If $F \subset E$ is Galois and algebraic, then splitting and separable.

$\leftarrow$ If $F \subset E$ is algebraic, splitting and separable then Galois.

<u>WTS</u> if $u \in E \setminus F$ then $\exists \tau \in Gal(E/F)$ st $\tau . u \neq u$.

$u \in E \setminus F$ so u is algebraic, let $p(x) \in F(x)$ its minimal polynomial.

<u>Observe</u> since $u \notin F$, $\deg(p) > 1$
Since E is splitting, p splits over E
Since E is separable, roots of p are all different.
$\rightarrow$ $\exists \underset{\neq u}{u'} \in E$ also solving p

So, look at

$$\begin{tikzcd} & K(u) \arrow[r, phantom, "\subset"] \arrow[d, "\cong"', "u \mapsto u'"] & E \\ F \arrow[ur, phantom, "\subset"] \arrow[dr, phantom, "\subset"] & & \\ & K(u') \arrow[r, phantom, "\subset"] & E' \end{tikzcd}$$

$\rightsquigarrow$ extend iso

splitting

So, we built $\tau : E \longrightarrow E$ st $\tau|_F = id$ but $\tau . u = u'$.

Jan 21

If F is a finite field, then it has <u>positive</u> characteristic.

Examples of finite fields

$F_p = \mathbb{Z}/(p)$ p prime

$F_3 = \{0, 1, -1\} \longrightarrow -1$ is not a square
So $F_3(\sqrt{-1}) = F_3(x)/(x^2+1) \longrightarrow$ is a field

In F_5, $-1 = 2^2$ so $F_5(x)/(x^2+1)$ is not a field

Given any unital commutative ring, $\exists !$ unital map
$\mathbb{Z} \longrightarrow R$

$\mathrm{Ker}(\mathbb{Z} \longrightarrow R) = (m)$

If R is a field then $\underbrace{(m)}$ is prime or 0
called characteristic
of the field $\mathrm{char}(R)$

If $\mathrm{char}(F) = 0$ then $F \supset \mathbb{Q}$ "a rational field"
If $\mathrm{char}(F) = p > 0$, then $F \supset \mathbb{F}_p$

Fun Exercise

Ring homomorphism $\mathbb{Z} \rightarrow \mathbb{Q}$ is epic and monic not $\cong$
$\mathbb{Z} \rightarrow \mathbb{Z}_p$ is epic not monic

$\mathbb{Q}$
or $\mathbb{C}$ F are called <u>prime subfield</u> of F
$\mathbb{F}_p$

Let F be a finite field of order $q < \infty$.
Then $\mathbb{Z} \not\subset F$ so $\mathrm{char}(F) = p$, some positive prime number.
And $\mathbb{F}_p \subset F$ is finite field extension of deg $n < \infty$.
Must have $q = p^n$, a prime power.

Since F is a field, $F - \{0\}$ is a finite abelian group of order $q-1$.
Every finite abelian group is a product of cyclic groups.

If $C_n \times C_m$ cyclic group iff $(m, n) = 1$ (relatively prime)

A finite abelian group can fail to be cyclic iff it contains a subgroup $\cong C_r \times C_r$ for r, a prime.

Can $F^* \supset C_r \times C_r$? No.

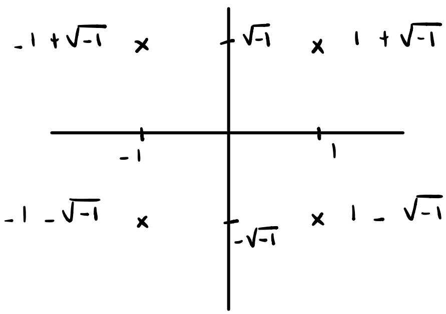
Because if $C_{r^2} \subset F$, then F contains at least r^2 roots to $x^r - 1$. But if r prime then $r^2 > r$.

Thm If F is a finite field, F^* is cyclic of order $q-1$ for some $q = p^n$.

Corollary $\exists\, u \in F$ such that $F = \mathbb{F}_p(u)$. Namely pick u any generator of cyclic group F^*.

The minimal polynomial of u has degree n.

Example $\mathbb{F}_3(\sqrt{-1})$



$u = 1 + \sqrt{-1}$ has order 8 in $\mathbb{F}_3(\sqrt{-1})$.

