<u>Lemma 12.1</u> If L is an étale K-alg. of degree n, there are exactly n K-algebra homomorphisms $L \to K^{sep}$.

<u>Pf</u> Write $L = L_1 \times \dots \times L_r$. Let $d_i = [L_i : K]$. There are d_i hom. $L_i \to K^{sep}$. Each hom. $L \to K^{sep}$ must factor through some L_i. ∎

~~Thm 12.1 Let L as above, $\sigma_1, \dots, \sigma_n : L \to K$ the K-alg hom~~

Let $\Gamma_K = Gal(K^{sep}|K)$.

To any L as above with the K-alg. hom. $\rho_1, \dots, \rho_n : L \to K^{sep}$, we can associate a continuous group hom. $f : Gal(K^{sep}|K) = \Gamma_K \to S_n$

$$\sigma \mapsto \pi \text{ such that } \sigma \circ \rho_i = \rho_{\pi(i)}$$

Note that relabeling $\rho_1, \dots, \rho_n$ conjugates by an element of S_n.

<u>Rmk</u> If L is the subfield of K^{sep} fixed by $H \leq \Gamma_K$, then this corr. to the action of Γ_K on the n-element set Γ_K/H.

<u>Thm 12.2</u> This gives rise to a bijection

$$\left\{ \begin{array}{l} L \text{ étale deg. } n \text{ alg.} \\ \text{(up to isomorphism)} \end{array} \right\} \longleftrightarrow \underbrace{S_n \backslash Hom_{cont}(\Gamma_K, S_n)}_{\text{orbits of conjugation action}}.$$

<u>Rmk</u> If L corr. to $f : \Gamma_K \to S_n$
and L' corr. to $f' : \Gamma_K \to S_{n'}$,
then $L \times L'$ corr. to $\Gamma_K \xrightarrow{f \times f'} S_n \times S_{n'} \xhookrightarrow[\text{incl.}]{\text{nat.}} S_{n+n'}$.

<u>Rmk</u> {The action of Γ_K on $\{1, \dots, n\}$ corr. to $L = L_1 \times \dots \times L_r$ has exactly r orbits.}

<u>Ex</u> $L = K^n$ corr. to the trivial map $\sigma \mapsto id$.

Pf of Thm

To construct the inverse, let $f: \Gamma_K \to S_n$.

This corr. to an action of Γ_K on $\{1, \dots, n\}$.

Assume there are r orbits, with representatives $t_1, \dots, t_r \in \{1, \dots, n\}$.

Then, the preimage of f is $L = L_1 \times \dots \times L_r$ with

L_i = subfield of K^{sep} fixed by $\mathrm{Stab}_{\Gamma_K}(t_i)$.

... $\square$

Thm 12.3

If L corr. to f, then

$$\mathrm{Aut}_{K\text{-alg}}(L) \xrightarrow{\sim} \mathrm{Stab}_{S_n}(f) = \text{centralizer of } \mathrm{im}(f) \leq S_n$$

$$\tau \longmapsto \text{the perm. } \alpha \in S_n \text{ such that } \rho_i \circ \tau^{-1} = \rho_{\alpha(i)}$$

Pf HW $\square$

Cor 12.4

$$\frac{1}{\# \mathrm{Aut}(L)} = \frac{\#\{f: \Gamma_K \to S_n \text{ corr. to } L\}}{\# S_n}$$

Pf Orbit-stabilizer theorem $\square$

Lemma 12.5 Consider the étale degree n extensions L of $\mathbb{R}$, up to isomorphism.

a) $\#\{L\} = \left\lfloor \frac{n}{2} \right\rfloor + 1$

b) $\sum_L \frac{1}{\#\mathrm{Aut}(L)} = \mathbb{P}_{\pi \in S_n}(\pi^2 = id)$

Pf a) $L = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ with $n = r_1 + 2r_2$

$(0 \leq r_2 \leq \frac{n}{2})$

b) $LHS = \frac{1}{\# S_n} \cdot \#\{f : \Gamma_{\mathbb{R}} \longrightarrow S_n\}$

$\Gamma_{\mathbb{R}} = \{e, \sigma\} = C_2$ (cyclic group of order 2)

$$\{f : C_2 \to S_n\} \longleftrightarrow \{\pi \in S_n \mid \pi^2 = id\}$$

$$f \longmapsto f(\sigma)$$

$\square$

Remark $\#\mathrm{Aut}(\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}) = r_1! \cdot r_2! \cdot 2^{r_2}$.

