Infinite Galois Theory

June 11, 2020

Galois Group of p-Power Cyclotomic Extension of $\mathbf{Q}$

For prime p, $\mathrm{Gal}(\mathbf{Q}(\zeta_{p^\infty})/\mathbf{Q})$ has two concrete descriptions:

$$\{x = (a_1 \bmod p, a_2 \bmod p^2, \ldots) : a_n \equiv a_{n-1} \bmod p^{n-1}, a_1 \not\equiv 0 \bmod p\},$$

$$\{x = c_0 + c_1 p + c_2 p^2 + \cdots : 0 \le c_n \le p-1, c_0 \neq 0\},$$

with x acting on finite layer $\mathbf{Q}(\zeta_{p^n})$ by

$$\zeta_{p^n} \mapsto \zeta_{p^n}^x = \zeta_{p^n}^{a_n} = \zeta_{p^n}^{c_0 + c_1 p + \cdots + c_{n-1}p^{n-1}}.$$

In terminology of p-adic integers, $\mathrm{Gal}(\mathbf{Q}(\zeta_{p^\infty})/\mathbf{Q}) \cong \mathbf{Z}_p^\times$.

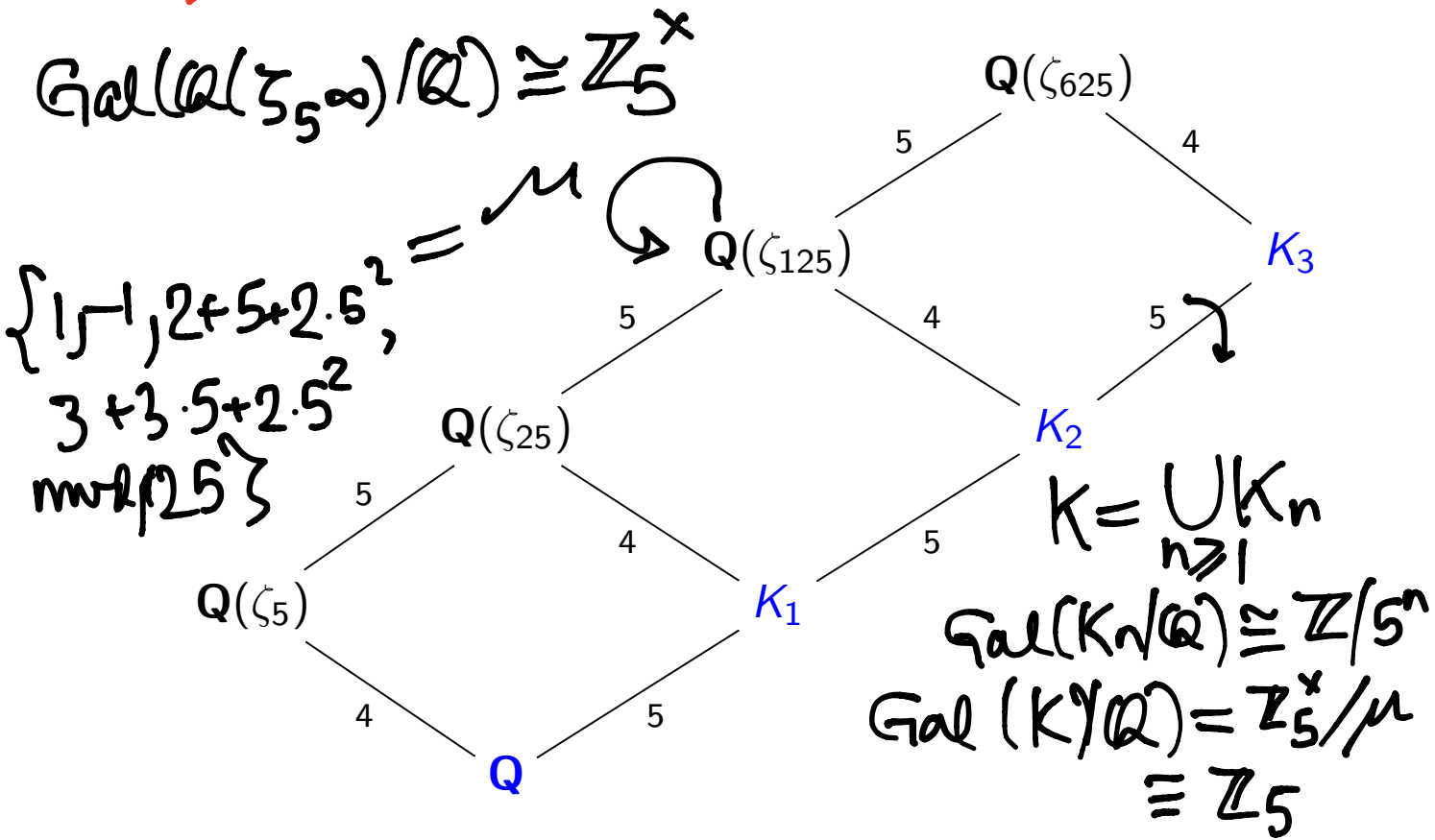
Example. From Lecture 1, $\mathrm{Gal}(\mathbf{Q}(\zeta_{2^\infty})/\mathbf{Q})$ has two different subgroups $\langle 5 \rangle$ and $\langle 13 \rangle$ with the same fixed field $\mathbf{Q}(i)$.