What is the minimal polynomial ?

$u^2 = 1 + 2\sqrt{-1} - 1 = 2\sqrt{-1} = -\sqrt{-1} = -u+1$

$\longrightarrow u^2 - u + 1$

$Gal(F/\mathbb{F}_3) = \mathbb{Z}/2$

$\# Gal(\text{any field extension}) \leq \deg(\text{field extension})$ with equality for Galois extension.

Let F be a finite field of order $q = p^n$.

Remark $\mathrm{char}(F) = p \qquad [F : \mathbb{F}_p] = n$

Look at reducible polynomial $f(x) = x^q - x \in \mathbb{F}_p(x)$

- if $x = 0$, $x^q = x$
- if $x \neq 0$, $x \in F^*$ (group of order $q-1$), so $x^{q-1} = 1$ and $x^q = x$

$\longrightarrow f(x) = 0$

$f(x)$ has deg $= q$ so q distinct roots in F.
So F is a splitting field of f over F_p and f is seperable.

1) Splitting field unique up to $\cong$

if $\#F = \#F' < \infty \rightarrow F \cong F'$

So any two extensions of F_p of same degree are $\cong$

$\rightarrow$ false for $\mathbb{Q}$!

{ F_q is well defined for any prime power of q }

2) Seperable splitting fields are Galois.

if F is finite of order q, then $F_p \subset F_q$ is Galois.
Its Galois group has order n where $q = p^n$.

3) F_q exists

↑ the field of order q

$\rightarrow$ the splitting field of $x^q - x$

4) If $F_q \subset F_{q'}$ any inclusion of finite fields, then Galois

When is there an inclusion $F_q \subset F_{q'}$?

- No, if char don't match
  $\rightarrow q = p^n$ and $q = p^m$
- No, if $m \nmid n$
- Yes, if $m \mid n$

If $m \mid n$, then $x^{p^m} - x$ divides $x^{p^n} - x$ over $\mathbb{Z}$ so also over F.

<u>Finite fields of char $= p$</u>

$F_p \quad F_{p^2} \quad F_{p^3} \quad F_{p^4}$

This poset is a copy of the poset of positive integers sorted by divisibility $\cong \mathbb{N}^\infty$

Suppose F, a field of char p. Consider

$$Fr: F \longrightarrow F$$
$$x \longmapsto x^p$$

$$(\alpha+\beta)^p = \alpha^p + \underbrace{\binom{p}{1}\alpha^{p-1}\beta + \dots + \binom{p}{p-1}\alpha\beta^{p-1}}_{\text{div by } p} + \beta^p$$

$$= \alpha^p + \beta^p$$

φ is field homomorphism hence inclusion. If F is finite, φ is $\cong$.

Let $F = F_q$, $q = p^n$, then $\varphi^n|_F = id|_F$.
On the other hand, if $\varphi^n|_F = id|_F$, that would solve $x^{p^n} - x$. So fixed points of φ^n roots of $x^{p^n} - x$, $\leq p^n$ of them.
$\varphi^n|_F \neq id|_F$ if $k<n$

$\rightarrow$ $Gal(F_{p^n}/F_p)$ is cyclic group of order n generated by Fr iso φ.

Jan 24

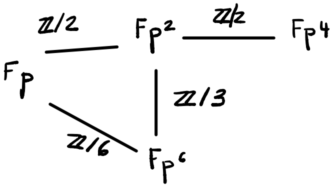
Fix prime $p > 0$.
Recall For each p, $\exists!$ (up to iso) field F_{p^n} of order p^n.
$Gal(F_{p^n}/F_p)$ is cyclic group of order n generated by Fr iso $\varphi: F \longrightarrow F$

$$x \longmapsto x^p$$

If $R \supseteq F_p$ is a commutative ring, then $(x+y)^p = x^p + y^p$ so $Fr: R \longrightarrow R$ is a ring endomorphism.

What is the algraic closure of $\overline{F_p}$?
$F_p \subset \overline{F_p}$ has to be algebraic so any element in $\overline{F_p}$ lives in some $F_{p^n} \subset \overline{F_p}$ and all F_{p^n} are in $\overline{F_p} = F_{p^\infty}$

$$F_p \quad \begin{matrix} \subset & F_{p^2} \\ & F_{p^3} \\ & F_{p^5} \end{matrix} \quad \subset \quad F_{p^{10}}$$



Whatever $\overline{\mathbb{F}_p}$ is, it is a splitting field.

