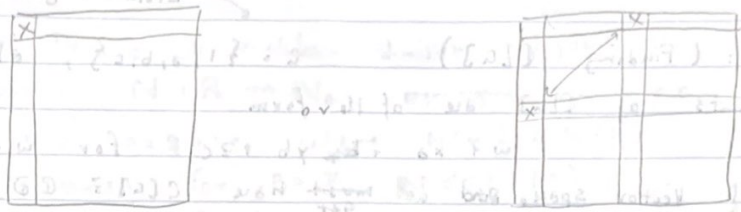
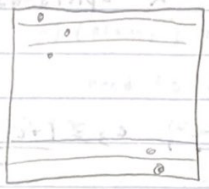
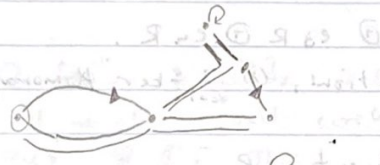
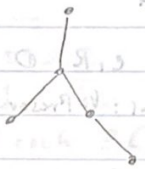
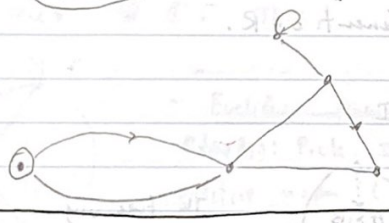










MATH 250
RING THEORY

Intro to Rings (Review of Basic Structures)

- Examples: Fields ($\mathbb{R}, \mathbb{C}$), $\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{R}[x]$, $M_n(\mathbb{R})$, ~~GRT~~ $R(G)$
- Definition: An abelian group with a multiplication that is associative, distributive
  ↳ In our class, all rings have identity, commutative, unless otherwise stated.
- Burnside Ring: Take a finite group G. We consider the ~~set~~ collection
- of finite sets acted on by G.
  ⟶ The operations are disjoint unions ($+$) and cartesian products ($\times$)
  For S_3, the elements are of the form $a A^1 + b A^2 + c A^3 + d A^6$ where A^k is the representation of the action on k points.
- Group Rings: (R a ring, G a group) $R[G]$ is the free abelian group with basis G, $\times$ is the group operation on G.
  ↳ left adjoint to the group of units:

$$\begin{array}{ccc} R & \longrightarrow & R^\times \\ \text{ring hom.} \uparrow & & \uparrow \text{Group Hom.} \\ \mathbb{Z}[G] & \dashrightarrow & G \end{array}$$

← Klein-4 group

- Example: (Finding $\mathbb{C}[G]$) - $G = \{1, a, b, c\}$, $ab = c$, $a^2 = b^2 = c^2 = 1$.

  All elements of $\mathbb{C}[G]$ are of the form

  $$w + xa + yb + zc \quad \text{for } w, x, y, z \in \mathbb{C}.$$

It is a 4D vector space, and we ~~must~~ get have $\mathbb{C}[G] \cong \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C}$.

We find the "idempotents": $e_i e_j = 0$, $e_i^2 = e_i$.

For a ring R, idempotent e, R splits as $eR \oplus (1-e)R$.

The idempotents of $\mathbb{C}[G]$ are

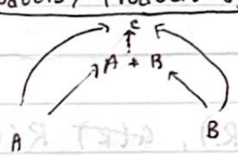
$$e_1 = \frac{1+a+b+c}{4}, \quad e_2 = \frac{1+b-a-c}{4}, \quad e_3 = \frac{1+c-b-a}{4}, \quad e_4 = \frac{1+a-b-c}{4}$$

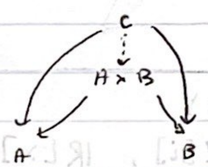
$$\Rightarrow \mathbb{C}[G] \cong e_1R \oplus e_2R \oplus e_3R \oplus e_4R.$$

- Ring Homomorphisms: (1) Preserve operations, (2) $\underset{\text{ideal}}{I}$ = ker "Homomorphism"

- Ideal has closure under any element of R.
  - ↳ contains 0, closed
  - ↳ $a \in I$, $b \in R \Rightarrow ab \in I$

Coproducts / Products of Rings:





The free ring on a set S is either

1. Free commutative ring: Form free group on S

UNIQUE FACTORIZATION:

Ex: • Define 1 as product of empty set of primes.
- Any integer is the product of primes in a unique way up to order, units.
- (units) non-zero elements of field
- (irreducible) Let $a \neq$, $a \neq$ unit, If $a = bc$, then b or c is a unit.
- (prime) If $a \neq 0$, $a \neq$ unit, If $a | bc$, then $a | b$ or $a | c$.
  - ↳ These notions being equivalents usually means UFD.

EUCLIDEAN ⟹ Principal Ideal Domains ⟹ Unique Factorization Domain.

• Euclidean: There is a euclidean division algorithm.

→ Given a function $N : R \to \mathbb{N}_0$, ~~we get~~ for $a \neq 0$, $b \in R$, $\exists q, r$ with $a = qb + r$ where $N(r) < N(b)$.

• Examples of Norms: for $R = \mathbb{Z}$, $N(a) = |a|$

for $R = K[x]$, $N(a) = \deg(a) + 1$ $(\text{or } 0 \text{ if } a = 0)$

• $\mathbb{Z}[i]$ is Euclidean:

Proof: Define $N(m+ni) = |m+ni|^2 = m^2 + n^2$.

