Lecture 3

§ Non-abelian extensions of $\mathbb{Q}$ — motivation

```
P := PrimesUpTo(NthPrime(10^4));
R<x> := PolynomialRing(Integers());
{* Roots(x^3-2, GF(p)) : p in P *};
```

<u>Ex</u> How often is $2 \in \mathbb{F}_p$ a cube?

x^3-2 has 3 roots mod $p = 31, 43, 109, \ldots$ density $1/6$?

1 root mod $p = 2, 3, 5, 11, \ldots$ density $1/2$?

0 roots mod $p = 7, 13, 19, 37, \ldots$ density $1/3$?

Later look at higher-dim varieties V and $\#V(\mathbb{F}_p)$

$F := \mathbb{Q}(\sqrt[3]{2})$. How often, for $p \neq 2,3$ (2,3 ramify)

$p = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ or $p = \underset{f=2}{\mathfrak{p}_1}\,\underset{f=1}{\mathfrak{p}_2}$ or $p = \underset{f=3}{\mathfrak{p}}$ in F?

Recall: $K/\mathbb{Q}$ Galois $\Rightarrow$ $p = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ all $f_i = f$ equal, all $e_i = e$ equal,

$efr = [K:\mathbb{Q}]$

<u>Q</u> What if $F/\mathbb{Q}$ non-Galois, as above?

<u>A</u> Convert f, e to groups $\subseteq \mathrm{Gal}(K/\mathbb{Q})$, K Galois closure of F.

§ Decomposition, inertia, Frobenius

$K/\mathbb{Q}$ finite Galois

p prime of $\mathbb{Q}$

$G = \mathrm{Gal}(K/\mathbb{Q})$ $\qquad |G| = [K:\mathbb{Q}] = d$

← Similar over a number field F

$\mathfrak{p}_1, \dots, \mathfrak{p}_r$ primes above p in K

ram. index e, res. degree f, $efr = d$

$$\begin{array}{ccc} \mathfrak{p}_1 \cdots \mathfrak{p}_r & \subseteq \mathcal{O}_K & \mathbb{F}_{p^f} \\ \backslash \ / & & | \\ p & \subseteq \mathbb{Z} & \mathbb{F}_p \end{array}$$

residue fields

Fact 1 G permutes $\mathfrak{p}_i$ transitively.

Def $D_{\mathfrak{p}_i} = \mathrm{Stab}_G\, \mathfrak{p}_i = \{\sigma \in \mathrm{Gal}(K/\mathbb{Q}) \mid \sigma(\mathfrak{p}_i) = \mathfrak{p}_i\}$ $\qquad$ decomposition gp of $\mathfrak{p}_i$

It acts on $\mathcal{O}_K/\mathfrak{p}_i \cong \mathbb{F}_{p^f}$ $\Rightarrow$

$$D_{\mathfrak{p}_i} \longrightarrow \mathrm{Gal}(\mathbb{F}_{p^f}/\mathbb{F}_p) \cong \langle x \mapsto x^p \rangle \cong C_f$$
$$\sigma \longmapsto \bar{\sigma}$$

reduction map

Fact 2 This is onto.

Def $I_{\mathfrak{p}_i} = \ker(\text{reduction map}) = \{\sigma \in D_{\mathfrak{p}_i} \mid \bar{\sigma} = \mathrm{id}\}$ $\qquad$ inertia group of $\mathfrak{p}_i$

Def $\mathrm{Frob}_{\mathfrak{p}_i} :=$ any elt $\sigma \in D_{\mathfrak{p}_i}$ s.t. $\bar{\sigma} : x \mapsto x^p$. $\qquad$ A Frobenius elt. at $\mathfrak{p}_i$

