Galois Code for arithmetic and geometry through the power of valuation theory

§ 0 Three Galois conjectures about $\mathbb{Q}$

K field $\rightsquigarrow$ $G_K = Gal(K^{sep}/K) = Aut(\bar{K}/K) = \varprojlim_{L/K \text{ fin. Gal.}} Gal(L/K)$

"absolute Galois group"

Example $G_{\mathbb{C}} = 1$, $G_{\mathbb{R}} = \mathbb{Z}/2\mathbb{Z}$, $G_{\mathbb{Q}} = ?$

Neukirch: K #-fields & $G_K \cong G_{\mathbb{Q}}$ $\Leftrightarrow$ $K = \mathbb{Q}$

Top: K f.g./$\mathbb{Q}$

AGC: Absolute Galois Conjecture (Kamy field)

$G_K \cong G_{\mathbb{Q}} \Leftrightarrow \exists$ hens. val. v with vK div. & $Kv = \mathbb{Q}$

Example: $K = \mathbb{Q}$ or $K = \mathbb{Q}((\mathbb{Q})) \equiv \bigcup_n \mathbb{Q}((t^{\frac{1}{n}}))$

Consequence of AGC

$G_K \cong G_{\mathbb{Q}}$ & $\mathcal{C}(K) = \mathcal{C}(\mathbb{Q})$, $\Leftrightarrow K = \mathbb{Q}$

where $\mathcal{C}: y^2 = x(x^2+1)$

Theorem 1

$G_K \cong G_{\mathbb{Q}}$ & $\forall a \in \mathbb{Q}^\times: \mathcal{C}_a(K) = \mathcal{C}_a(\mathbb{Q})$, $\Leftrightarrow K = \mathbb{Q}$

where $\mathcal{C}_a: y^2 = a \cdot x \cdot (x^2-1)(x^2-4)$

Corollary (Faltings)

$(G_K \cong G_{\mathbb{Q}}$ & $K \equiv_\forall \mathbb{Q}) \Leftrightarrow K = \mathbb{Q}$

EGC: Elementary Galois Conjecture (Kamy field)

$G_K \equiv G_{\mathbb{Q}} \Leftrightarrow \exists$ hens. val. v with vK div. & $Kv \equiv \mathbb{Q}$

in the language of profinite groups a la Chatzidakis, van Dries, Macintyre

Consequence of AGC

$G_K \equiv G_{\mathbb{Q}}$ & $\mathcal{C}(K) = \mathcal{C}(\mathbb{Q})$ $\Leftrightarrow K \equiv \mathbb{Q}$
(C as above)

In part., "$Th(\mathbb{Q}) = Th(G_{\mathbb{Q}}) + \forall x,y\ (x=0 \vee y^2 \neq x(x^2+1))$"
(+ field axioms)

and so $Th(G_{\mathbb{Q}})$ is undecidable.

BSC: Birational Section Conjecture (Grothendieck)

$\mathcal{C}$ smooth proj. curve over $\mathbb{Q}$ with fct. fld. $F = \mathbb{Q}(\mathcal{C})$
$\Rightarrow$ every section s of res.: $G_F \twoheadrightarrow G_{\mathbb{Q}}$ ($s: G_{\mathbb{Q}} \dashrightarrow G_F$)
comes from a $\mathbb{Q}$-rational point $P \in \mathcal{C}(\mathbb{Q})$,
i.e. $s(G_{\mathbb{Q}}) \subseteq D_P :=$ a decomp. subgp. of G_F w.r.t. P

(Hope: $\rightsquigarrow$ effective Faltings; cf. Minhyong Kim 2010)
best evidence (Stix Invent. 2015): BSC true for some special curves $\mathcal{C}$

N.B.: Mochizuki proved "fundamental Conj. in bir. anabelian geom.":
$G_F \twoheadrightarrow G_{\mathbb{Q}}$ "knows" F and $\mathbb{Q}$ up to iso.

Theorem 2: EGC $\Rightarrow$ AGC $\Leftrightarrow$ BSC

§1 The local picture

All three conjectures are true locally (i.e. for $\mathbb{R}$ & for all $\mathbb{Q}_p$):

$$G_K \equiv \begin{matrix} G_{\mathbb{R}} \\ \diagdown\!\diagup \\ G_{\mathbb{Q}_p} \end{matrix} \Leftrightarrow G_K \equiv \begin{matrix} G_{\mathbb{R}} \\ \diagdown\!\diagup \\ G_{\mathbb{Q}_p} \end{matrix}$$

$$\Leftrightarrow K \overset{\text{real}}{\underset{p\text{-adically}}{\quad}} \text{closed}$$

$$\Leftrightarrow K \equiv \begin{matrix} \mathbb{R} \\ \diagdown\!\diagup \\ \mathbb{Q}_p \end{matrix}$$