Theorem. In $\mathbf{Z}_2^\times$, $\overline{\langle 5 \rangle} = \overline{\langle 13 \rangle} = 1 + 4\mathbf{Z}_2$. How is 5 a 2-adic limit point of $\langle 13 \rangle$? Check $5 = 13^x$ for $x = 1 + 2 + 2^2 + 2^3 + 2^8 + \cdots$, which is ~~$\log(13)/\log(5)$~~ using 2-adic logarithm series.

A $\mathbf{Z}_5$-extension of $\mathbf{Q}$

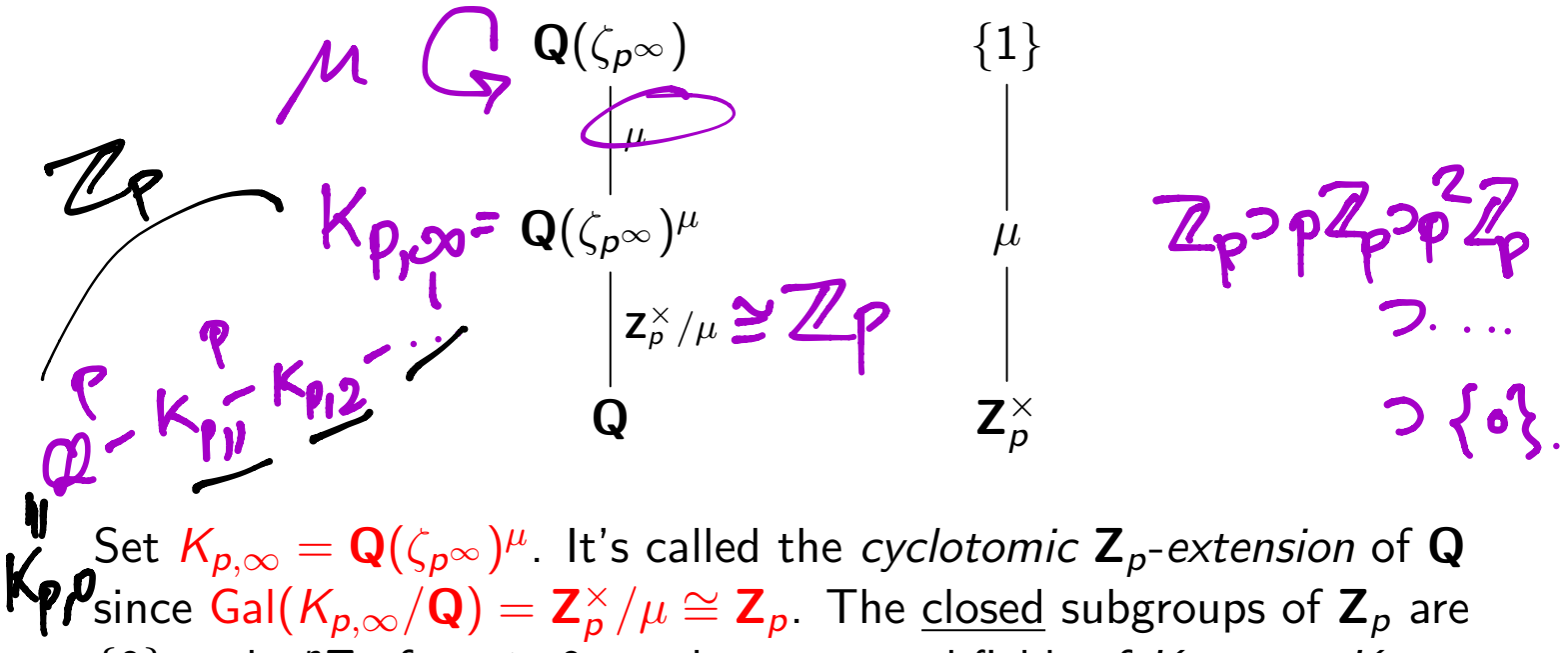
For $n \in \mathbf{Z}^+$, $(\mathbf{Z}/5^{n+1}\mathbf{Z})^\times = \mu \times \langle 1 + 5 \bmod 5^{n+1} \rangle$. Make $n \to \infty$: $\mathbf{Z}_5^\times = \mu \times \overline{\langle 1+5 \rangle} = \mu \times (1 + 5\mathbf{Z}_5)$, where