So

$$G \overset{r}{>} D_{\mathfrak{p}_i} \overset{f}{\triangleright} I_{\mathfrak{p}_i} \overset{e}{\triangleright} \{1\}$$

cyclic quo. gen. by $\mathrm{Frob}_{\mathfrak{p}_i}$

By Galois theory corresponds to

$$\mathbb{Q} \underset{p \text{ tot. split}}{\overset{r}{\text{———}}} K_1 \underset{\mathfrak{p}_i \text{ tot. inert}}{\overset{f}{\text{———}}} K_2 \underset{\tilde{\mathfrak{p}}_i \text{ tot. ramified}}{\text{———}} K$$

$$\begin{array}{ccccccc} p & \equiv & \tilde{\tilde{\mathfrak{p}}}_i & \text{———} & \tilde{\mathfrak{p}}_i & \text{———} & \mathfrak{p}_i \\ \mathbb{F}_p & & \mathbb{F}_p & & \mathbb{F}_{p^f} & & \mathbb{F}_{p^f} \end{array}$$

$p = (\mathfrak{p}_1)^e \cdots (\mathfrak{p}_r)^e$

__Rmk__ For $\tau \in G$

$$D_{\tau(\mathfrak{p}_i)} = \{\sigma \in G \mid \sigma(\tau(\mathfrak{p}_i)) = \tau(\mathfrak{p}_i)\} = \{\tau\sigma\tau^{-1} \mid \sigma(\mathfrak{p}_i) = \mathfrak{p}_i\} = \tau D_{\mathfrak{p}_i}\tau^{-1}$$

So $D_{\mathfrak{p}_1}, \dots, D_{\mathfrak{p}_r}$ are conjugate ; full conj. orbit of sgps.

Convenient to descend to $\mathbb{Q}$:

__Def__ $K/\mathbb{Q}$ Galois, p prime

$D_p := D_{\mathfrak{p}_i}$ of some $\mathfrak{p}_i | p$ $\quad\leftarrow$ defined up to conjugacy

$I_p := I_{\mathfrak{p}_i}$ of $\mathfrak{p}_i$ $\quad\leftarrow$ — " —

$\mathrm{Frob}_p :=$ Frob. elt. at $\mathfrak{p}_i$ $\quad\leftarrow$ — " — and modulo inertia.

For the unramified primes (all but fin. many) $\quad I_p = \{1\}$, $D_p = \langle \mathrm{Frob}_p \rangle$

this conj. class determines everything

__Thm__ (Prime decomposition) $K/\mathbb{Q}$ Galois, $\mathbb{Q} \subseteq F \subseteq K$ subfield.

$G = \mathrm{Gal}(K/\mathbb{Q})$

$H = \mathrm{Gal}(K/F)$, so $F = K^H$.

$$\begin{tikzcd}
 & K \arrow[dd, dash, "G"] \\
F \arrow[ur, dash, "H"] \arrow[dr, dash] & \\
 & \mathbb{Q}
\end{tikzcd}$$

Let p be a prime of $\mathbb{Q}$, with

(Frob$_p \in$) D = decomposition gp at p $\quad < G$

I = inertial gp at p $\quad < D_p$

Then

primes $\mathfrak{P}_j | p$ in F $\quad\xleftrightarrow{1:1}\quad$ double cosets $D g_j H \in D\backslash G/H$

res. degree f_j, ram. index e_j $\quad\xleftrightarrow{1:1}\quad$ orbits of D on G/H ;

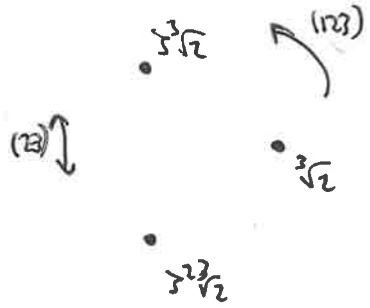
each orbit has length $e_j f_j$ and is a union of f_j I-orbits of length e_j, cyclically permuted by Frob_p.