$\Leftrightarrow \exists$ henselian val. v on K with vK divisible
and $Kv \subseteq \begin{matrix} \mathbb{R} \text{ \& real closed} \\ \diagdown\!\diagup \\ \mathbb{Q}_p \text{ \& } p\text{-adically closed} \end{matrix}$
$\mathcal{O}_v = \begin{matrix} \text{the convex hull of } \mathbb{Z} \text{ in } K \\ \diagdown\!\diagup \\ \mathcal{O}_{v_p}\left[\frac{1}{p}\right] =: \mathcal{O}_{\tilde{v}_p} \end{matrix}$

Examples: $K = \mathbb{Q}_p$, $K = \mathbb{Q}_p^{alg} := \mathbb{Q}_p \cap \overline{\mathbb{Q}}$ (both with v trivial)
or $K = \mathbb{Q}_p((\mathbb{Q}))$ (v non-trivial)

Note: $G_K \cong G_{\mathbb{Q}_p}$ respects inertia & ram. subgps.

§ 2 From local to global

Proposition (K any field)

Assume $G_K \cong G_{\mathbb{Q}}$. Then:

(1) $\operatorname{char} K = 0$ and $\operatorname{res}: G_K \to G_{\mathbb{Q}}$ is an isomorphism

(2) For each prime p, $\exists!$ p-adic val. v_p on K
& $\exists!$ ordering $\leq_K$ on K

(3) w.r.t. these v_p and $\leq_K$, K satisfies most thms of alg. #-theory:
- only finitely many primes ramify in finite L/K
- Čebotarev density thm.
- Hasse-Minkowski LGP
- Quadratic reciprocity law: $\prod_p (a,b)_p = 1$
- Kronecker-Weber
- 4 squares Thm.

"**Proof**": Set for $\varphi: G_K \xrightarrow{\cong} G_{\mathbb{Q}}$ and any prime p,

$$K_p := \operatorname{Fix} \varphi^{-1}\left(G_{\mathbb{Q}_p^{alg}}\right). \quad \text{Then}$$

$$\Rightarrow \left\langle G_{K_p} \mid p \in \mathbb{P} \right\rangle = G_K \xrightarrow[\cong]{\varphi} G_{\mathbb{Q}} = \left\langle G_{\mathbb{Q}_p^{alg}} \mid p \in \mathbb{P} \right\rangle$$

$$\begin{array}{ccc} \wr & & \wr \\ G_{K_p} & \xrightarrow[\cong]{} & G_{\mathbb{Q}_p^{alg}} \end{array} \quad \ldots$$

for (1)(b) use: $\exists$ only finitely many $L/\mathbb{Q}$ (i.e. L'/K) of degree $\leq n$, ramifying only at p's $\leq n$ ∎

Pf. of Thm. 1: $G_K \cong G_{\mathbb{Q}}$ & $K \neq \mathbb{Q}$
$\Rightarrow$ for $x \in K \setminus \mathbb{Q}$, by Prop. (1)(b), $\exists\, a \in \mathbb{Q}^\times, y \in K$ s.t. $(x,y) \in \mathcal{C}_a(K) \setminus \mathcal{C}_a(\mathbb{Q})$ ∎

Pf. of Thm. 2: • EGC $\Rightarrow$ AGC by Prop. (1)(b)

• AGC $\Rightarrow$ BSC: easy

• BSC $\Rightarrow$ AGC: $\forall L$ with $\mathbb{Q} \subseteq L \subseteq K$ rel. alg. cl. (& $t.d.\, L/\mathbb{Q} = 1$) get

$$G_K \xrightarrow{\cong} G_L \xrightarrow[\text{res}]{\cong} G_{\mathbb{Q}}$$

and, by BSC (= AGC for all such L): $\forall p \neq q$: $\{0\} \neq m_{\tilde{v}_p} = m_{\tilde{v}_q}$ on L
$\Rightarrow$ $\tilde{v}_p^k$ on K
$\Rightarrow v = \tilde{v}_p^k$ does it. ∎

§ 3 Towards Effectiveness

The (model theoretic) EGC requires more effectivity, as one needs explicit degree bounds.

Partial result in this direction

Philip Dittmann (2015)

$G_K \equiv G_{\mathbb{Q}} \Rightarrow$ For each prime p, $\exists!$ p-adic val. on K & $\exists!$ ordering $\leq_K$ on K

($\equiv$ in language augmented by "ver")

Pf. finds, e.g., degree bounds $d(n)$ for involutions in a Gal. ext. L/K of degree n to guarantee that they lift (conjugate) to involutions in extensions M/K above L/K of degree $\leq d(n)$. —

Pop-Stix: finite conditions for p-adic valuations ($\mathbb{Z}/p$-metabelian quotients of $G_{\mathbb{Q}_p}$...)

K.-Stommen (2015) finite Demushkin quotient of $G_{\mathbb{Q}_2}$...