

Exercise: Show $\mathbb{Q}_p^{\text{tr}}$ contains a primitive p th root of unity.

Diagram showing field extensions: $\mathbb{Q}_p \subset \mathbb{Q}_p^{\text{tr}}$. The degree of field extension is $p-1$. $\bigcup_{n=1}^{\infty} \mathbb{Q}_p(\mu_n) \cong \bigcup_{n=1}^{\infty} \mathbb{Q}_p(\zeta_n)$. $\text{Gal}(\mathbb{Q}_p^{\text{tr}}/\mathbb{Q}_p)$ is isomorphic to $\mathbb{Z}_{(p)}$.

things in $\mathbb{Q}$ w/ denominator prime to p .

Apply Herstein's Lemma after adding in $p^{1/(p-1)}$.

$$|\mathbb{Q}_p^{\text{tr}}| = p$$

② Give a Galois extension of $\mathbb{Q}_p^{\text{tr}}$.

$\mathbb{Q}_p^{\text{tr}}(\zeta_{p^2})$ is Galois. $\zeta_{p^2} \notin \mathbb{Q}_p^{\text{tr}}$. Need to justify $\zeta_{p^2} \notin \mathbb{Q}_p^{\text{tr}}$.

$$|p^2 - 1| = |p - 1|$$

$\mathbb{Q}_p^{\text{tr}}(p^{1/p})$ absolute value has to be $p^{-1/p}$. $x^p - p$.

$\mathbb{Z}$ roots of unity

1 sends $\zeta \mapsto \zeta^p$

$(\mathbb{Z}/(p))^{\times}$ roots of unity

$1 \mapsto p$.

Absolute Galois group of $\mathbb{F}_q$:

$\mathbb{F}_q$ = a field with q elements $q = p^n$.

can fix as follows:

$$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$$

Fix an algebraic closure $\overline{\mathbb{F}_p}$.

$\mathbb{F}_q$ = Roots of $x^q - x$ in $\overline{\mathbb{F}_p}$.

Note $x \mapsto x^q$ $(\text{Frob}_p)^n =: \text{Frob}_q$ Field automorphism. $\text{Frob}_p: x \mapsto x^p$.

Roots of $X^q - X = \text{Fixed points of } \text{Frob}_q$

so $\mathbb{F}_q \subseteq \overline{\mathbb{F}_p}$ is a subfield.

$$(X^q - X)' = -1 \quad \text{so has } q \text{ roots in } \overline{\mathbb{F}_q}$$

↑
so separable

$$\text{thus } |\mathbb{F}_q| = q.$$

$\overline{\mathbb{F}_p}$ is also a alg. closure of $\mathbb{F}_q$ will write it as $\overline{\mathbb{F}_q}$.

$$\overline{\mathbb{F}_q} = \bigcup_{n \geq 1} \mathbb{F}_{q^n}$$

$$\mathbb{F}_{q^n} = \text{Fix}(\text{Frob}_q^n).$$

If $\alpha \in \overline{\mathbb{F}_q}$. Then $\mathbb{F}_q(\alpha)$ is a finite ext'n of $\mathbb{F}_q$. So it has cardinality

$$|\mathbb{F}_q(\alpha)| = q^{\deg \alpha}$$

$$|\mathbb{F}_q(\alpha)^\times| = q^{\deg \alpha} - 1$$

Everything has order $q^{\deg \alpha} - 1$

i.e., is a root of $X^{q^{\deg \alpha} - 1} - 1$

thus of $X^{q^{\deg \alpha}} - X$

$$\text{Also see } [\mathbb{F}_{q^n} : \mathbb{F}_q] = n$$

and thus Galois theory gives

$$\text{Aut}(\mathbb{F}_{q^n}/\mathbb{F}_q) = \langle \text{Frob}_q \rangle \cong \mathbb{Z}/n\mathbb{Z}.$$

Conclusion: $\text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q) = \varprojlim_n \mathbb{Z}/n\mathbb{Z} \cong \varprojlim_n \text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \ni (\text{Frob}_q)_n = (1)_n$

↓
Generates a dense $\mathbb{Z}$.

Note: "The absolute Galois group of the finite field of order q " makes sense independent of choices.

↑ Because it's abelian.

Also makes sense to say this group
is $\hat{\mathbb{Z}}$. ↪ canonical choice of generator.