So, $\mathbb{F}_p \subset \mathbb{F}_{p^n} \subset \overline{\mathbb{F}_p}$

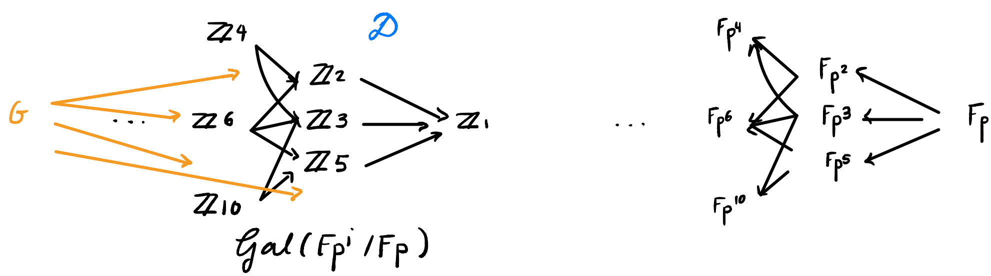
We have $Gal(\overline{\mathbb{F}_p} / \mathbb{F}_p) \longrightarrow \underbrace{Gal(\mathbb{F}_{p^n} / \mathbb{F}_p)}_{\mathbb{Z}/n}$

Moreover,

$$\begin{tikzcd}
Gal(\overline{\mathbb{F}_p} / \mathbb{F}_p) \arrow[r] \arrow[dr] & Gal(\mathbb{F}_{p^{mn}} / \mathbb{F}_p) = \mathbb{Z}/mn \arrow[d, "\text{standard map}"] \\
& Gal(\mathbb{F}_{p^n} / \mathbb{F}_p) = \mathbb{Z}/n
\end{tikzcd}$$

Any endomorphism of $\overline{\mathbb{F}_p}$ is non-trivial on some finite extensions.

We have a diagram of groups



The projective limit, projlim$(\mathcal{D}) = \varprojlim(\mathcal{D})$ is the group such that if G is any group that map to all entries in the diagram, making everything commute then we should have $G \longrightarrow \varprojlim(\mathcal{D})$

Slogan $\varprojlim(\mathcal{D})$ is the universal object with a map to the diagram from itself.
Dual $\varinjlim(\mathcal{D})$ is the universal object with a map from the diagram to itself.

$$\varprojlim(\mathcal{D}) \longrightarrow \mathcal{D} \qquad\qquad \mathcal{D} \longrightarrow \varprojlim(\mathcal{D})$$

Diagram of all cyclic group

$$\begin{tikzcd}
\varprojlim\big(\cdots \arrow[r] & \mathbb{Z}/mn \arrow[r] & \mathbb{Z}n \arrow[r] & \cdots \big) & = \mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) \\
& \mathbb{Z} \arrow[ul] \arrow[u] \arrow[ur] & & & \mathrm{Fr} : x \longmapsto x^p \arrow[u, phantom, "\in" rotate=90]
\end{tikzcd}$$

Pick $\ell = 10$, get the diagram:

$$\begin{tikzcd}
\cdots \arrow[r] & \mathbb{Z}/\ell^4 \arrow[r] & \mathbb{Z}/\ell^3 \arrow[r] & \mathbb{Z}/\ell^2 \arrow[r] & \mathbb{Z}/\ell \arrow[r] & \mathbb{Z}/1 \\
\cdots & & \text{last 3 digits} \arrow[u] & \text{last 2 digits} \arrow[u] & \text{ones digits} \arrow[u] &
\end{tikzcd}$$

So, any sequence of digits even if it goes ∞ to the left, still has a residue mod ℓ^n $\forall n$.

Take infinite sequences of digits

$$\begin{array}{rcccc}
 & \cdots & a_3 & a_2 & a_1 & a_0 \\
+ & \cdots & b_3 & b_2 & b_1 & b_0 \\
\hline
 & & & a_2 + b_2 + \text{carry} & a_1 + b_1 + \text{carry} & a_0 + b_0
\end{array}$$

Definition $\mathbb{Z}_\ell$ is the set of infinite to the left sequences of digits in base ℓ.