$$\mu = \{1, -1, 2+5+2\cdot 5^2+5^3+\cdots, 3+3\cdot 5+2\cdot 5^2+3\cdot 5^3+\cdots\}.$$



A $\mathbf{Z}_p$-extension of $\mathbf{Q}$

The group $\mathbf{Z}_p^\times$ has a finite torsion subgroup μ and $\mathbf{Z}_p^\times \cong \mu \times \mathbf{Z}_p$, which is analogous to $\mathbf{R}^\times = \{\pm 1\} \times (0,\infty) \cong \{\pm 1\} \times \mathbf{R}$.

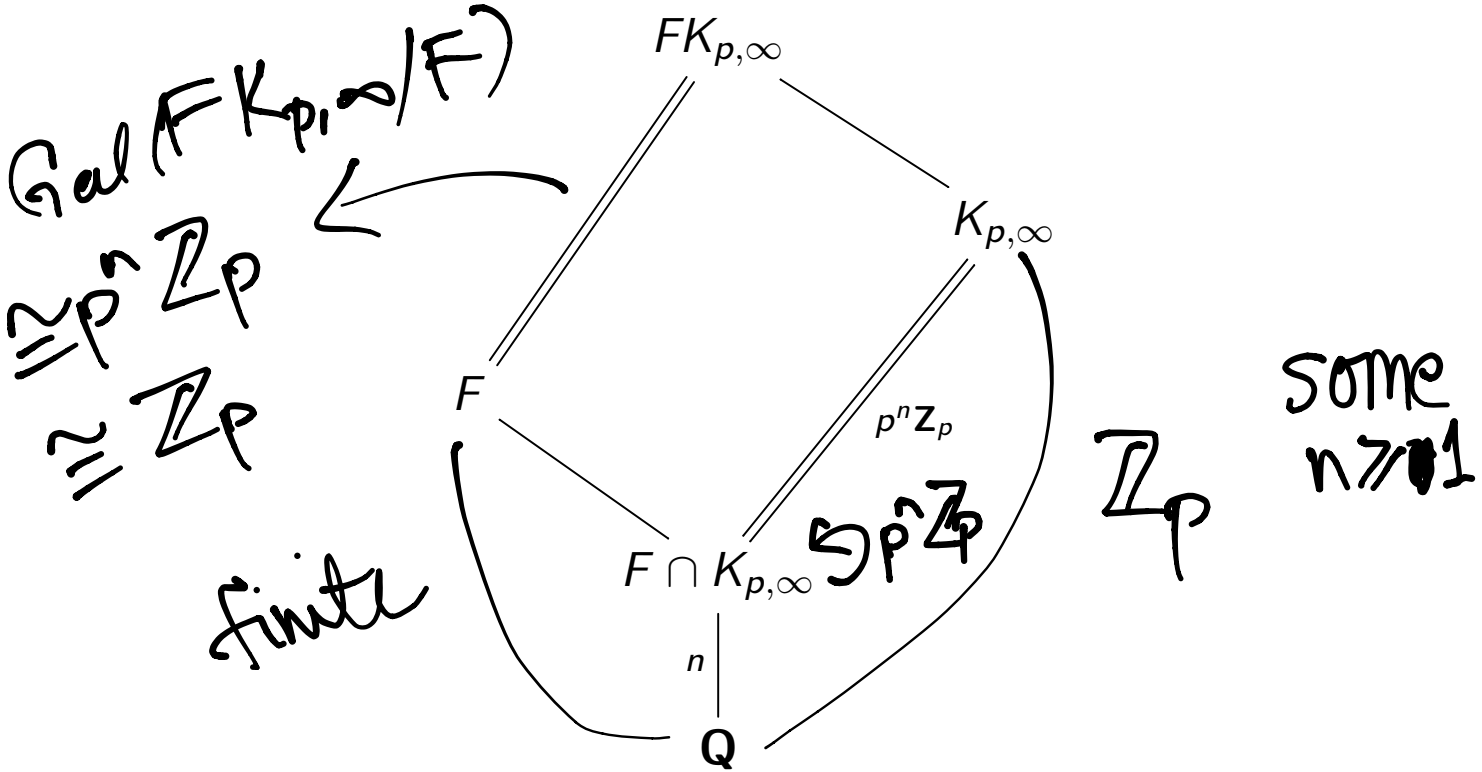


Set $K_{p,\infty} = \mathbf{Q}(\zeta_{p^\infty})^\mu$. It's called the *cyclotomic* $\mathbf{Z}_p$*-extension* of $\mathbf{Q}$ since $\mathrm{Gal}(K_{p,\infty}/\mathbf{Q}) = \mathbf{Z}_p^\times/\mu \cong \mathbf{Z}_p$. The closed subgroups of $\mathbf{Z}_p$ are $\{0\}$ and $p^n\mathbf{Z}_p$ for $n \geq 0$, so the proper subfields of $K_{p,\infty}$ are $K_{p,n}$ of degree p^n over $\mathbf{Q}$ for $n \geq 1$, $\mathrm{Gal}(K_{p,n}/\mathbf{Q}) \cong \mathbf{Z}_p/p^n\mathbf{Z}_p \cong \mathbf{Z}/p^n\mathbf{Z}$.

Conjecture (Coates). For all p and all $n \geq 1$, the field $K_{p,n}$ has class number 1. See MO questions 41219 and 82480.

A $\mathbf{Z}_p$-extension of a Number Field

For a number field F, $\mathrm{Gal}(FK_{p,\infty}/F) \cong \mathrm{Gal}(K_{p,\infty}/(K_{p,\infty} \cap F))$, which is open in $\mathrm{Gal}(K_{p,\infty}/\mathbf{Q}) \cong \mathbf{Z}_p$, so $\mathrm{Gal}(FK_{p,\infty}/F) \cong \mathbf{Z}_p$.



Call FK_{p^∞} the *cyclotomic* $\mathbf{Z}_p$*-extension of* F. It is the subfield of $F(\zeta_{p^\infty})$ fixed by elements of finite order in $\mathrm{Gal}(F(\zeta_{p^\infty})/F) \subset \mathbf{Z}_p^\times$.

More $\mathbf{Z}_p$-extensions of a Number Field

Besides cyclotomic $\mathbf{Z}_p$-extensions, others are not constructed concretely, but they are out there.

