} \right]$$

Thm | $\exists\, a, b \in \mathbb{C}$ so

$$4\wp'(z)^2 = \wp(z)^3 + a\,\wp(z) + b$$

let $E : y^2 = x^3 + ax + b$

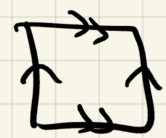
$(\wp, \wp') : \mathbb{C}/\Lambda \xrightarrow{\sim} E(\mathbb{C})$

2) Start w/ elliptic curve E

$\omega = \frac{dx}{y}$ ⇝ 1-form on $E(\mathbb{C})$ → think of as 1 mfd.

Integrate ω over $\underbrace{H_1(E(\mathbb{C}), \mathbb{Z})}_{= \mathbb{Z}^2}$ this gives $\Lambda \subset \mathbb{C}$

↳ generators of H_1



$\underbrace{E(\mathbb{C})[n]}_{\to\ n \text{ torsion}} = \{ P \in E(\mathbb{C}) \mid nP = \infty \}$ subgrp

$= (\mathbb{Z}/n\mathbb{Z})^2$ ⇝ corr to n^{th} roots in each $S^1 \times S^1$.

$K = \mathbb{Q}$.

Mordell's Thm $E(\mathbb{Q})$ is a f.g. ab grp

$\Rightarrow E(\mathbb{Q}) \cong \mathbb{Z}^r \times T \rightsquigarrow$ torsion.

Rmks

1) It's not clear if r can get inf large (might be ≤ 30)
2) Finite list of possible T's (Mazur Thm)

Say E is defined over $\mathbb{Q}$ ($a, b \in \mathbb{Q}$)

now consider $E(\bar{\mathbb{Q}}) \rightsquigarrow$ solutions in $\bar{\mathbb{Q}}$

$\rightsquigarrow$ consider $E(\bar{\mathbb{Q}})[n]$

$\cong (\mathbb{Z}/n\mathbb{Z})^2$

$G_{\mathbb{Q}}$

it is compatible w/ ab grp struct

$G_{\mathbb{Q}} \longrightarrow GL_2(\mathbb{Z}/n\mathbb{Z}) \rightsquigarrow$ this is like a 2-d rep.

$\hookrightarrow$ interesting source of gal reps.

Rmk 1) if E is "random"

$\Rightarrow$ for most primes p $G_{\mathbb{Q}} \xrightarrow{\varphi} GL_2(\mathbb{F}_p)$

is surj (thm of Serre).

$\Rightarrow$ eg of gal extn of $\mathbb{Q}$ w/ grp $GL_2(\mathbb{F}_p)$

$\hookrightarrow$ corr to ker φ which is normal.

2) $E = \mathbb{C}/\Lambda$, $\Lambda = \mathbb{Z}[i]$

$y^2 = x^3 + x$ mult by i on (x,y)

$(x,y) \xmapsto{\sigma} (-x, iy)$ is an order 4 aut of E.

Say $p \equiv 3 \ (4)$ prime

$G_{\mathbb{Q}(i)} \circlearrowright E(\overline{\mathbb{Q}})[p]$ commutes w/ σ

$E(\overline{\mathbb{Q}})[p] = $ 2-d vs $/\mathbb{F}_p$

σ makes it 1-d vs $/ \mathbb{F}_{p^2} \cong \mathbb{F}_p(i)$

$G_{\mathbb{Q}(i)} \longrightarrow GL(\mathbb{F}_{p^2}) = \mathbb{F}_{p^2}^{\times}$ $\rightsquigarrow$ abelian extn of $\mathbb{Q}(i)$

Thm) $\mathbb{Q}(i)^{ab} = \bigcup \mathbb{Q}(i)\left(\begin{matrix}\text{coords of tors pts on} \\ E(\overline{\mathbb{Q}}) \quad E: y^2 = x^3 + x\end{matrix}\right)$