__Proof__ Computation.

__Thm__ (Čebotarev Density Theorem) $\mathrm{Frob}_p \in G$ is equidistributed: for every conj. class $C \subset G$, density of primes p with $\mathrm{Frob}_p \in C$ is $\frac{|C|}{|G|}$.

$\underline{\text{Ex}}$ $F = \mathbb{Q}(\sqrt[3]{2})$, $\zeta = \zeta_3$

$K = \mathbb{Q}(\sqrt[3]{2}, \zeta) = \mathbb{Q}(\text{roots of } x^3 - 2)$ Galois



$G = \mathrm{Gal}(K/\mathbb{Q}) = S_3$

$$\begin{array}{c} K \\ \big|\ \langle(23)\rangle \\ F \\ \big| \\ \mathbb{Q} \end{array} \quad S_3$$

$(123):$ $\sqrt[3]{2} \longmapsto \zeta\sqrt[3]{2}$ order 3
$\qquad\quad \zeta \longmapsto \zeta$

$(23):$ $\sqrt[3]{2} \longrightarrow \sqrt[3]{2}$ order 2 complex conj.
$\qquad\quad \zeta \longrightarrow \zeta^2$ $\quad K^{\langle(23)\rangle} = F$

All $p \neq 2,3$ unramified in $K/\mathbb{Q}$ $\Rightarrow$ $I_p = \{id\}$, $D_p = \langle \mathrm{Frob}_p \rangle$ cyclic.

$$D \curvearrowright G/H = \left\{ \boxed{\begin{matrix} id \\ (23) \end{matrix}}, \boxed{\begin{matrix} (123) \\ (13) \end{matrix}}, \boxed{\begin{matrix} (132) \\ (12) \end{matrix}} \right\}$$

Frob_p	$D_p = \langle \mathrm{Frob}_p \rangle$ up to conjugacy	$D \curvearrowright G/H$	f_i	density $\lvert C\rvert/\lvert G\rvert$
id	$\{id\}$	id (123) (132)	1, 1, 1	1/6
2-cycle	$\langle(23)\rangle$	id $\quad (123) \leftrightarrow (132)$	1, 2	1/2
3-cycle	$\langle(123)\rangle$	id $\to (123) \to (132)$	3	1/3

Primes $p = 2,3$ are ramified in $K/\mathbb{Q}$:

$p = 2$: $\quad I_p = C_3 \quad D_p = S_3$

$p = 3$: $\quad I_p = D_p = S_3$

$\longrightarrow$ $\underline{\text{Exc}}$ Check, using prime decomposition in $\mathbb{Q}(\zeta_3)$ and $\mathbb{Q}(\sqrt[3]{2})$

§ Artin representations

Def G finite group. A d-dimensional (complex) representation of G is a group hom.

$$\rho: G \longrightarrow GL_d(V) \underset{\cong}{} GL_d(\mathbb{C}) \qquad V \ \mathbb{C}\text{-v. space of dim } d$$

When K/F fin. Gal. ext. of number fields,

$$\rho: \quad \mathrm{Gal}(K/F) \longrightarrow GL(V)$$
$$\mathrm{Gal}(\bar{F}/F) \nearrow$$

is an Artin representation (over F).

Ex 1-dim Artin rep. $=$ gp. hom $\mathrm{Gal}(K/F) \longrightarrow \mathbb{C}^\times$ "1-dim character"

Ex $F = \mathbb{Q}$

$K = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$

$$\Delta: \mathrm{Gal}(K/F) \cong S_3 \longrightarrow GL_2(\mathbb{C})$$
$$(123) \longmapsto \text{rot. by } 2\pi/3 = \begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}$$
$$(23) \longmapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

we are "representing" $\mathrm{Gal}(K/F)$ as a group of matrices

is a 2-dim. Artin rep. over $\mathbb{Q}$. ← **Exc** find it on LMFDB.

