I

Nov 2023

References:
- Szamuely – Galois groups and fundamental groups chap. 3-4
- Serre – Topics in Galois theory chap. 6-8
- Völklein – Groups as Galois groups chap. 2-7

To go further:
- Malle-Matzat – Inverse Galois theory chap. I-II
- Fried-Jarden – Field Arithmetic

Coverings and rigidity

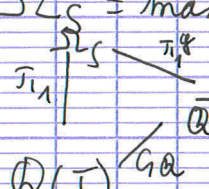
My goal: black box all the geometry into as small a lemma as is needed.

⚠ For conjugacy, we write $a^b = bab^{-1}$. Note that $(a^b)^c = a^{cb}$.

S = finite set of distinct rational numbers
i.e. places $\neq \infty$ of $\bar{\mathbb{Q}}(T) \subseteq \mathbb{P}^1_{\bar{\mathbb{Q}}}$.
↳ This choice of a point is arbitrary but practical

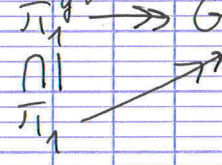
$|S| = n$

Ω_S = maximal extension of $\bar{\mathbb{Q}}(T)$ unramified outside S.



Let:
$$\begin{cases} G_{\mathbb{Q}} = Gal(\bar{\mathbb{Q}}|\mathbb{Q}) = Gal(\bar{\mathbb{Q}}(T)|\mathbb{Q}(T)) \\ \pi_{1,1} = Gal(\Omega_S | \mathbb{Q}(T)) \\ \pi_{1,1}^g = Gal(\Omega_S | \bar{\mathbb{Q}}(T)) \end{cases}$$

Our plan: * Understand extensions of $\bar{\mathbb{Q}}(T)$
i.e. surjective morphisms $\pi_{1,1}^g \to G$
* Define a Galois action $G_{\mathbb{Q}} \curvearrowright \pi_{1,1}^g$
* Find "fixed" extensions for this action, which in good cases allow one to extend



$\rightsquigarrow$ regular G-extension of $\bar{\mathbb{Q}}(T)$, i.e. $F \cap \bar{\mathbb{Q}} = \mathbb{Q}$.

I. Galois actions on extensions of $\bar{\mathbb{Q}}(T)$.

Fundamental exact sequence:

$$1 \to \pi_{1,1}^g \to \pi_{1,1} \to G_{\mathbb{Q}} \to 1 \qquad (*)$$

(Note: this exact sequence has a geometric meaning. $X = \mathbb{P}^1_{\bar{\mathbb{Q}}} \setminus S$, $X_{\bar{\mathbb{Q}}} = X \times_{\operatorname{Spec}\mathbb{Q}} \operatorname{Spec}\bar{\mathbb{Q}}$

then $\pi_{1,1} = \pi_1^{ét}(X, \infty)$, $\pi_{1,1}^g = \pi_1^{ét}(X_{\bar{\mathbb{Q}}}, \infty)$ and $\pi_{1,1}^g \to \pi_{1,1}$ is the image under the functor $\pi_1^{ét}$ of $X_{\bar{\mathbb{Q}}} \to X$

Proposition: The exact sequence (★) is split by a morphism $s_\infty : G_{\mathbb{Q}} \to \Pi_1$.

Proof: ~~[illegible]~~

Note that Ω_S embeds in $\overline{\mathbb{Q}(T)} \subseteq \overline{\mathbb{Q}((1/T))} = \overline{\mathbb{Q}}((1/T))$ where $\mathbb{Q}((1/T))$ denotes Laurent series over $\mathbb{Q}$

$= \overline{\mathbb{Q}}((1/T-\infty))$: Puiseux series

Note: the choice of the embedding in $\overline{\mathbb{Q}}((1/T-\infty))$ is dependent on the choice of ∞ as a basepoint.
For a different $x \in \mathbb{P}^1_{\mathbb{Q}}$, we could have embedded Ω_S in $\overline{\mathbb{Q}}((T-x))$; this would yield another splitting $s_x : G_{\mathbb{Q}} \to \Pi_1$.
(Grothendieck's section conjecture: all splittings come from a rational point $\operatorname{Spec}\mathbb{Q} \to X$ via $\pi_1^{\text{ét}} \rightsquigarrow G_{\mathbb{Q}} \to \pi_1^{\text{ét}}(X)$)

An automorphism $\sigma \in G_{\mathbb{Q}}$ acts on $\overline{\mathbb{Q}}((1/T-\infty))$ via its action on coefficients:

$$\sum_{r \in \mathbb{Q}} a_r T^r \mapsto \sum_{r \in \mathbb{Q}} (\sigma \cdot a_r) T^r$$

For this action, the subfield $\mathbb{Q}(T)$ is acted trivially upon.
$\overline{\mathbb{Q}}(T)$ is globally stable.
Moreover: Ω_S is stable.
Indeed: if an algebraic extension $L \mid \overline{\mathbb{Q}}(T)$ is unramified at $t \in \overline{\mathbb{Q}}$, then $\sigma \cdot L$ is unramified at $\sigma \cdot t$. The result then follows from $S \subseteq \mathbb{Q}$.
Pf: [illegible]

(Idea) denote by α_t the automorphism of $\bar{\mathbb{Q}}(T)$ mapping T to $\frac{1}{T-t}$.