Lemma 12.6 Consider the étale degree n extensions L of $\mathbb{F}_q$, up to $\cong$.

a) $\#\{L\}$ = number of partitions of the integer n (ignoring order)

b) $$\sum_L \frac{1}{\#\mathrm{Aut}(L)} = 1$$

Pf a)

$$L = \mathbb{F}_{q^{k_1}} \times \dots \times \mathbb{F}_{q^{k_r}} \quad \text{with } n = k_1 + \dots + k_r$$

b) $\Gamma_{\mathbb{F}_q} = \hat{\mathbb{Z}}$

$$\{f : \hat{\mathbb{Z}} \underset{(\text{cont.})}{\longrightarrow} S_n\} \longleftrightarrow \{f : \mathbb{Z} \longrightarrow S_n\} \longleftrightarrow S_n$$

$$\Rightarrow \text{LHS} = \frac{1}{\# S_n} \cdot \# S_n = 1$$

$\square$

13. p-adic integration

References:

- Igusa: An introduction to the theory of local zeta functions
- Popa: p-adic integration (lecture notes on his webpage)

Let K be a nonarch. local field with residue field $\mathbb{F}_q$, uniformizer π_K, normalized valuation v_K, norm $|x| = q^{-v_K(x)}$,

Haar measure dx normalised so $\int_{\mathcal{O}_K} 1\,dx = 1$.

vol$(\mathcal{O}_K)$

Lemma 13.1 Let $A \subseteq K$ be a measurable subset. For any $t \in K$,

$$\mathrm{vol}(t\cdot A) = |t| \cdot \mathrm{vol}(A).$$

Rmk That's like for $K = \mathbb{R}$, Lebesgue measure.

Pf $t = 0$: clear

$t \in \mathcal{O}_K^\times$: The isom. $K \to K$, $x \mapsto tx$ sends $\mathcal{O}_K$ to $\mathcal{O}_K$.

~~$\Rightarrow$ It must send the Haar measure dx to itself~~

~~$\Rightarrow \mathrm{vol}(t\cdot A) = \mathrm{vol}(A)$.~~

$\Rightarrow$ The pushforward of dx is dx.

$\Rightarrow \mathrm{vol}(f^{-1}(f(A))) = \mathrm{vol}(f(A))$.

$\underline{t=\pi}$: The isom. $f: K \to K$, $x \mapsto tx$ sends $\mathcal{O}_K$ to the prime ideal $\pi\mathcal{O}_K$.

Let $r_1, \dots, r_q \in \mathcal{O}_K$ be representatives of the residue classes mod π.

$$\Rightarrow \mathcal{O}_K = \bigsqcup_{i=1}^{q} (r_i + \pi\mathcal{O}_K)$$

$$\Rightarrow \mathrm{vol}(\mathcal{O}_K) = \sum \mathrm{vol}(r_i + \pi\mathcal{O}_K) \underset{\substack{\uparrow \\ \text{Haar measure}}}{=} \sum \mathrm{vol}(\pi\mathcal{O}_K) = q \cdot \mathrm{vol}(\pi\mathcal{O}_K)$$

$$\Rightarrow \mathrm{vol}(\pi\mathcal{O}_K) = \frac{1}{q} \cdot \mathrm{vol}(\mathcal{O}_K) = |\pi| \cdot \mathrm{vol}(\mathcal{O}_K).$$

The pushforward of the Haar measure dx with $\mathrm{vol}(\mathcal{O}_K) = 1$ must be a Haar measure with $\mathrm{vol}(\pi\mathcal{O}_K) = 1$.

$\Rightarrow$ It is $|\pi|^{-1} \cdot dx$.

$$\Rightarrow \mathrm{vol}(A) = \mathrm{vol}(f^{-1}(f(A)))$$
$$= \text{volume of } f(A) \text{ w.r.t. pushforward}$$
$$= |\pi|^{-1} \cdot \mathrm{vol}(f(A)) \qquad \square$$

Thm 13.2 Let $A \subseteq K$ be compact and open (or more generally measurable).

Let $f \in K[x]$ be a polynomial (or more generally a K-analytic function). For any $y \in K$, let $m(y) := \#\{x \in A \mid f(x) = y\}$.