Def $\rho: \mathrm{Gal}(K/F) \to GL(V)$ Artin representation. The Artin L-function

$$L(\rho, s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} := \prod_{\mathfrak{p} \text{ prime of } F} \frac{1}{F_{\mathfrak{p}}(N_{F/\mathbb{Q}}\mathfrak{p})^{-s}} \quad ; \quad F_{\mathfrak{p}}(T) = \det\left(1 - \rho(\mathrm{Frob}_{\mathfrak{p}}^{-1})T \,\middle|\, V^{I_{\mathfrak{p}}}\right)$$

⚠ Have no interpretation for a_n for composite n

for unramified primes has degree d, depends only on conj. class of $\mathrm{Frob}_{\mathfrak{p}} \in \mathrm{Gal}(K/F)$

inertia invariants $\{v \in V \mid \sigma(v) = v \ \ \forall \sigma \in I_{\mathfrak{p}}\}$ $= V$ if $\mathfrak{p}$ unramified in K/F

Exc (Highly recommended) Prove that this is well-defined.

independent of choices for $I_{\mathfrak{p}}$, $\mathrm{Frob}_{\mathfrak{p}}$.

Ex $\quad \Delta : \mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}) \cong S_3 \longrightarrow GL(V), \quad \dim V = 2.$

$$\begin{array}{lcll} \mathrm{id} & \longmapsto & \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & \text{char pols. } (1-T)^2 \\ \text{2-cycles} & \longmapsto & \sim \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} & \text{char. poly } (1-T)(1+T) \\ \text{3-cycles} & \longmapsto & \sim \begin{pmatrix} \zeta_3 & 0 \\ 0 & \zeta_3^{-1} \end{pmatrix} & \text{charpoly } 1+T+T^2 \end{array}$$

$$L(\Delta, s) = \underbrace{1}_{\substack{I_2 = C_3 \\ V^{I_2} = 0}} \cdot \underbrace{1}_{\substack{I_3 = S_3 \\ V^{I_3} = 0}} \cdot \underbrace{\frac{1}{(1-5^{-s})(1+5^{-s})}}_{\mathrm{Frob}_5\ \text{2-cycle}} \cdot \underbrace{\frac{1}{1+7^{-s}+7^{-2s}}}_{\mathrm{Frob}_7\ \text{3-cycle}} \cdot \ldots$$

Exc $\quad$ Find Δ and $L(\Delta, s)$ on LMFDB.

§ 1-dimensional Artin representations

Thm There is a bijection

$\leftarrow$ actually iso of groups
• on the left, $\otimes$ on the right

$$\{\text{Dirichlet characters}\} \longleftrightarrow \{\text{1-dim Artin reps } \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{C}^\times\}$$
$$\chi \longmapsto \rho_\chi$$

such that

(A) χ has modulus $m \iff \rho_\chi$ factors through $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ and not for smaller $n | m$

(B) $L(\chi, s) = L(\rho_\chi, s)$

Proof Take $\chi : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$ primitive, let

$$\rho_\chi : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \overset{\text{can.}}{\cong} (\mathbb{Z}/m\mathbb{Z})^\times \xrightarrow{\chi} \mathbb{C}^\times$$
$$\sigma : \zeta_m \mapsto \zeta_m^a \longmapsto a^{-1} \longmapsto \chi(a)^{-1}$$

(A) is clear.

Conversely, if $\rho : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{C}^\times$ one dim. Artin rep.

$N := \ker \rho \quad$ Normal

$K := \bar{\mathbb{Q}}^N. \quad$ Galois

$\mathrm{Gal}(K/\mathbb{Q}) \cong \mathrm{Im}\,\rho < \mathbb{C}^\times$ abelian, so $K \subseteq \mathbb{Q}(\zeta_m)$ by Kronecker-Weber, some m

Therefore $\rho \cong \rho_\chi$ for some χ.

(B) Compare L-functions $L(\chi, s)$ and $L(\rho_\chi, s)$ by local factors.