For $\sigma \in G_{\mathbb{Q}}$, we have (for the action on coefficients):

$$\sigma \cdot \alpha_t(x) = \alpha_{\sigma(t)}(\sigma \cdot x).$$

The extension $\alpha_t^* L$ is unramified at ∞. So it embeds in $\bar{\mathbb{Q}}((1/T))$, which is stable under the $G_{\mathbb{Q}}$-action on coefficients: so $\sigma \cdot \alpha_t^* L$ is unramified at ∞.

$$\sigma \cdot \alpha_t^* L = \alpha_{\sigma(t)}^* (\sigma \cdot L).$$

So $\sigma \cdot L$ is unramified at $\sigma(t)$.

So we have obtained a morphism:

$$s_\infty : G_{\mathbb{Q}} \to \mathrm{Gal}(\Omega_S \mid \bar{\mathbb{Q}}(T)) = \pi_1.$$

That it is a section of $\pi_1 \to G_{\mathbb{Q}}$ is a tautology. ∎

Note:

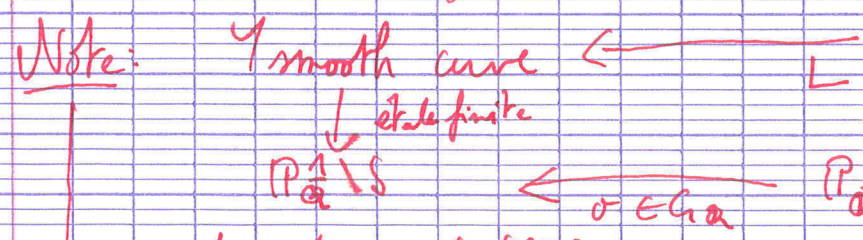
This section lets us define an action of $G_{\mathbb{Q}}$ on $\bar{\pi}_1^g$:

$$\sigma \cdot x = x^{s_\infty(\sigma)} \quad \text{with } s_\infty(\sigma) \in \pi_1 \text{ and } x \in \bar{\pi}_1^g \text{ since } \bar{\pi}_1^g \lhd \bar{\pi}_1.$$

($\sigma \in G_{\mathbb{Q}}$, $x \in \bar{\pi}_1^g$)

Note: This action $G_{\mathbb{Q}} \to \mathrm{Aut}(\bar{\pi}_1^g)$ lifts the outer action $G_{\mathbb{Q}} \to \mathrm{Out}(\bar{\pi}_1^g)$ deduced from the exact sequence. Any other choice of basepoint would give another lift.

Note:



The action (on universal unramified covers, no outer) has a natural geometric origin.

We now state a theorem which we shall use as a black box:

Theorem:

- Each inertia subgroup of $\bar{\pi}_1^g = \mathrm{Gal}(\Omega_S | \bar{\mathbb{Q}}(T))$ is isomorphic to $\hat{\mathbb{Z}}$. One can choose for each $t_i \in S$ a (topological) generator γ_i of the inertia group such that $\gamma_1, \dots, \gamma_n$ generate all of $\bar{\pi}_1^g$ (topologically) with the only relation $\gamma_1 \cdots \gamma_n = 1$.
- ~~such that γ_i is $\bar{\pi}_1^g$-conjugate to $\gamma_j^{\pm 1}$ for all i,j~~
- In particular, $\bar{\pi}_1^g$ is isomorphic to the profinite free group $F_{n-1} \cong \langle \gamma_1, \dots, \gamma_n | \gamma_1 \cdots \gamma_n = 1 \rangle$.

Remark: This defines an action $G_{\mathbb{Q}} \curvearrowright \hat{F}_{n-1}$.
For $n \geq 3$, this action is faithful by Belyi's theorem.
Hence: $G_{\mathbb{Q}} \subseteq \mathrm{Aut}(\hat{F}_2)$.

Trying to reconstruct $G_{\mathbb{Q}}$ as a subgroup of $\mathrm{Aut}(\hat{F}_2)$ is the starting point of SGA.

