Reminder: Consider a galois extension of fields L/K which may or may not be finite.

$$\begin{array}{c} \Gamma \curvearrowright L \\ | \\ k \end{array}$$

Proposition 10.3.1: There is a natural injective group homomorphism

$$\mathrm{Gal}(L/K) \to \bigtimes_{K'} \mathrm{Gal}(K'/K),\ \gamma \mapsto (\gamma|_{K'})_{K'},$$

where the product extends over all intermediate fields K' that are finite and galois over K. Its image is the closed subgroup

$$\varprojlim_{K'} \mathrm{Gal}(K'/K) \ := \ \big\{(\gamma_{K'})_{K'} \,\big|\, \forall\, K''/K'/K\colon \gamma_{K''}|_{K'} = \gamma_{K'}\big\}.$$

This turns $\Gamma := \mathrm{Gal}(L/K)$ into a profinite group.

Theorem 10.3.2: *(Main Theorem of Galois theory)* There are natural mutually inverse bijections

$$\begin{array}{ccc} \{\text{Intermediate fields of } L/K\} & \underset{\sim}{\rightleftarrows} & \{\text{closed subgroups of } \Gamma\} \\ K' & \longmapsto & \mathrm{Gal}(L/K') \\ L^{\Gamma'} & \longleftarrow\!\shortmid & \Gamma' \end{array}$$

Here the open subgroups of Γ correspond to the subfields of finite degree over K.

Example 10.3.3: For any finite field k with algebraic closure $\bar{k}$, there is a natural isomorphism $\hat{\mathbb{Z}} \cong \mathrm{Gal}(\bar{k}/k)$ that sends 1 to the Frobenius automorphism $x \mapsto x^{|k|}$.

For all $k' \subset \bar{k}$ with k'/k finite: $[k'/k] = n'$

$$\mathbb{Z}/n'\mathbb{Z} \xrightarrow{\sim} \mathrm{Gal}(k'/k), \quad 1 \longmapsto (x \mapsto x^{|k|})$$

Vary $k' \supset k''$:

$$\left.\begin{array}{ccc} \mathbb{Z}/n'\mathbb{Z} & \xrightarrow{\sim} & \mathrm{Gal}(k'/k) \\ \uparrow & /// & \uparrow \\ \mathbb{Z}/n''\mathbb{Z} & \xrightarrow{\sim} & \mathrm{Gal}(k''/k) \end{array}\right) \Rightarrow \hat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \mathrm{Gal}(\bar{k}/k).$$

Example 10.3.4: Consider a prime number p.

natural isomorphism.

$L = \mathbb{Q}(\mu_{p^\infty})$

(a) The extension $L := \mathbb{Q}(\bigcup_{n \geqslant 0} \mu_{p^n})/\mathbb{Q}$ has galois group $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}_p^\times$.

(b) It has a unique subfield L' with $\mathrm{Gal}(L'/\mathbb{Q}) \cong \mathbb{Z}_p$.

In Iwasawa theory one is interested in more general Galois extensions of a number field with galois group $\mathbb{Z}_p$, which are called *$\mathbb{Z}_p$-extensions.*

$$\mathrm{Gal}(\mathbb{Q}(\mu_{p^n})/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/p^n\mathbb{Z})^\times, \quad \gamma \mapsto a_\gamma \text{ s.th. } \forall \zeta \in \mu_{p^n}: \gamma\zeta = \zeta^{a_\gamma}$$

$$\mathrm{Gal}(L/\mathbb{Q}) \xrightarrow{\sim} \varprojlim_n (\mathbb{Z}/p^n\mathbb{Z})^\times = \boxed{\mathbb{Z}_p^\times \cong \begin{cases} \mu_{p-1} \times \mathbb{Z}_p & p \text{ odd} \\ \mu_2 \times \mathbb{Z}_2 & p = 2. \end{cases}}$$

Remark 10.3.5: Many questions in number theory, among them highly interesting unproven conjectures, can be phrased as questions concerning the structure of the galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

11 Galois theory of local fields

Throughout this chapter we fix a nonarchimedean local field K with normalized valuation v and valuation ring $\mathcal{O}$ and finite residue field $k = \mathcal{O}/\mathfrak{m}$ of characteristic p.

11.1 Multiplicative group

Proposition 11.1.1: The reduction homomorphism $\mathcal{O}^\times \to k^\times$ is surjective and has a unique splitting, that is, a homomorphism $k^\times \to \mathcal{O}^\times$, $\alpha \mapsto \tilde{\alpha}$, such that $\tilde{\alpha} + \mathfrak{m} = \alpha$.

Definition 11.1.2: The element $\tilde{\alpha}$ is called the *Teichmüller representative* of α.

Proof: Write $|k| = q \Rightarrow k^\times$ cyclic of order $q-1$.
its elements are the zeros of $X^{q-1} - 1 = \prod_{\alpha \in k^\times} (X - \alpha)$ in $k[X]$

Hensel's Lemma $\Rightarrow \exists!$ factorization $X^{q-1} - 1 = \prod_{\tilde{\alpha} \in S} (X - \tilde{\alpha})$ in $\mathcal{O}[X]$.

with $\tilde{\alpha} + \mathfrak{m} = \alpha$. These $\tilde{\alpha}$ are $(q-1)$-st roots of unity, so

$$\underbrace{\mu_{q-1}(\mathcal{O})}_{\text{order} \leq q-1} \xrightarrow{\text{red}} \mu_{q-1}(k) = \underbrace{k^\times}_{\text{order} = q-1} \text{ : surjective homom!} \Rightarrow \text{isomorphism.}$$

Qed.

2^{nd} Proof: For any $\alpha \in k^\times$ choose $a \in G^\times$ with $a \bmod m = \alpha$.

Claim: $\lim\limits_{n\to\infty} a^{q^n} =: \tilde{\alpha}$ does it.

① $\forall\, b, b' \in G^\times : v(b'-b) > 0 \implies v(b'^q - b^q) > v(b'-b)$.

Proof: $b'^q = (b + (b'-b))^q = b^q + \sum\limits_{0<i<q} \binom{q}{i} \cdot b^{q-i} \cdot (b'-b)^i + (b'-b)^q$

$v \geq v(b'-b)$ $\quad v = q \cdot v(b'-b) > v(b'-b)$

$p \mid \binom{q}{i} \implies v\left(\binom{q}{i}\right) > 0$

qed

② Take $a' \in G^\times$ with $a' \bmod m = \alpha$

$\implies v(a'-a) > 0 \implies \geq 1$

$\overset{①}{\implies} v(a'^{q^n} - a^{q^n}) \geq n$

$\implies (a'^{q^n})$ has the same limit.

③ In particular $(a^q \bmod m) = \alpha^q = \alpha$

$\implies v(a^{q^{n+1}} - a^{q^n}) \geq n.$

$\implies (a^{q^n})$ is a Cauchy sequence in $G^\times$

$\Downarrow$

converges in $G^\times$

④

$\tilde{\alpha}^q = \lim\limits_{n\to\infty} a^{q^{n+1}} = \lim\limits_{n\to\infty} a^{q^n} = \tilde{\alpha} \implies \tilde{\alpha}^{q-1} = 1.$

⑤ Lift α, β to $a, b \in G^\times$

$\implies \tilde{\alpha} \cdot \tilde{\beta} = \lim\limits_{n\to\infty} a^{q^n} \cdot \lim\limits_{n\to\infty} b^{q^n} = \lim\limits_{n\to\infty} (ab)^{q^n} = \widetilde{\alpha\beta}$.

qed