If F is not totally real (*e.g.*, $F = \mathbf{Q}(\sqrt[3]{2})$) then it has infinitely many $\mathbf{Z}_p$-extensions, but only finitely many "independent" ones (analogy: $\mathbf{R}^2$ is infinite with finite basis). Number of independent $\mathbf{Z}_p$-extensions is between $1 + r_2(F)$ and $[F : \mathbf{Q}] = r_1(F) + 2r_2(F)$.

If F is totally real (*e.g.*, $\mathbf{Q}$, $\mathbf{Q}(\sqrt{2})$, $\mathbf{Q}(\alpha)$ where $\alpha^3 - 9\alpha - 9 = 0$) then $r_2(F) = 0$ and we *expect* its cyclotomic $\mathbf{Z}_p$-extension is its only $\mathbf{Z}_p$-extension. This is a theorem if $F/\mathbf{Q}$ is abelian, *e.g.*, the only $\mathbf{Z}_p$-extension of $\mathbf{Q}$ and real quadratic field is their cyclotomic $\mathbf{Z}_p$-extension.

Study of $\mathbf{Z}_p$-extensions of number fields was initiated by Iwasawa, leading to *Iwasawa theory*, a major area of contemporary number theory.

Galois Representation into a Complex Matrix Group

If $\rho\colon \mathrm{Gal}(L/K) \to \mathrm{GL}_n(\mathbf{C})$ is a continuous homomorphism ("Artin representation"), then it has finite image!

1. A small open neighborhood U of the identity in $\mathrm{GL}_n(\mathbf{C})$ has *no nontrivial subgroup* ("no small subgroups").
2. Then $\rho^{-1}(U)$ is open in $\mathrm{Gal}(L/K)$ and contains the identity, so $\mathrm{Gal}(L/F) \subset \rho^{-1}(U)$ for some finite extension F/K.
3. The image $\rho(\mathrm{Gal}(L/F))$ is in U and is a *subgroup*, so it is trivial. Thus $\rho(\sigma\,\mathrm{Gal}(L/F)) = \rho(\sigma)$ for all σ: ρ is constant on cosets of $\mathrm{Gal}(L/F)$.
4. The open subgroup $\mathrm{Gal}(L/F)$ in $\mathrm{Gal}(L/K)$ has finite index (index is $[F : K]$), so ρ has finitely many values in $\mathrm{GL}_n(\mathbf{C})$.

Lesson: the Krull topology on $\mathrm{Gal}(L/K)$ and complex topology on $\mathrm{GL}_n(\mathbf{C})$ do not interact in an interesting way.

A Galois Representation With Infinite Image

For $\sigma \in G_{\mathbf{Q}} = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, its effect on the p-power roots of unity is by raising to some p-adic unit exponent: $\sigma(\zeta_{p^n}) = \zeta_{p^n}^{a(\sigma)}$ for some $a(\sigma) \in \mathbf{Z}_p^\times$ (independent of n). This gives us a homomorphism

$$\chi_p \colon G_{\mathbf{Q}} \to \mathbf{Z}_p^\times$$

called the *p-adic cyclotomic character*.

$\chi_p(\sigma) = a(\sigma)$: $\sigma(\zeta_{p^n}) = \zeta_{p^n}^{\chi(\sigma)}$ for all $n \geq 1$.

Example: $\chi_p(\mathrm{id.}) = 1$.

Example: $\chi_p(\text{cpx. conj.}) = -1$.

How can we calculate χ_p anywhere else when we have no formula for other elements of $G_{\mathbf{Q}}$?!? Stay tuned...

The function χ_p is surjective and continuous: inverse image of $1 + p^n\mathbf{Z}_p$ is $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}(\zeta_{p^n}))$, which is open in $G_{\mathbf{Q}}$ since $\mathbf{Q}(\zeta_{p^n})$ is finite.