This theorem relies on deep results from topology, analytic geometry, algebraic geometry

- topology: classification of covers of $\mathbb{P}^1 \setminus S$ by $\pi_1^{\mathrm{top}}(\mathbb{P}^1 \setminus S, \infty)$
- analytic geometry: analytification of covers; Grauert–Remmert: the covers extend to branched covers of $\mathbb{P}^1$
- algebraic geometry: "GAGA principle"; here, Riemann's existence theorem is enough

Riemann's existence theorem: A finite branched cover of $\mathbb{P}^1(\mathbb{C})$ can be algebraized into a finite generically étale cover of $\mathbb{P}^1_{\mathbb{C}}$.

e.g. a polynomial $P(x,t) \in \mathbb{C}[x,t]$

$$\{(x,t) \in \mathbb{C}^2 \mid P(x,t) = 0\} \xrightarrow{(x,t) \mapsto x} \mathbb{C}$$

III

These theorems imply a series of isomorphisms:

$\pi_1^{top}(\mathbb{P}^1(\mathbb{C})\setminus S, \infty)$ — classifies marked covers (topology)

$\pi_1^{for}(\mathbb{P}^1(\mathbb{C})\setminus S, \infty)$ — classifies finite marked covers

$\cong$

$\pi_1^{et}(\mathbb{P}^1_{\bar{\mathbb{Q}}}\setminus S, \infty)$ — classifies finite étale (algebraic) covers

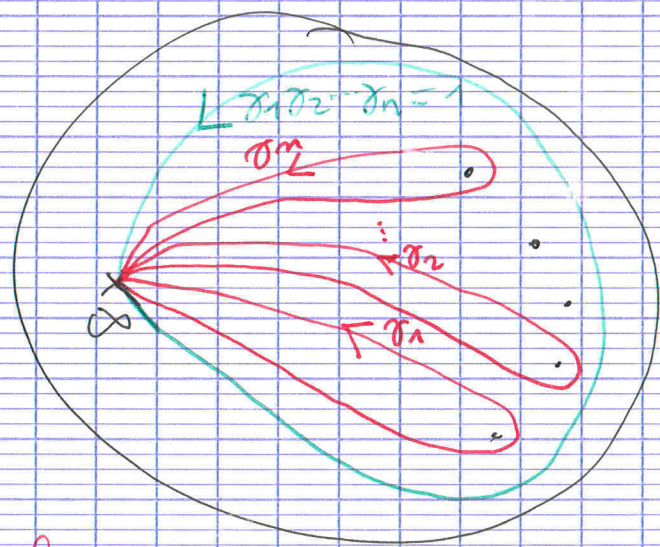
$\cong$

$\pi_1^{et}(\mathbb{P}^1_{\bar{\mathbb{Q}}}\setminus S, \infty)$ — formal argument: if the branch points are algebraic, the coeffs. can be chosen for.

$\cong$

π_1^{g} — comes from the equivalence of categories between smooth curves and function fields.

And $\mathbb{P}^1(\mathbb{C})\setminus S$ has topological fundamental group $\cong \langle \gamma_1, \dots, \gamma_n \rangle / \gamma_1 \cdots \gamma_n$:



We now fix generators $\gamma_1, \dots, \gamma_n$.

Lemma (Fried's branch cycle argument)
Let $t_i \in S$ and γ_i the corresponding generator.
In $\bar{\pi}_1^{\mathbb{Q}}$, $\sigma \cdot \gamma_i$ is conjugate to $\gamma_i^{\chi(\sigma)}$ for all $\sigma \in G_{\mathbb{Q}}$, where $\chi : G_{\mathbb{Q}} \to \hat{\mathbb{Z}}^\times$ is the cyclotomic character.

Pf: We prove it at the level of a finite Galois extension $L \,|\, \bar{\mathbb{Q}}(T)$, $L \subseteq \Omega_S$.

Let e be the ramification index of L at $T - t_i$.

$$\begin{array}{c} \bar{\mathbb{Q}}((\sqrt[e]{T-t_i})) \\ \| \\ L_{T-t_i} \\ | \\ \bar{\mathbb{Q}}((T-t_i)) \end{array}$$

We have:
$$\mathrm{Gal}\left(\bar{\mathbb{Q}}\left(\!\!\left(\sqrt[e]{T-t_i}\right)\!\!\right) \,\middle|\, \bar{\mathbb{Q}}((T-t_i))\right) \simeq \mathbb{Z}/e\mathbb{Z}.$$
(obtained as the projection of γ_i)

Choose the generator ω. We have:
$$\omega\left(\underbrace{\sqrt[e]{T-t_i}}_{\text{uniformizer}}\right) = \underbrace{\zeta_e}_{\substack{\text{a primitive} \\ e\text{-th root of } 1}} \sqrt[e]{T-t_i}.$$

Let $\sigma \in G_{\mathbb{Q}}$. By action on the coefficients, it induces an automorphism $\tilde{\sigma} \in \mathrm{Aut}\left(\bar{\mathbb{Q}}\left(\!\!\left(\sqrt[e]{T-t_i}\right)\!\!\right)\right)$.