We have $\mathbb{F}_q/\mathbb{F}_p \rightsquigarrow W(\mathbb{F}_q)[\frac{1}{p}] / W(\mathbb{F}_p)[\frac{1}{p}]$
"extending coefficients from $\mathbb{F}_p$ to $\mathbb{F}_q$ "

like $\mathbb{F}_q((t)) \rightsquigarrow \mathbb{F}_q \otimes_{\mathbb{F}_p} \mathbb{F}_p((t)) / \mathbb{F}_p((t))$
 $\mathbb{F}_q((t)) / \mathbb{F}_p((t)).$

$W(\cdot)[\frac{1}{p}] \rightsquigarrow \cdot \otimes_{\mathbb{F}_p} \mathbb{F}_p((t))$

↗ Turns extension of $\mathbb{F}_p$ into extens of $\mathbb{Q}_p$

↗ turns extension of $\mathbb{F}_p$ into $\mathbb{F}_p((t))$

Exercise = Let $q = p^n$. Show $W(\mathbb{F}_q)[\frac{1}{p}] / W(\mathbb{F}_p)[\frac{1}{p}] = \mathbb{F}_p$
is a degree n field extension.

$$x^q - x \in \mathbb{F}_p[x]$$

Claim is $W(\mathbb{F}_q)[\frac{1}{p}]$ is a splitting field for $x^q - x$
 " $x^{p^n} - x$.

Hensel's Lemma shows $x^q - x$
 splits in $W(\mathbb{F}_q)[\frac{1}{p}]$
 because each of its roots will lift.

$\mathbb{F}_q / \mathbb{F}_p$ take α a primitive element in $\mathbb{F}_q$
 i.e. α is a root of $x^q - x$
 not a root of $x^{p^k} - x$ for $k < n$

$M(X)$ = minimal polynomial in $\mathbb{F}_p[X]$.

$$X^n + a_{n-1}X^{n-1} + \dots + a_0.$$

$$\tilde{m}(X) = X^n + \sum a_{n-1} X^{n-1} + \dots + a_0 \in \mathbb{Z}_p[X]$$

Gauss-Lemma: $\tilde{m}$ reducible in $\mathbb{F}_p[X]$.

$\Rightarrow$ reducible in $\mathbb{Z}_p[X]$

$\Rightarrow$ reducing mod p gives
 reducible in $\mathbb{F}_p[X]$ $\Leftarrow$

$\Rightarrow$ irreducible.

Hensel's lemma gives zero of $\tilde{m}(X)$.
 $\mathbb{F}_p[X] / \tilde{m}(X) \rightarrow W(\mathbb{F}_q)[\frac{1}{p}]$

(1)

Don't need any of this for exercise.

One good way: IF $\mathbb{F}_q = \langle \alpha_1, \alpha_2, \dots, \alpha_n \rangle$
as an $\mathbb{F}_p$ -vector space

show $W(\mathbb{F}_q)[\frac{1}{t}]$
is a $W(\mathbb{F}_p)[\frac{1}{p}]$ vector space
with basis
 $[\alpha_1], [\alpha_2], \dots, [\alpha_n]$.

In fact
(Any lifts of a basis of $\mathbb{F}_q$ are a
vector space $\leadsto$ a basis
of $W(\mathbb{F}_q)$ as a
 $\mathbb{Z}_p$ -module.)

Look at analogy with

$$\mathbb{F}_q((t)) / \mathbb{F}_p((t)).$$

Get $W(\mathbb{F}_q)[\frac{1}{p}]$ is a splitting field for

$$X^q - X \text{ over } \mathbb{F}_p.$$

$$\leadsto \bigcup_{q=p^n} W(\mathbb{F}_q)[\frac{1}{p}] \subseteq W(\overline{\mathbb{F}_q})[\frac{1}{p}].$$

is a splitting field for $\{X^N - 1\}_{(N,p)=1}$.

Above see roots of $X^{p^n-1} - 1$
generate the field

Hensel's lemma $\Rightarrow$ contains all roots
of $X^N - 1$

Valued Fields:

A valued field is a pair $(K, |\cdot|)$

K a field

$|\cdot|$ absolute value on K

$$|\cdot|: K \rightarrow \mathbb{R}$$

$$\text{c.t. } |xy| = |x||y|$$

$$|x| = 0 \Leftrightarrow x = 0$$

$$|x+y| \leq |x| + |y|$$

($|\cdot|$ ultrametric if $|x+y| = \max(|x|, |y|)$.)

For $c > 1$ and $|\cdot|$ is ultrametric $\Rightarrow$

valuation

$$v(x) = \log_c |x|$$

$$v(xy) = v(x) + v(y)$$

$$v(x+y) \geq \min(v(x), v(y))$$

Remark Every archimedean (= not ultrametric) valued field
 has an embedding $(K, |\cdot|) \rightarrow (\mathbb{C}, |\cdot|_{\text{std}})$
 s.t. $|\cdot| \sim |\cdot|_{\text{std}}$.
 $\uparrow$ equivalent to.

For us we'll only use non-archimedean / ultrametric.

Def'n 1) $(K, |\cdot|)$ is complete if Cauchy sequences converge.

($|\cdot|$ defines a topology on K).

2) $(K, |\cdot|)$ is discretely valued if

$|K^\times| \subseteq \mathbb{R}_{>0}$ is a discrete set

E.g. $|\Phi_p^x|_p = p^{\mathbb{Z}} = \{ \dots, \frac{1}{p^2}, \frac{1}{p}, 1, p, p^2, \dots \}$

$v_p(\Phi_p^x) = \left(\mathbb{Z} \subseteq \mathbb{R} \right)$
 discrete