$\mathbb{Z}_p^\times \supset \cdots \subset 1+p^3\mathbb{Z}_p \subset 1+p^2\mathbb{Z}_p \subset 1+p\mathbb{Z}_p$

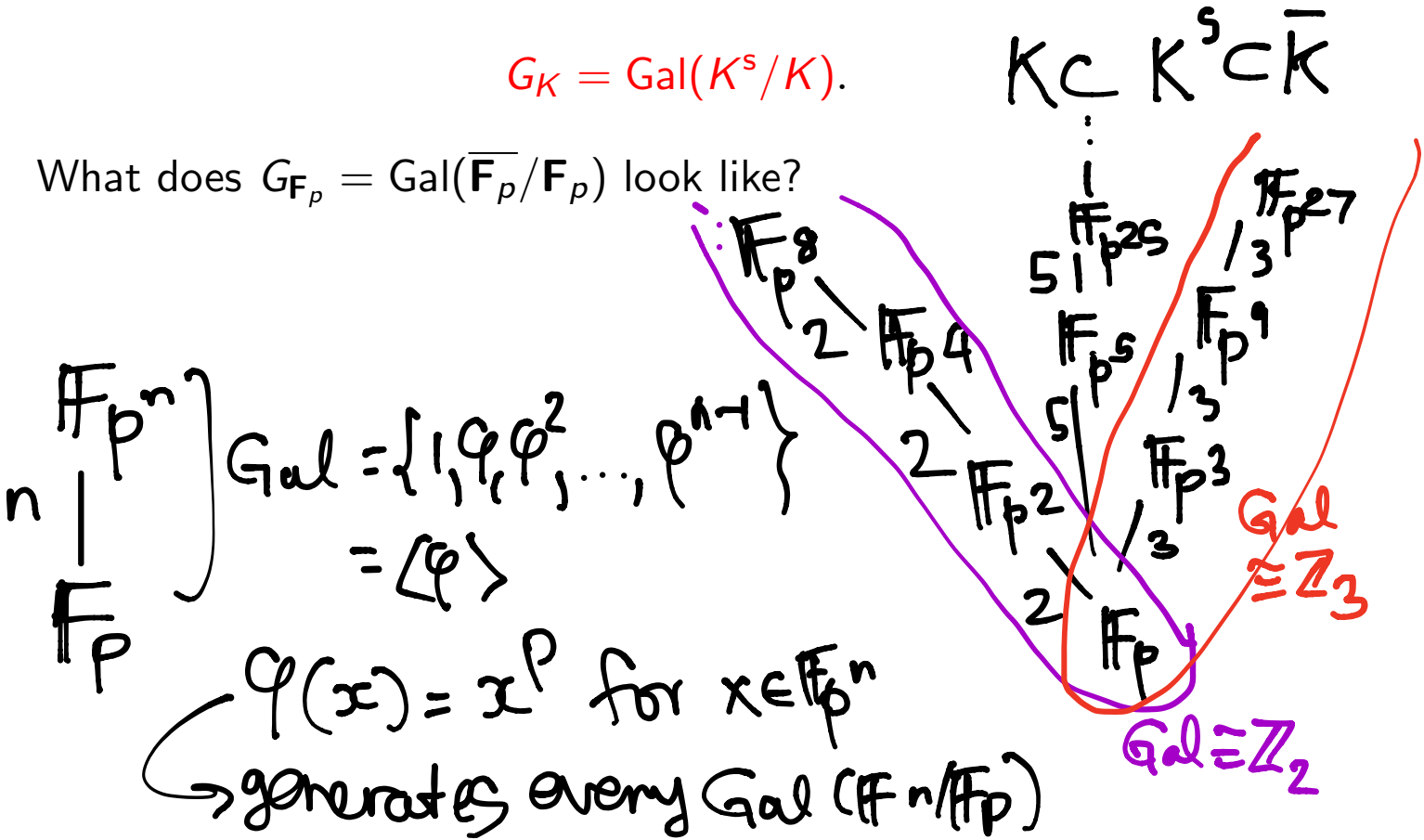
Lesson: the Krull topology on $G_{\mathbf{Q}}$ interacts in an interesting way with p-adic groups like $\mathbf{Z}_p^\times$ or $\mathrm{GL}_n(\mathbf{Z}_p)$.