We compute $\tilde{\sigma}\omega\tilde{\sigma}^{-1}$ in $\mathrm{Aut}\left(\bar{\mathbb{Q}}\left(\!\!\left(\sqrt[e]{T-t_i}\right)\!\!\right)\right)$:

$$\tilde{\sigma}\omega\tilde{\sigma}^{-1}\left(\sqrt[e]{T-t_i}\right) = \tilde{\sigma}\omega\left(\sqrt[e]{T-t_i}\right) = \tilde{\sigma}\left(\zeta_e \sqrt[e]{T-t_i}\right)$$
$$= \zeta_e^{\chi(\sigma)} \sqrt[e]{T-t_i};$$

so $\tilde{\sigma}\omega\tilde{\sigma}^{-1} = \omega^{\chi(\sigma)}$ in $\mathrm{Aut}(L_{T-t_i})$.

so $\tilde{\sigma}\gamma_i\tilde{\sigma}^{-1} = \gamma_i^{\chi(\sigma)}$ in $\mathrm{Aut}\left(\bar{\mathbb{Q}}\left(\!\!\left(\sqrt[e]{T-t_i}\right)\!\!\right)\right)$.

not "our" Galois action, but the one corresponding to the splitting $t_i \Rightarrow$ hence only conjugate

Proposition:

A morphism $\varphi : \bar{\pi}_1^g \to G_1$ extends to a morphism $\tilde{\varphi} : \bar{\pi}_1 \to G_1$ (necessarily surjective) if and only if there exist a group morphism $\gamma : G_{\mathbb{Q}} \to G_1$ such that (Δ)

$$\forall \sigma \in G_{\mathbb{Q}}, \forall x \in \bar{\pi}_1^g, \quad \varphi(x^{s_\infty(\sigma)}) = \varphi(x)^{\gamma(\sigma)} \quad (\bullet)$$
$$= \gamma(\sigma)\, \varphi(x)\, \gamma(\sigma)^{-1}$$

Proof:

$(\Rightarrow)$ $\varphi(x^{s_\infty(\sigma)}) = \tilde{\varphi}(x^{s_\infty(\sigma)}) = \tilde{\varphi}(x)^{\tilde{\varphi}(s_\infty(\sigma))} = \varphi(x)^{\tilde{\varphi}(s_\infty(\sigma))}$

It suffices to let: $\gamma(\sigma) = \tilde{\varphi}(s_\infty(\sigma))$.

$(\Leftarrow)$ Write: $1 \to \bar{\pi}_1^g \subseteq \bar{\pi}_1 \xrightarrow{\tau} G_{\mathbb{Q}} \to 1$, with s_∞ a section of τ.

If $x \in \bar{\pi}_1$, then $x(s_\infty \tau(x))^{-1} \in \bar{\pi}_1^g$.

We define:

$$\tilde{\varphi}(x) = \varphi\left(x(s_\infty\tau(x))^{-1}\right)(\gamma\tau(x)) \quad (\diamond)$$

which is a map $\bar{\pi}_1 \to G_1$ extending φ.

Why is this a group morphism?

$$\tilde{\varphi}(xy) \overset{(\diamond)}{=} \varphi\left(xy(s_\infty\tau(xy))^{-1}\right)(\gamma\tau(xy)) \overset{(\Delta)}{=}$$
$$= \varphi\left[x(s_\infty\tau(x))^{-1}\,(s_\infty\tau(x))\,y(s_\infty\tau(y))^{-1}(s_\infty\tau(x))^{-1}\right]\gamma\tau(x)\,\gamma\tau(y)$$
($\diamond$) on the first factor; ($\bullet$), ($\diamond$) on the second factor
$$= \varphi(x)\,(\gamma\tau(x))^{-1}\,(\gamma\tau(x))\left[\varphi(y)(\gamma\tau(y))^{-1}\right](\gamma\tau(x))^{-1}\,\gamma\tau(x)\,\gamma\tau(y)$$
$$= \varphi(x)\,\tilde{\varphi}(y). \qquad \blacksquare$$

"extensions of $\bar{\mathbb{Q}}(T)$ fixed by the $G_{\mathbb{Q}}$-actions ⟷ extensions of $\bar{\mathbb{Q}}(T)$"

Corollary:

Assume $id: Z(G) \to Z(G)$ extends to a $r: G \to Z(G)$ i.e. $Z(G)$ is a direct factor of G; e.g. G abelian or $Z(G)=1$. Then a morphism $\varphi: \pi_1^{\mathbb{Q}} \twoheadrightarrow G$ extends to $\tilde{\varphi}: \pi_1 \twoheadrightarrow G$ if and only if for all $\sigma \in G_{\mathbb{Q}}$, there exists a $\gamma \in G$ such that:

$$\forall t_i \in S, \quad \varphi(\gamma_i^{s_{ab}(\sigma)}) = \varphi(\gamma_i)^{\gamma(\sigma)}. \quad (\bullet)'$$

pf: We need to transform the map $\gamma: G_{\mathbb{Q}} \to G$ into a morphism $\tilde{\gamma}$ such that it still satisfies $(\bullet)'$.

Since φ is surjective, $\varphi(x)^{\sigma} = \varphi(x)^{\gamma'}$ $\forall x \in \bar{\pi}_1^{\mathbb{Q}}$ happens if and only if $\gamma\gamma' \in Z(G)$.

$$1 \to Z(G) \to G \to \mathrm{Inn}(G) \to 1.$$
$$\qquad\qquad\quad \overleftarrow{\qquad r \qquad}$$

- There is a morphism $f: \mathrm{Inn}(G) \to G$ splitting this sequence, defined like so:

  if $\alpha \in \mathrm{Inn}(G)$ and $\tilde{\alpha}$ is a lift in G, then $f(\alpha) = \tilde{\alpha} r(\tilde{\alpha})^{-1}$.

