Field ext. of fixed degree

Two ways of counting degree n ext. of a fixed field K:

- count field ext. $L|K$ up to isom.
- count subfields $L \subseteq \overline{K}$

Lemma Any separable ext. $L|K$ of degree n is isomorphic to exactly $\frac{n}{\# \mathrm{Aut}(L)}$ subfields $L \subseteq K^{sep}$

aut. as K-algebra

separable closure

$$" \frac{1}{n} \sum_{L \subseteq K^{sep}} f(L) = \sum_{L/\cong} \frac{f(L)}{\# \mathrm{Aut}(L)} "$$

Pf There are n embeddings $L \hookrightarrow K^{sep}$. Two embeddings have the same image if and only if they differ by an automorphism of L.

$$\begin{tikzcd} L \arrow[r, hook] \arrow[d, "\wr"'] & K^{sep} \\ L \arrow[ur, hook] & \end{tikzcd}$$

$\square$

Extensions of rings

Def Let R be a Dedekind dom. with field of fractions K.
An an R-*lattice* is a fin. gen. torsionfree R-module A. Its *rank* is the (finite!) dimension of the K-vector space $A \otimes_R K$.

Rmk $A \longrightarrow A \otimes_R K$ is injective for any R-lattice A.

Rmk Any free R-module is an R-lattice.
Ex If R is PID, any R-lattice is free.

Def Let R, K as above. A *degree n extension* of R is a (commutative, unitary) R-algebra S, which (as R-module) is an R-lattice of rank n.
Its *discriminant* is the ideal $\mathrm{disc}(S|R) \subseteq R$ gen. by the elements $\det((\mathrm{Tr}(w_i w_j))_{i,j}) \in R$ with $w_1, \dots, w_n \in S$.
It is *nondegenerate* if $\mathrm{disc}(S|R) \neq 0$.

Ex R is a deg. 1 ext. of R with disc $= (1)$.

Ex Let $L|K$ be a field ext. of deg. n. Then, $L|K$ is a deg. n ext. with

$$\mathrm{disc}(L|K) = \begin{cases} K = (1), & \text{if } L|K \text{ is separable} \\ (0), & \text{else.} \end{cases}$$

Ex If $f(X) \in R[X]$ is monic of degree n, then $S = R[X]/(f(X))$ is a deg. n ext. with $\mathrm{disc}(S|R) = (\mathrm{disc}(f))$.

Rmk (base change)
If S is a deg. n ext. of R and $R' \supseteq R$ is another Dedekind dom., then $S' = S \otimes_R R'$ is a deg. n ext. of R' with $\mathrm{disc}(S'|R') = \mathrm{disc}(S|R) \cdot R'$.

Rmk (cartesian product)
If $S_1, \dots, S_r$ are deg. $n_1, \dots, n_r$ ext. of R, then $S = S_1 \times \dots \times S_r$ is a deg. $n = n_1 + \dots + n_r$ ext of R with $\mathrm{disc}(S|R) = \mathrm{disc}(S_1|R) \cdots \mathrm{disc}(S_r|R)$.

Ex $S = \underbrace{R \times \dots \times R}_{n}$ is a deg. n ext. of R with $\mathrm{disc}(S|R) = (1)$, called the <u>trivial ext</u>.

Thm The nondegenerate ext. of a field K (also called étale extensions) are exactly the K-algebras of the form $L = L_1 \times \dots \times L_r$ where $L_1, \dots, L_r$ are separable degree $n_1, \dots, n_r$ ext. of K.

Cor If K is separably closed, there is only the trivial nondeg. ext.

Cor For any nondeg. deg. n ext. $L|K$, there are exactly n ring hom. $L \longrightarrow K^{sep}$.

Pf There are n_i embeddings $L_i \hookrightarrow K^{sep}$.
Compose with proj. $L \twoheadrightarrow L_i$.
$\leadsto$ Total of n ring hom. $L \longrightarrow K^{sep}$.
All hom. are of this form. $\square$

Lemma Let L, K as above and assume that K is the field of fractions of a Dedekind dom. $\mathcal{O}_K$. Then, the ring of int. $\mathcal{O}_L$ $\left(= \left(\text{int. closure of } \mathcal{O}_K \text{ in } L\right) = \mathcal{O}_{L_1} \times \dots \times \mathcal{O}_{L_r}\right)$ is a deg. n ext. of $\mathcal{O}_K$ with

$$\operatorname{disc}(\mathcal{O}_{L_i} | \mathcal{O}_K) = D_{L_i|K} \quad \text{(relative discriminant of } L_i|K\text{)}.$$

It is maximal: there is no deg. n ext. $S \supsetneq \mathcal{O}_L$ of $\mathcal{O}_K$.

Extensions of finite fields

Thm The number of nondeg. deg. n ext. of $\mathbb{F}_q$ up to isomorphism is the number of partitions of the integer n.