$\mathbb{Z}_\ell$ called ℓ-adic integers

It is a ring because you can add a multiply from right to left.

decimal expansion

$\mathbb{Z} \subset \mathbb{Z}_\ell$ as the eventally zero expansion.

Now, $\ell = -5$. What decimal expansion base 5 of -2?

$-2 = 3 \mod 5$

$-2 = 23 \mod 25$ $\qquad -2 = \dots 4443$

$$= 4 \times 5 + 3$$

$-2 = 4 \times 5^2 + 4 \times 5 + 3 \mod 125$

$$\begin{array}{rcccc} & \dots & \overset{1}{4} & \overset{1}{4} & \overset{1}{4} & 3 \\ + & \dots & 0 & 0 & 0 & 2 \\ \hline & \dots & 0 & 0 & 0 & 0 \end{array}$$

Slogan No room to the left for minus sign.

What decimal expansion base 5 of $1/2$?

$1 = 6 \mod 5 \longrightarrow 1/2 = 3 \mod 5$

$\longrightarrow$ 3 is the unique solution of $2x = 1 \mod 5$.

$1/2 = 3 \mod 5$ $\qquad 1/2 = \dots 2223$

$1/2 = 13 \mod 25$ $\qquad 2 \times 5 + 3$

$1/2 = 63 \mod 125$ $\qquad 2 \times 5^2 + 2 \times 5 + 3$

$1/2 = 2 \times 5^3 + 2 \times 5^2 + 2 \times 5 + 3$

$$\begin{array}{rccccc} & \dots & 2 & 2 & 2 & 3 \\ \times & \dots & 0 & 0 & 0 & 2 \\ \hline & & & 0 & 0 & 1 \end{array} \qquad \begin{array}{rccccc} & \dots & \overset{1}{2} & \overset{1}{2} & \overset{1}{2} & 3 \\ + & \dots & 2 & 2 & 2 & 3 \\ \hline & & & 0 & 0 & 1 \end{array}$$

So, the finite length expansions are "dense" in $\mathbb{Z}_\ell$.
Projective limits are often thought of as topological objects.

$$\begin{tikzcd}
\varprojlim (\cdots \arrow[r] & \mathbb{Z}/mn \arrow[r] & \mathbb{Z}_n \arrow[r] & \cdots) = \hat{\mathbb{Z}} = Gal(\overline{F_p}/F_p) \\
& \mathbb{Z} \arrow[ul] \arrow[u] \arrow[ur] &
\end{tikzcd}$$

$$\hat{\mathbb{Z}} = \prod_{\text{primes}} \mathbb{Z}/\ell$$

$$\mathbb{Z}/n = \prod_{\ell \in \text{prime}} \mathbb{Z}/\ell^n$$

Jan 26

If $F \subset E$ extension of finite fields, then Galois.
Fix $p > 0$ char.
Fields of char(p) have a distinguished endo
$$Fr : u \longmapsto u^p \quad (\text{inj})$$
In finite field case, Galois(F/F^p) is cyclic $= \mathbb{Z}/\dim \mathbb{F}$
Fr is $\cong$ $\qquad$ Galois$(E/E^p) = \mathbb{Z}/\dim_{\mathbb{Z}^p}(\mathbb{F})$

So, $Gal(E/F) = \dfrac{\mathbb{Z}}{[\mathbb{E}:\mathbb{F}]}$ generated by $Fr^{[F:F^p]}$

In the infinite case
Example $F^p(t) \longleftarrow$ rational fct field over F_p
field of fractions of $F_p[t]$
Typical element: $\dfrac{f(t)}{g(t)}$ $\quad f,g$ are relatively prime in $F_p[t]$

$$Fr\left(\frac{f(t)}{g(t)}\right) : \quad Fr(a_0 + a_1 t + \dots + a_n t^n) = a_0 + a_1 Fr(t) + \dots + a_n Fr(t^n)$$
$$= \frac{f(t^p)}{g(t^p)}$$

Remark In this case Fr is not surjective
$t \in F_p[t]$, $\quad t \neq Fr(\text{anything})$