  Indeed, if $\tilde{\alpha} z$ ($z \in Z(G)$) is another lift then $\tilde{\alpha} z\, r(\tilde{\alpha} z)^{-1} = \tilde{\alpha} z z^{-1} r(\tilde{\alpha})^{-1} = \tilde{\alpha} r(\tilde{\alpha})^{-1}$.

  So this morphism is well-defined.

Let $\tilde{\gamma}(\sigma) = f(\gamma(\sigma) \bmod Z(G)): G_{\mathbb{Q}} \to G$.

To check that $\tilde{\gamma}$ is a morphism, it suffices to check that $\gamma(\sigma) \bmod Z(G): G_{\mathbb{Q}} \to \mathrm{Inn}(G)$ is a morphism. But:

$$\varphi(x)^{\gamma(\sigma\sigma')} = \varphi(x^{s_{ab}(\sigma\sigma')}) = \varphi((x^{s_{ab}(\sigma')})^{s_{ab}(\sigma)}) = \varphi(x^{s_{ab}(\sigma')})^{\gamma(\sigma)} = \varphi(x)^{\gamma(\sigma)\gamma(\sigma')}$$

so $\gamma(\sigma\sigma') = \gamma(\sigma)\gamma(\sigma') \bmod Z(G)$. ∎

III

II. Rationality.

G a finite group

Def: A conjugacy class $c \subseteq G$ is *rational* (more generally: K-rational for $K \neq$ field) if $c_\ell = c$ for all ℓ coprime with $\exp(c)$.
(more generally: for $\ell \in \mathrm{Im}(\chi : G_K \to \hat{\mathbb{Z}}^\times)$)

Prop: A conjugacy class $c \subseteq G$ is rational (resp. K-rational) if and only if its image by every character is rational (resp. $\in K$)

Pf: Let $N = \exp(G)$ and $\Gamma = (\mathbb{Z}/N\mathbb{Z})^\times$.

~~$\lambda \in \Gamma$ acts on a conjugacy class by a character χ~~

$\lambda \in \Gamma$ acts on $\chi(c) \in \mathbb{Q}(\mu_N)$ via its natural action on μ_N.

Claim: $\lambda \cdot \chi(c) = \chi(c^\lambda)$.

Pf: $\chi = \mathrm{Tr}(\rho)$, $g \in c$. We have $\rho(g^\lambda) = \rho(g)^\lambda$.
Since $\rho(g)^N = \rho(g^N) = \rho(1) = \mathrm{Id}$, the eigenvalues of $\rho(g)$ belong to μ_N. Let $\alpha_1, \dots, \alpha_d$ be the eigenvalues w/ multiplicity.

$$\chi(c^\lambda) = \chi(g^\lambda) = \mathrm{Tr}(\rho(g^\lambda)) = \mathrm{Tr}(\rho(g)^\lambda) = \sum \underbrace{\alpha_i^\lambda}_{=\lambda \cdot \alpha_i} = \lambda \cdot \sum \alpha_i = \lambda \cdot \mathrm{Tr}(\rho(g)) = \lambda \cdot \chi(c).$$

By taking the particular case $\lambda = \chi(\sigma) \bmod N$ for $\sigma \in G_{\mathbb{Q}}$, and using that two conj. classes are equal iff all characters coincide on them (follows e.g. from orthogonality relations), the result follows.

Prop: If $\tilde{\varphi} : \pi_1 \to G$, then the conjugacy class of $\tilde{\varphi}(\gamma_i)$ is rational.

Pf: We have: $\tilde{\varphi}(\gamma_i)^{\chi(\sigma)} = \tilde{\varphi}(\gamma_i^{\chi(\sigma)})$ which is conjugate to $\tilde{\varphi}(\gamma_i^{s_\infty(\sigma)}) = \tilde{\varphi}(\gamma_i)^{\tilde{\varphi}(s_\infty(\sigma))}$.

+ Natural generalization to extensions of $K(T)$.
(w) monodromy classes are K-rational)

III. The rigidity criterion.

Definition: A list $C = (C_1, \dots, C_n)$ of conjugacy classes of G is *rigid* if there exists a tuple $(g_1, \dots, g_n) \in G^n$ such that:

(i) $g_1 \in C_1, \dots, g_n \in C_n$

(ii) $g_1 \cdots g_n = 1$

(iii) $g_1, \dots, g_n$ generate G.

(iv) For each tuple $(g'_1, \dots, g'_n) \in G^n$ satisfying (i)–(iii), there is a $\gamma \in G$ such that $\forall i \in \{1, \dots, n\}$, $g'_i = g_i^{\gamma}$.
(i.e. $(g_1, \dots, g_n)$ is unique up to conjugacy).