Pf The nondeg. ext. are

$$\mathbb{F}_{q^{n_1}} \times \dots \times \mathbb{F}_{q^{n_r}} \text{ with } n_1 + \dots + n_r = n. \qquad \square$$

We can do a weighted count:

Thm
$$\sum_{\substack{\text{nondeg. deg } n \\ \text{ext. } L | \mathbb{F}_q \\ \text{up to isom.}}} \frac{1}{\# \mathrm{Aut}_K(L)} = 1.$$

Pf Let $L = \mathbb{F}_{q^{n_1}} \times \dots \times \mathbb{F}_{q^{n_r}}$ with $n = n_1 + \dots + n_r$.

Let the number l occur c_l times in $(n_1, \dots, n_r)$.

$$\Rightarrow \# \mathrm{Aut}(L) = \prod_{l=1}^{n} l^{c_l} \cdot c_l!$$

each of the c_l factors $\mathbb{F}_{q^l}$ has l autom.

there are $c_l!$ permutations of the c_l factors $\mathbb{F}_{q^l}$

$$\Rightarrow \frac{1}{\# \mathrm{Aut}(L)} = \mathbb{P}(\pi \text{ has cycletype } (n_1, \dots, n_r) \mid \pi \in S_n).$$

$$\Rightarrow \sum_{L \dots} \frac{1}{\# \mathrm{Aut}(L)} = 1$$ (any $\pi \in S_n$ has exactly one cycle type).

$\square$

Extensions of local fields

(Serre, Sur une formule de masse ...)

Thm Let K be a local field with residue field $\mathbb{F}_q$, normalized val. v_K and norm $|x| = q^{-v_K(x)}$.
Consider the ~~totally~~ ramified (separable) degree n field ext. $L|K$. We have

$$\frac{1}{n} \sum_{L \subseteq K^{sep}} |D_{L|K}| = \sum_{\substack{L|K \\ \text{up to} \cong}} \frac{|D_{L|K}|}{\# \mathrm{Aut}(L)} = \frac{1}{q^{n-1}}.$$

Pf For any L as above, let
$U_L = \{ \pi \in \mathcal{O}_L \mid v_L(\pi) = 1 \}$ be the set of uniformizers of L.

$$v_L(\pi) = n \cdot v_K(\pi)$$

Let $\sigma_1, \dots, \sigma_n$ be the embeddings $L \hookrightarrow K^{sep}$.
Identify monic deg. n pol. $f(X) = X^n + a_{n-1}X^{n-1} + \dots + a_0 \in \mathcal{O}_K[X]$ with vectors $(a_{n-1}, \dots, a_0) \in \mathcal{O}_K^n$.
Let $P_n \subseteq \mathcal{O}_K^n$ be the set of monic separable degree n Eisenstein pol. $f(X)$.

$v_K(a_{n-1}), \dots, v_K(a_1) \geq 1$, $v_K(a_0) = 1$

The min. pol. $f(X) = \prod_{i=1}^{n} (X - \sigma_i(\pi))$ of any $\pi \in U_L$ lies in P_n.

$\rightsquigarrow$ map $\varphi_L : U_L \longrightarrow P_n$
$\pi \longmapsto$ min. pol.

$\rightsquigarrow$ map $\varphi : \bigsqcup_{\substack{L \subseteq K^{sep} \\ \text{as above}}} U_L \longrightarrow P_n$

(disjoint union because $L = K(\pi)$).

All n roots of any $f(X) \in P_n$ have $v_K(\pi) = \frac{1}{n}$, so they each generate a tot. ram. sep. deg. n ext. L/K, so lie in some U_L.

$\Rightarrow$ Any $f(X) \in P_n$ has exactly n preimages in $\bigsqcup U_L$.

Endow K and L with Haar measures such that $\mathrm{vol}(\mathcal{O}_K) = \mathrm{vol}(\mathcal{O}_L) = 1$.

$$\mathrm{vol}(\underbrace{\{\text{mon. deg. } n \text{ Eisenstein pol.}\}}_{\subseteq \mathcal{O}_K^n})$$

$$= \mathrm{vol}(\{x \in \mathcal{O}_K \mid v_K(x) \geq 1\})^{n-1}$$ (coeff. $a_{n-1}, \dots, a_1$)

$$\cdot \mathrm{vol}(\{x \in \mathcal{O}_K \mid v_K(x) = 1\})$$ (coeff. a_0)

$$= (q^{-1})^{n-1} \cdot (q^{-1} \cdot (1 - q^{-1}))$$

$$= q^{-(n-1)} \cdot (q^{-1} - q^{-2}).$$

$$\mathrm{vol}(\underbrace{\{\text{mon. deg. } n \text{ inseparable pol.}\}}_{\subseteq \mathcal{O}_K^n})$$

$$= 0$$

f(x) inseparable
$\Leftrightarrow$ disc(f) = 0
disc(f) is a polynomial ($\neq 0$)
in the coeff. of f(x)

$$\Rightarrow \mathrm{vol}(P_n) = q^{-(n-1)} \cdot (q^{-1} - q^{-2})$$