Set $s = t^p = Fr(t)$

$F_p(s) \subsetneq F_p(t)$

$\uparrow$ image of Fr

$K = F_p(s) \subsetneq F_p(t) = L$

$K \subseteq L$ is algebraic

$L = K[\sqrt[p]{s}]$ algebraic extension of degree p.

$$\begin{array}{l} K \subset L \\ \quad\; \cup\!\!\!\! \mid \\ \quad\; t \end{array} : \text{What is the minimal polynomial of } t \text{ in } K[x]?$$

$$\longrightarrow \underbrace{x^p - s}_{\text{irreducible in } K[x]}$$

Definition A polynomial $f(x) \in K[x]$ is <u>separable</u> if in some splitting field of f, f has no repeated roots.
This happens iff $\gcd(f, f') = 1$

Definition A polynomial $f(x) \in K[x]$ is <u>purely inseparable</u> if in some splitting field of f, all roots of f are the same.
This happens if $f(x) = (x - \alpha)^p$

<u>Remark</u> f both separable and purely inseparable if it is linear.

If $K \subset L$ an alg extension and $u \in L$, u is <u>seperable</u> over K or <u>purely inseperable</u> if minimal poly $f(u)$ is.

If $f(x)$ is irreducible
Then $\gcd(f, f') = \begin{cases} 1 & f' \neq 0 \\ 0 & f' = 0 \end{cases}$

$[a_0 + a_1 x + \dots + a_n t^n]' = a_1 + 2a_2 x + \dots + p\, a_p{}^{p-1}$

is zero if $f_0(x) = f'(x^p)$.

Let $K \subset L$, $u \in L$ alg.
$\longrightarrow$ u is seperable or minimal poly of u is $f(x) = f_1(x^p)$
So $u_0^p = u_1$.

Roots of f_1 are p^{th} powers of roots of f_0.
After passing into a splitting field of f_0, we find that f_1 also splits.

If f_1 is not purely inseperable $\rightarrow$ so is f_0

If f_1 is purely inseperable $\longrightarrow$ so is f_0.
f_1 has only 1 root, roots of f_0 are $\sqrt[p]{u_1}$

If char $= p$ then $(x^p - 1) = (x-1)^p$ so 1 has only one p^{th} root so every element has one p^{th} root.

Let $K \subset L$, $u \in L$ alg.
$\longrightarrow$ u is seperable or $u = \sqrt[p]{Fr u}$ and either $Fr u$ is seperable or repeat
min poly of u is $g(u^p)$ where g is min poly of $Fr(u)$

So some u^{p^k} is seperable for some k : $Fr^k(u)$.

u is purely inseperable iff $Fr(u)$ is purely inseperable iff $Fr^2(u)$ is purely inseperable ...

If $K \subset L$, $u \in L$ alg, then u is purely inseperable over K iff after applying Fr some # of times you stay in K.

$$\left\{\begin{matrix}\text{purely insep} \\ \text{elements of } L\end{matrix}\right\} = Fr^{\infty}(K)$$

$$\begin{matrix} \parallel \\ L^{insep} \end{matrix}$$

Corollary

L^{insep} is a field.

Theorem

$F \subset K \subset E$

$\rightarrow$ if $F \subset K$ and $K \subset E$ alg and Galois then $F \subset E$ is alg and Galois (not true)

Theorem

(1) L^{sep} and L^{insep} are subfields

$K \subset L$ alg extension

$$\begin{matrix} & & \text{purely insep} & & \\ & \subset & L^{insep} = \{\text{purely inseperables}\} & \subset & \\ K & & \text{purely insep} & & L \\ & \subset & L^{sep} = \{\text{purely seperable}\} & \cup & \end{matrix}$$

(2) $L^{sep} \subset L$ is purely inseperable

$L^{insep} \subset L$ is seperable iff $L^{sep} \times L^{insep}$

(3) If $K \subset L$ is splitting then so are L^{sep}, L^{insep}, and $K \subset L^{sep}$ and $L^{insep} \subset L$ are Galois.

$$Gal(L/K) \cong Gal(L^{sep}/K)$$
$$\cong Gal(L/L^{insep})$$

Remark If $F \subset E$ is purely inseperable then $Gal(E/F)$ is trivial.