Theorem: Assume that $Z(G)$ is a direct factor of G.
Let C be a rigid tuple of n rational conjugacy classes of G.
Then there exists a surjective morphism $\tilde{\varphi} : \pi_1 \twoheadrightarrow G$ mapping γ_i to g_i as in the definition.
In particular: G is the Galois group of a Galois extension of $\mathbb{Q}(T)$, regular and unramified outside S.

Note: In particular, by Hilbert's irreducibility theorem, G is then a Galois group over $\mathbb{Q}$.

Proof of the theorem:

Recall that $\pi_1^g \simeq \langle \gamma_1, \dots, \gamma_n \rangle / \gamma_1 \cdots \gamma_n$.
Define φ as the only continuous morphism $\pi_1^g \twoheadrightarrow G$ mapping γ_i to the elements g_i from the definition of rigidity.
Let $\sigma \in G_{\mathbb{Q}}$, and define $g'_i = \varphi(\gamma_i^{\chi(\sigma)})$.

We have:

(i) $g_i' = \varphi(\gamma_i^{s_\infty(\sigma)})$. Since $\gamma_i^{s_\infty(\sigma)}$ is conjugate to $\gamma_i^{\gamma(\sigma)}$, g_i' is conjugate to $g_i^{\gamma(\sigma)}$, and thus to g_i since c_i is rational.
So: $\boxed{g_i' \in c_i}$.

(ii) $\boxed{g_1' \cdots g_n' = \varphi(\gamma_1^{s_\infty(\sigma)}) \cdots \varphi(\gamma_n^{s_\infty(\sigma)}) = \varphi((\gamma_1 \cdots \gamma_n)^{s_\infty(\sigma)})}$
$= \varphi(1^{s_\infty(\sigma)}) = 1.$

(iii) $\boxed{\langle g_1', -, g_n' \rangle = \langle \varphi(\gamma_1^{s_\infty(\sigma)}), -, \varphi(\gamma_n^{s_\infty(\sigma)}) \rangle = \varphi(\langle \gamma_1, -, \gamma_n \rangle^{s_\infty(\sigma)})}$
$= \varphi((\pi_1^g)^{s_\infty(\sigma)}) = \varphi(\pi_1^g) = G_-$

By rigidity: there exists a $\gamma(\sigma) \in G$ such that:
$\forall i \in \{1, -, n\}$, $g_i' = g_i^{\gamma(\sigma)}$.
By an earlier proposition, this implies that φ extends to a morphism $\tilde{\varphi}: \tilde{\pi}_1 \to G$ which corresponds to a G-extension of $\mathbb{Q}(T)$, included in Ω_S (i.e., unramified outside S), and regular because $\tilde{\varphi}|_{\tilde{\pi}_1^g}$ is already surjective. ▨

Remark: Rationality can be relaxed if S is not assumed to be $\subseteq \mathbb{Q}$.
$\rightsquigarrow$ we need only $c_i^{\gamma(\sigma)} = c_j$ where $t_j = \sigma \cdot t_i$.
The cyclotomic action defines a morphism $G_a \to \mathfrak{S}_C$.
If one realizes $G_a \to \mathfrak{S}_C$ as the permutation representation of a Galois extension of degree $|C|$, and let S be the roots.
($S \subseteq \mathbb{Q}$ is the particular case $\{\sigma \mapsto id\}$)

The "true" necessary condition is that the tuple C is "globally" rational... but general situations may require solving an inverse Galois problem.

Examples:

0) 2-torsion abelian groups ($\mathbb{F}_2$-vector spaces)
→ immediate!
(For general abelian groups: rigidity is obvious, rationality is a problem).
ok in a cyclotomic ext^{n}

1) $G_1 = \mathfrak{S}_n$: $Z(G)=1$ $\quad c_1$ = transpositions; c_2 = n-cycles; c_3 = $n-1$-cycles

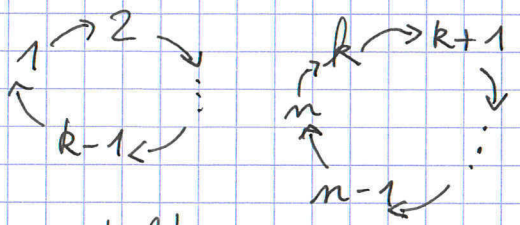
* All these classes are rational:
  — transpositions ⇝ classes of involutions are always rational
  — only one class of elements of order n & $n-1$.

* Rigid? $\quad (g_1, g_2, g_3) \in c_1 \times c_2 \times c_3$

WLOG (conjugate everything by a permutation)
$g_2 = (1 \ \cdots \ n)$

WLOG (conjugate everything by a power of $(1 \cdots n)$)
$g_1 = (1 \ \ k)$

To have $g_1 g_2 g_3 = 1$, we must have $(1\ k)(1\ 2 \cdots n)$ is an $(n-1)$-cycle:



Only two possibilities: $k=2$ or $k=n$.

WLOG (conjugate by $(1\ 2 \cdots n)$)
$g_1 = (1 \ \ 2)$

But then $g_3 = (g_1 g_2)^{-1} = (2 \ \ n \ \ n-1 \ \cdots \ 3)$.