Absolute Galois group

To each field K we can associate a compact group: the Galois group over K of its maximal separable extension (= its algebraic closure, in characteristic 0). This is called its *absolute Galois group*:

$$G_K = \mathrm{Gal}(K^s/K).$$

What does $G_{\mathbf{F}_p} = \mathrm{Gal}(\overline{\mathbf{F}_p}/\mathbf{F}_p)$ look like?



$\varphi(x) = x^p$ is topological generator of $G_{\mathbb{F}_p}$: $\langle \varphi \rangle$ is dense in $G_{\mathbb{F}_p}$.

$\sigma \in G_{\mathbb{F}_p} \Rightarrow \sigma|_{\mathbb{F}_{p^n}} = \varphi^k|_{\mathbb{F}_{p^n}}$

$\Rightarrow \sigma \in \varphi^k \mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_{p^n})$

$\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) \cong \underbrace{\prod_{l \text{ prime}} \mathbb{Z}_l}_{\hat{\mathbb{Z}}} = \overline{\langle \varphi \rangle}$

$\hat{\mathbb{Z}} \hookleftarrow \left\{ \sum_{n \geq 0} c_n n! \, , \, 0 \leq c_n \leq n \right\}$

$n! \to 0$ in $\mathbb{Z}_l$ for all l.

For $x \in \overline{\mathbb{F}_p}$, $x^{p^t} = x^{c_0 + c_1 p + c_2 p^2 + \cdots}$

Subgroups of $G_{\mathbf{Q}}$ and Prime Ideals

In $\overline{\mathbf{Q}}$, let $\overline{\mathbf{Z}}$ be the ring of *all* algebraic integers (the roots of monic polynomials with integer coefficients). For $\sigma \in G_{\mathbf{Q}}$, $\sigma(\overline{\mathbf{Z}}) = \overline{\mathbf{Z}}$.

For a nonzero prime (maximal) ideal $\mathfrak{p}$ of $\overline{\mathbf{Z}}$, the field $\overline{\mathbf{Z}}/\mathfrak{p}$ is a model of $\overline{\mathbf{F}_p}$, where $\mathfrak{p} \cap \mathbf{Z} = p\mathbf{Z}$.

Analogue. $\mathbf{Z}[i]/(3) = \mathbf{F}_9$, $\mathbf{Z}[i]/(1+2i) = \mathbf{F}_5$, $\mathbf{Z}[i]/(1-2i) = \mathbf{F}_5$.

The group $G_{\mathbf{Q}}$ acts on $\{\mathfrak{p} : \mathfrak{p} \cap \mathbf{Z} = p\mathbf{Z}\}$ with one orbit. (Proof: prove it in finite extensions of $\mathbf{Q}$, then use compactness of $G_{\mathbf{Q}}$.)

Analogue. $\mathrm{Gal}(\mathbf{Q}(i)/\mathbf{Q}) = \{1, c\}$ and $c((1+2i)) = (1-2i)$.

For groups actions, stabilizer subgroup of each point is important. In this setting, for historical reasons, it is called the *decomposition group* at $\mathfrak{p}$:

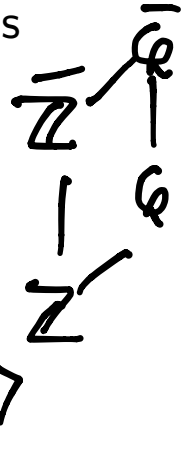
$$D(\mathfrak{p}) = \{\sigma \in G_{\mathbf{Q}} : \sigma(\mathfrak{p}) = \mathfrak{p}\}.$$

Can show this is a *closed* subgroup of $G_{\mathbf{Q}}$ by looking at its image in $\mathrm{Gal}(F/\mathbf{Q})$ for all finite Galois $F/\mathbf{Q}$ and its effect on $\mathfrak{p} \cap F$.