Then,
$$\underbrace{\int_K m(y)\,dy}_{\text{vol}(f(A) \text{ as a multiset})} = \int_A |f'(x)|\,dx .$$

Ex $K = \mathbb{Q}_p$, $A = \mathbb{Z}_p^\times$, $f(x) = x^2$

Case $p \neq 2$:

By Hensel's lemma,
$$m(y) = \begin{cases} 2, & (y \bmod p) \in \mathbb{F}_p^{\times 2} \text{ (quadr. res.)} \\ 0, & \text{otherwise} \end{cases}$$

$$\Rightarrow \text{LHS} = 2 \cdot \frac{\#\text{nonzero quadr. res.}}{p} = \frac{p-1}{p} = 1 - \frac{1}{p}.$$

$$v_p(f'(x)) = v_p(2x) = 0 \quad \forall x \in \mathbb{Z}_p^\times$$
$$\Downarrow$$
$$|f'(x)| = 1$$

$$\Rightarrow \text{RHS} = \int_{\mathbb{Z}_p^\times} 1\,dx = \text{vol}(\mathbb{Z}_p^\times) = 1 - \frac{1}{p}.$$

Case $p=2$:

By Hensel's lemma,

$$m(y) = \begin{cases} 2, & y \equiv 1 \bmod 8, \\ 0, & \text{otherwise.} \end{cases}$$

$$\Rightarrow LHS = 2 \cdot \frac{1}{8} = \frac{1}{4}$$

$$v_2(f'(x)) = v_2(2x) = 1 \quad \forall x \in \mathbb{Z}_2^\times$$

$$\Downarrow$$

$$|2x| = \frac{1}{2}$$

$$\Rightarrow RHS = \int_{\mathbb{Z}_2^\times} \frac{1}{2}\,dx = \frac{1}{2}\,\mathrm{vol}(\mathbb{Z}_2^\times) = \frac{1}{4}$$

Exe $K = \mathbb{F}_p((T))$, $A = \mathcal{O}_K = \mathbb{F}_p[[T]]$, $f(x) = X^p$.

$(a_0 + a_1 X + a_2 X^2 + \dots)^p = a_0 + a_1 X^p + a_2 X^{2p} + \dots$

$$\Rightarrow m(y) = \begin{cases} 1, & y = b_0 + b_p X^p + b_{2p} X^{2p} + \dots \text{ for some } b_0, b_p, \dots \in \mathbb{F}_p \\ & (\infty \text{ many "digits" of } Y \text{ have to be } 0\dots) \\ 0, & \text{otherwise} \end{cases}$$

$$\Rightarrow LHS = 0$$

$$|f'(x)| = |pX^{p-1}| = 0$$

$$\Rightarrow RHS = 0$$

Pf of Thm

Replacing A by $\pi^a A$, f by $\pi^b f(\frac{X}{\pi^a})$ for large a, b, we can arrange $A \subseteq \mathcal{O}_K$, $f \in \mathcal{O}_K[X]$.

$$\begin{aligned} A &\longrightarrow \mathbb{Z} \cup \{\infty\} \text{ is continuous.} \\ x &\longmapsto v(f'(x)) \end{aligned}$$

Claim Let $B = \{x \in \mathcal{O}_K \mid f'(x) = 0\}$. We have $\mathrm{vol}(f(B)) = 0$.

Pf If $f' \neq 0$, then $\# B < \infty$. ($\checkmark$)

If $f' = 0$, then f = constant ($\checkmark$) or $\mathrm{char}(K) = p$, $f = g(X^p)$ for some $g \in \mathcal{O}_K[X]$.

By the last example, $C = \{x^p \mid x \in \mathcal{O}_K\}$ has volume 0.

$\Rightarrow$ $f(B) = g(C)$ has volume 0.

f cont.

$\square$

For any $t \in \mathbb{Z}$, $\{x \in A \mid v(f'(x)) = t\}$ is compact and open.

W.l.o.g. $v(f'(x)) = t \quad \forall x \in A$.

Let $a \in A$ and let $e > 2t$. By Hensel's lemma, we have $f(a + \mathfrak{p}^e) = f(a) + \mathfrak{p}^{t+e}$ and each $y \in f(a) + \mathfrak{p}^{t+e}$ has exactly one preimage in $a + \mathfrak{p}^e$.

We have $$\int_{a+\mathfrak{p}^e} \underbrace{|f'(x)|}_{q^{-t}}\, dx = q^{-e-t} = \int_{f(a)+\mathfrak{p}^{e+t}} 1\, dy.$$

The result follows by splitting up A into (finitely many) disjoint sets of the form $a+\mathfrak{p}^e$. $\square$