⇒ G_n is a Galois group over $\mathbb{Q}(T)$, ramified at 3 places.

IV

IV. How to check rigidity from a character table.

G a finite group; $C_1, \dots, C_n$ conjugacy classes.

$\overline{\Sigma} = \{(g_1, \dots, g_n) \in \prod C_i \mid g_1 \cdots g_n = 1\}$. $\Sigma = \{(g_1, \dots, g_n) \in \overline{\Sigma} \mid \langle g_1, \dots, g_n \rangle = G\}$.

If $Z(G) = 1$, then the conjugacy action of G on Σ is free. ($\triangle$ not on $\overline{\Sigma}$).

(Pf: if $(g_1, \dots, g_n)^\gamma = (g_1, \dots, g_n)$ then $[\gamma, g_i] = 1 \ \forall i \Rightarrow \gamma$ commutes w/ $\langle g_1, \dots, g_n \rangle = G$.)

($Z(G) = 1$) $C_1, \dots, C_n$ rigid $\Leftrightarrow \Sigma \neq \emptyset$ and G acts transitively on Σ

$\Leftrightarrow |\Sigma| = |G|$.

Def: $(C_1, \dots, C_n)$ strictly rigid if rigid and $\Sigma = \overline{\Sigma}$.

i.e. one does not need to check $\langle g_1, \dots, g_n \rangle = G$, $\forall$.

our $\mathfrak{S}_n$ - example.

Theorem:
$$|\overline{\Sigma}| = \frac{|C_1| \cdots |C_n|}{|G|} \sum_{\substack{\chi \text{ irred.} \\ \text{char.}}} \frac{\chi(C_1) \cdots \chi(C_n)}{\chi(1)^{n-2}}$$

$$= \frac{|G|^{n-1}}{|Z_1| \cdots |Z_n|} \sum_{\chi} \frac{\chi(C_1) \cdots \chi(C_n)}{\chi(1)^{n-2}}$$

($|Z_1|, \dots, |Z_n|$: centralizers of an elt of C_i)

Note: this does not help with $|\Sigma|$! (generation)

For this, we need to use our knowledge of subgroups of G.

Proof: Choose representatives $g_i \in C_i$. Let $Z_i \leq G$ be the centralizer of g_i. Let $\delta(x) = \begin{cases} 1 \text{ if } x = 1 \\ 0 \text{ otherwise} \end{cases}$. We have:

$$\sum_{\gamma_1, \dots, \gamma_n \in G} \delta(g_1^{\gamma_1} \cdots g_n^{\gamma_n}) = \left(\prod_i |Z_i|\right) |\overline{\Sigma}| = \frac{|G|^n}{\prod_i |C_i|} |\overline{\Sigma}|.$$

So we only need to show:

$$\sum_{\gamma_1, \dots, \gamma_n \in G} \delta(g_1^{\gamma_1} \cdots g_n^{\gamma_n}) = |G|^{n-1} \sum_{\substack{\chi \text{ irred} \\ \text{char}}} \frac{\chi(C_1) \cdots \chi(C_n)}{\chi(1)^{n-2}}.$$

Schur's orthogonality relations:

$$\sum_{\chi} \chi(g)\overline{\chi(h)} = \begin{cases} |C_G(g)| & \text{if } g,h \text{ conjugate} \\ 0 & \text{otherwise} \end{cases}$$

In particular: $\sum_{\chi} \chi(g)\chi(1) = \begin{cases} |G| & \text{if } g=1 \\ 0 & \text{otherwise} \end{cases}$

So: $\delta(x) = \frac{1}{|G|}\sum_{\chi} \chi(g)\chi(1)$.

Therefore, it suffices to show the following:

Lemma: Let $\chi = \mathrm{Tr}(\rho)$ be a character, with $\rho: G \to GL(V)$ irreducible.

Then $\frac{1}{|G|^n} \sum_{g_1 \cdots g_n = 1 \in G} \chi(g_1^{\sigma_1} \cdots g_n^{\sigma_n}) = \frac{\chi(C_1)\cdots\chi(C_n)}{\chi(1)^{n-1}}$.

Proof: By induction on n ($\forall g_1, \dots, g_n$).

$n=1$: **Sublemma:** $\frac{1}{|G|}\sum_{g\in G} \rho(x^g) = \frac{\chi(x)}{\chi(1)} I$.

Pf: Let $f_x = \frac{1}{|G|}\sum_{g\in G} \rho(x^g) \in \mathrm{End}_G(V)$. Then:

$$\forall y \in G,\ f_x \rho(y) = \frac{1}{|G|}\sum_{g\in G} \rho(x^g y) = \frac{1}{|G|}\sum_{g} \rho(y x^{y^{-1}g}) \overset{g := yg}{=} \frac{1}{|G|}\sum_{g} \rho(y x^g) = \rho(y) f_x.$$

Over $\mathbb{C}$, f_x has an eigenvalue λ. Let $\tilde{f}_x = f_x - \lambda I$, which has $\ker(\tilde{f}_x) \neq 0$ and $\tilde{f}_x \rho(g) = \rho(g)\tilde{f}_x$.