Normal: $K \subset L$, $u \in L$, min poly of u splits completely over K. If irreducible poly over K has root in L then has all roots in L.

$$\begin{tikzcd}
& \text{inseparables} \arrow[dr, "G"] & \\
K \arrow[ur, "\text{trivial}"] \arrow[rr, "G"] \arrow[dr, "G"'] & & L \\
& \text{separables} \arrow[ur, "\text{trivial}"'] &
\end{tikzcd}$$

Jan 28

Theorem

$F \subset K \subset E$

$\rightarrow$ if $F \subset K$ and $K \subset E$ $\overbrace{\text{alg and Galois}}^{\text{1) splitting, 2) separable}}$ then $F \subset E$ need not be Galois

An algebraic extension $F \subset E$ is normal if for any $u \in E$, the minimal polynomial of u over E splits completely over E.

Suppose $E = F(u_1, \dots, u_n)$. The minimal polynomials of these u_i's split completely, then $\forall u \in E$, the minimal polynomial of u over E splits completely in E.

proof Let f minimal polynomial of u.
Look at $F \subset F(u) \subset E \subset E(\dots)$
(on the homework)

This part of a pattern where if $E = F(u_1, \dots, u_n)$ and all the u_i's have some property, often, all $u \in E$ have that property.

Example

- If all u_i's are purely inseparable over F then $\forall u \in E$ is.
u_i is purely inseparable iff $Fr^N(u_i) \in F$ for large N.

If all u_i's are purely inseperable over F, then
$Fr^N E \subseteq F \quad N >> 0$

- If $E = F(u_1, \dots, u_n)$ and all u_i's are seperable then $\forall u \in E$ is seperable.

proof Let f minimal polynomial of u
Let $u \in E$
$F \subset F(u) \subset E \subset K$ = splitting field of u_i's
We proved that $F \subset K$ is finite and Galois by counting sizes of various Galois group.
And, every element of a Galois exctension is seperable.

Seperable $\longleftrightarrow$ sub of Galois

Let $F \subset E$ algebraic

$$\begin{array}{cccc} & \overset{\text{purely insep}}{\subset} E^{insep} = \{\text{purely inseparables}\} & \subset & \\ F & & & E \\ & \overset{\text{seperable}}{\subset} E^{sep} = \{\text{purely seperable}\} & \subset & \end{array}$$

both fields and stable (we have restriction maps)

$$\begin{array}{ccc} & \nearrow & Gal(E^{sep}/F) \\ Gal(E/F) & & \\ & \searrow & Gal(E^{insep}/F) \end{array}$$

Because these subfields are stable we get a left-exact sequence:
$\forall$ stable $F \subset K \subset E$

$$1 \longrightarrow Gal(E/K) \longrightarrow Gal(E/F) \longrightarrow Gal(K/F)$$

Recall: A sequence of groups $1 \longrightarrow N \longrightarrow G \longrightarrow K$ is left-exact, if $N \longrightarrow G$ is injective and $\operatorname{Im} N = \operatorname{Ker}(G \longrightarrow K)$

$Gal(E^{insep}/F)$ is trivial so
$Gal(E/E^{insep}) \longrightarrow Gal(E/F)$ is isomorphic.
In particular $E^{Gal(E/F)} \supset E^{insep}$.
Also, if $F \subset E$ is Galois, no inseparables.

$\subset E^{insep} = \{\text{purely inseparables}\} \subset \qquad \subset$
F purely insep $\qquad\qquad\qquad\qquad K \subset \qquad E$
$\subset E^{sep} = \{\text{purely separable}\} \cup \qquad \cup$
separable $\qquad\qquad\qquad\qquad\qquad$ purely insep

Theorem In the diagram
Let $K = E^{insep}E^{sep}$, then $E^{insep} \subset E$ is separable iff $K = E$.

proof
$E^{insep} \subset K$ separable $\longleftarrow$
$\longrightarrow$ if $E^{insep} \subset E$ is separable then K is separable
But $K \subset E$ is purely inseparable. Must have $K = E$

Theorem If $F \subset E$ is splitting, all subextensions are splitting:
$F \subset E^{sep}$, $F \subset E^{insep}$ splitting.
- $F \subset E^{sep}$ is Galois
- E^{insep} is Galois

If $F \subset E$ is normal, $Gal(E/E^{insep}) \longrightarrow Gal(E/F)$
$\longrightarrow Gal(E^{sep}/F)$
$\cong$ both and Galois