Frobenius Elements

Elements of $D(\mathfrak{p}) = \{\sigma \in G_{\mathbf{Q}} : \sigma(\mathfrak{p}) = \mathfrak{p}\}$ preserve congruences mod $\mathfrak{p}$: for α and β in $\overline{\mathbf{Z}}$,

$$\alpha \equiv \beta \bmod \mathfrak{p} \Longrightarrow \alpha - \beta \in \mathfrak{p} \Longrightarrow \sigma(\alpha) \equiv \sigma(\beta) \bmod \mathfrak{p}.$$



So $D(\mathfrak{p})$ makes sense on $\overline{\mathbf{Z}}/\mathfrak{p} \cong \overline{\mathbf{F}_p}$: we get a homomorphism

$$D(\mathfrak{p}) \to \mathrm{Gal}((\overline{\mathbf{Z}}/\mathfrak{p})/\mathbf{F}_p) = G_{\mathbf{F}_p}.$$

This is continuous and *surjective*. (Proof: prove analogue in finite extensions of $\mathbf{Q}$, then use compactness of $G_{\mathbf{Q}}$).

Definition. A *Frobenius element* at $\mathfrak{p}$ in $G_{\mathbf{Q}}$ is $\varphi_{\mathfrak{p}} \in G_{\mathbf{Q}}$ that looks like pth power map mod $\mathfrak{p}$: $\varphi_{\mathfrak{p}}(\alpha) \equiv \alpha^p \bmod \mathfrak{p}$ for all $\alpha \in \overline{\mathbf{Z}}$.

Example. For a root of unity ζ_m with order m not divisible by p, $\varphi_{\mathfrak{p}}(\zeta_m) = \zeta_m^a$ where $(a, m) = 1$. Also $\varphi_{\mathfrak{p}}(\zeta_m) \equiv \zeta_m^p \bmod \mathfrak{p}$, so $\zeta_m^a \equiv \zeta_m^p \bmod \mathfrak{p}$. The mth roots of unity stay distinct when reduced mod $\mathfrak{p}$, so $\zeta_m^a = \zeta_m^p$. Thus $\varphi_{\mathfrak{p}}(\zeta_m) = \zeta_m^p$ when $p \nmid m$. When ℓ is prime, $\ell \neq p$, $\varphi_{\mathfrak{p}}(\zeta_{\ell^n}) = \zeta_{\ell^n}^p$, so $\chi_\ell(\varphi_{\mathfrak{p}}) = p$ in $\mathbf{Z}_\ell^\times$.

Frobenius Elements

A *Frobenius element* at $\mathfrak{p}$ in $G_{\mathbf{Q}}$, where $\mathfrak{p} \cap \mathbf{Z} = p\mathbf{Z}$, is an element $\varphi_{\mathfrak{p}} \in G_{\mathbf{Q}}$ that looks like pth power map mod $\mathfrak{p}$: $\varphi_{\mathfrak{p}}(\alpha) \equiv \alpha^p \bmod \mathfrak{p}$ for all $\alpha \in \overline{\mathbf{Z}}$.

The Chebotarev density theorem says that for finite Galois $F/\mathbf{Q}$, each element of $\mathrm{Gal}(F/\mathbf{Q})$ is a "Frobenius element in $\mathrm{Gal}(F/\mathbf{Q})$" (in many ways). In our topological language, this means for each $\sigma \in G_{\mathbf{Q}}$ that $\sigma|_F = \varphi_{\mathfrak{p}}|_F$ for some (in fact infinitely many) $\varphi_{\mathfrak{p}}$ in $G_{\mathbf{Q}}$, so the Frobenius elements of $G_{\mathbf{Q}}$ are a *dense* subset of $G_{\mathbf{Q}}$.

This is why continuous representations of $G_{\mathbf{Q}}$ are often described by their behavior just on suitably chosen Frobenius elements.

Chebotarev proved his "density theorem" in 1922, as a theorem about Frobenius elements (conjugacy classes) in *finite* Galois groups over $\mathbf{Q}$, before Krull developed infinite Galois theory. That his theorem can be interpreted as saying a certain subset of $G_{\mathbf{Q}}$ is dense is an accident.