So $\ker(\tilde{f}_x)$ is a stable subset under ρ

(Pf: if $\tilde{f}_x(v) = 0$ then $\tilde{f}_x(\rho(g)(v)) = \rho(g)(\tilde{f}_x(v)) = 0$).

Since ρ is irreducible and $\ker(\tilde{f}_x) \neq 0$, we have $\ker \tilde{f}_x = V$

so $\tilde{f}_x = 0$. Hence $f_x = \lambda I$.

Taking traces: $\mathrm{Tr}(f_x) = \lambda\chi(1) \rightsquigarrow \lambda = \frac{\chi(x)}{\chi(1)}$.

($\mathrm{Tr}(f_x) = \frac{1}{|G|}\sum_g \chi(x^g) = \chi(x)$)

Thus: $f_x = \frac{\chi(x)}{\chi(1)} I$.

~~Taking traces in the subdemma:~~

$n=1$: $\frac{1}{|G|}\sum_{g_1\in G}\chi(g_1^{\gamma_1}) = \chi(g_1) = \frac{\chi(g_1)}{\chi(1)^0}$.

$n\geq 2$: Assume the result for $n-1$. Then:

$$\frac{1}{|G|^n}\sum_{\gamma_1,\dots,\gamma_n\in G}\chi(g_1^{\gamma_1}\cdots g_n^{\gamma_n})$$

$$=\frac{1}{|G|^{n-1}}\sum_{\gamma_1,\dots,\gamma_{n-1}\in G}\mathrm{Tr}\left(\frac{1}{|G|}\sum_{\gamma_n\in G}\rho(g_1^{\gamma_1}\cdots g_n^{\gamma_n})\right)$$

~~Set a field $\beta=(\gamma_1,\dots,\gamma_{n-1})\in G^{n-1}$, set~~

~~$x=\frac{1}{|G|}\sum_{\gamma_n\in G}\rho(g_1^{\gamma_1}\cdots g_n^{\gamma_n})$.~~

(Sudemma)
$$=\frac{1}{|G|^{n-1}}\sum_{\gamma_1,\dots,\gamma_{n-1}\in G}\mathrm{Tr}\left(\rho(g_1^{\gamma_1}\cdots g_{n-1}^{\gamma_{n-1}})\frac{\chi(g_n)}{\chi(1)}I\right)$$

$$=\frac{\chi(g_n)}{\chi(1)}\times\frac{1}{|G|^{n-1}}\sum_{\gamma_1,\dots,\gamma_{n-1}\in G}\chi(g_1^{\gamma_1}\cdots g_{n-1}^{\gamma_{n-1}})$$

(Induction hypothesis)
$$=\frac{\chi(g_n)}{\chi(1)}\times\frac{\chi(c_1)\cdots\chi(c_{m-1})}{\chi(1)^{n-2}}=\frac{\chi(c_1)\cdots\chi(c_n)}{\chi(1)^{n-1}}.$$

V. Examples.

Remark: $H=\langle\sigma_1,\dots,\sigma_n\rangle$, $\sigma_1\cdots\sigma_n=1$ OF (pairwise) COPRIME ORDERS.
Then H is perfect.

Pf: $H^{ab}=\langle\bar\sigma_1,\dots,\bar\sigma_n\rangle$ w/ $\bar\sigma_1\cdots\bar\sigma_n=1$; copime orders.
$H^{ab}=\langle\bar\sigma_1,\dots,\widehat{\bar\sigma_j},\dots,\bar\sigma_n\rangle$ so $|H^{ab}|\mid a_1\cdots\hat a_j\cdots a_n$. $a_1,\dots,a_n$

$\bigwedge_{j=1}^{n} a_1\cdots\hat a_j\cdots a_n=1$ so $|H^{ab}|=1$.

⇝ Can be used to restrict the possibilities for subgroups.

M = Monster group ($Z(G) = 1$ because M simple)

Triple $(2A, 3B, 29A)$ of rational classes.

Using the character table and the formulas, we get $|\Sigma| = |M|$.

The problem is to check strict rigidity.

Assume $g_1, g_2, g_3 \in 2A \times 3B \times 29A$ generate a $H \subsetneq M$.
$g_1 g_2 g_3 = 1$

Let S be a simple quotient of G. It is generated by $\bar{g}_1, \bar{g}_2, \bar{g}_3$.

If $\bar{g}_1 = 1$, then $\bar{g}_2 = \bar{g}_3$ (non-trivial) which implies $\bar{g}_2 = \bar{g}_3 = 1$ because of coprime orders. So $\bar{g}_1 \neq 1$; similarly $\bar{g}_2 \neq 1$ and $\bar{g}_3 \neq 1$.

So S is a simple group of order a multiple of $2 \times 3 \times 29$ generated by elements of order 2, 3, 29 — One can use the classification of finite simple groups (!) to check that this is not possible.