<u>$p \nmid m$</u> $\iff$ p unramified in $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ $\iff I_p = \{id\}$.

$$F_p(T)_{LHS} = 1 - \chi(p)T$$

$$F_p(T)_{RHS} = 1 - \rho_\chi(\mathrm{Frob}_p^{-1})T \qquad \text{under } \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$$

$$\underset{\substack{\| \\ \mathrm{Frob}_p^{-1}}}{(\zeta_m \mapsto \zeta_m^{p^{-1}})} \longleftrightarrow p$$

$$= 1 - \chi(p)T$$

<u>$p \mid m$</u> $\quad F_p(T)_{LHS} = 1$

$m = m_0 p^k \qquad \left.\begin{array}{l} \mathbb{Q}(\zeta_m) \\ \quad | \; I_p \\ \mathbb{Q}(\zeta_{m_0}) \\ \quad | \\ \mathbb{Q} \end{array}\right) (\mathbb{Z}/m\mathbb{Z})^\times$

χ primitive $\Rightarrow$ does not factor through $(\mathbb{Z}/m_0\mathbb{Z})^\times$

$\Rightarrow \chi(I_p) \neq 1 \Rightarrow V^{I_p} = \{0\}$

$\Rightarrow F_p(T)_{RHS} = 1$

∎

<u>Rmk</u> Same holds over any number field F:

Hecke characters $/F$ of trivial ∞ type	$\overset{1:1}{\longleftrightarrow}$	1-dim Artin reps over F
χ	$\longmapsto$	ρ_χ
$L(\chi, s)$	$=$	$L(\rho_\chi, s)$

<u>Proof</u> Instead of Kronecker-Weber, full force of global CFT.

§ Permutation representations & Dedekind ζ

K/F finite Galois, $G = \mathrm{Gal}(K/F)$

$$\begin{array}{ccccc} \text{Transitive } G\text{-sets}/\cong & \xleftrightarrow{1:1} & \text{Sgps of } G \text{ up to conjugacy} & \xleftrightarrow{1:1} & \text{fields } F \subseteq M \subseteq K \text{ up to iso.}/F \\ X & \longmapsto & \text{Stabiliser (elt)} & & \\ G/H & \longleftarrow & H & & \end{array}$$

$\uparrow$ left cosets $g_1H, \dots, g_dH$
$g \cdot (g_iH) = (gg_i)H$

$$H \longmapsto K^H$$
$$\mathrm{Gal}(K/M) \longleftarrow M$$

$$\begin{tikzcd} K \arrow[d, dash, "H"] \\ M \arrow[d, dash, "d"] \\ F \end{tikzcd} \quad G \qquad \rightsquigarrow \qquad X = G/H \text{ size } d$$

Explicitly if $M = F(\alpha)$, α root of $f(x) \in F[x]$, irr. deg d

$$H = \mathrm{Stab}_G\, \alpha$$
$$X = \{\text{roots of } f\} \circlearrowleft G$$
$$1:1 \updownarrow$$
$$X_{M/K} = \{F\text{-embeddings } M \hookrightarrow \bar{F}\} \circlearrowleft \mathrm{Gal}(\bar{F}/F)$$

independent of the choice of K/F Galois containing M

Ex $G = S_3$
$F = \mathbb{Q}$
$K = \mathbb{Q}(\zeta_3, \sqrt[3]{2})$) or any other S_3-extension

fields M	Sgps H	G-sets X	
$\mathbb{Q}$	S_3	•	G acts trivially
$\mathbb{Q}(\zeta_3)$	C_3	• •	G acts through $S_3/C_3 \cong C_2$
$\mathbb{Q}(\sqrt[3]{2})$	C_2	• • •	G acts as $S_3 \circlearrowleft \{1,2,3\}$
K	C_1	• • • • • •	G acts as $G \circlearrowleft G$ by left mult. (regular action)