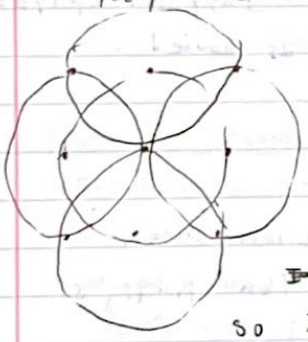
Given $a \neq 0$, b, need to find q, r with $N(r) < N(b)$ and

$a = qb + r \iff \frac{a}{b} = q + \frac{r}{b}$

$= q + x$ where $N(x) < 1$.

$a/b \in \mathbb{Q}[i]$, $q \in \mathbb{Z}[i]$, $x \in \mathbb{Q}[i] < 1$.

This, If we place unit circles at each $\mathbb{Z}[i]$, note that they cover $\mathbb{C}$. Thus, $\mathbb{Z}[i]$ is Euclidean.



• Euclidean Domains are PIDs.

claim: Pick $I \neq 0$ ideal. Pick b in I of smallest positive norm (possible by the well-ordering principle.)

$\Rightarrow I = bR$. Proof: If $a \in I$, put $a = qb + r$, $N(r) < N(b)$.

~~$I = bR$~~ $N(b)$ is minimal, so $N(r) = 0 \Rightarrow a = bq \Rightarrow a \in bR$

so $I = bR$.

• (PID ⇒ UFD) All principal ideal domains are unique factorization domains.

Proof:

(1) Every element a (not 0 or a unit) is divisible by an irreducible unit.

↳ • Start with an element a. if it's irreducible, done. Else $a = bc$.

• If b irreducible, done. Else let $b = ef$.

• Repeat this process until termination

* The process must terminate. If not, we have an infinite strictly increasing chain of ideals $(a) \subsetneq (c) \subsetneq (ef) \subsetneq \cdots$

~~Set $I = (a, b, d, \ldots) = (x)$ since PID.~~

Set $I = \bigcup (k) = (x)$. Then x is in I so it has to be in one of the ideals, so the chain stops.

- This holds because all PIDs are Noetherian.

(2) Every element is the product of irreducibles (Also true for Noetherian rings)

- From before (1), we have $a = bc$, $b = de$, ... which terminates.
b irreducible, d irreducible so $a = bdf \cdots$

(3) In a PID, irreducibles are prime.

Proof: Suppose p is irreducible, and $p \mid ab$. It suffices to show $p \mid a$ or $p \mid b$.

Consider the ideal $(p, a) = \{ xa + yp : x, y \in R \}$.

- $(p, a) = (c)$ since PID.
- if $p \nmid a$, then $\gcd(p, a) = 1$, so by ~~Bezout's lemma~~, $\exists x, y$ s.t. ✓ we don't have this for PID's yet.

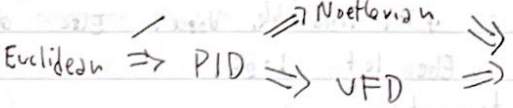
$$xp + ya = 1 \Rightarrow (p, a) = (1) = R. \quad (\times)$$

- ~~If $p \nmid a$, then~~ Suppose $p \nmid a$. since $c \mid p, a$ so c
- $c \mid p$ so $c = up$ for u a unit. If $c = up$, since $c \mid a$, then $p \mid a$ ↯
or $c = u$
Thus $c = u$.
- $(c) = (1)$ since c is a unit, so $(p, a) = R \Rightarrow \exists x, y$ s.t. $xp + ya = 1$.
- $xp + ya = 1 \Rightarrow \underbrace{xpb}_{\text{divisible by } p} + \underbrace{yab}_{\text{divisible by } p} = b$, ~~and~~ so $p \mid b$, as desired.

(4) Unique factorization

- Suppose $a = p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n$ where p_i, q_j are irreducible.
- p_1 is prime, so p_1 divides at least one of $q_1, \ldots, q_n$. Then $p_1 \mid q_i$, so $q_i = p_1 \cdot u$, (u a unit) as q_i is irreducible.
- ~~Repeat for each~~ Divide by p_1, q_i and repeat.

Summary:



• (Fermat) If p is prime and $p \equiv 1 \pmod 4$, $\exists\, x, y$ s.t. $p = x^2 + y^2$ (unique up to sign differences of x and y)

~~If $p \equiv 1 \pmod 4$, then $4 \mid p-1$. Now $(\mathbb{Z}/p\mathbb{Z})^\times$ has $= \mathbb{Z}/(p-1)\mathbb{Z}$, $p-1$ elements, so let g be a primitive root of $\mathbb{Z}/p\mathbb{Z}$. Then~~

Proof: $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic of order $p-1$, so let g be a primitive root of $(\mathbb{Z}/p\mathbb{Z})^\times$.

$g^{(p-1)/2} \equiv g^{4k} \equiv 1 \pmod p \Rightarrow g^{2k} \equiv -1 \pmod p$

$\Rightarrow -1 = a^2 - np$ for some n, a, so $np = a^2 + 1 = (a+i)(a-i) \in \mathbb{Z}[i]$

$p \nmid a-i, a+i$ so not irreducible, so $p = (a+bi)(a-bi) \in \mathbb{Z}[i]$

$\Rightarrow p = a^2 + b^2$, as desired.

• Interesting Notes: Principle ideals look rectangular. Non-principle ideals have more complicated structures ($(2, 1+i\sqrt{3})$ is hexagonal).

Prime and Maximal Ideals (Take all rings to be commutative)

• (Field) where $0 \neq 1$, a ring where all nonzero elements have inverses.

• (Integral Domain) $0 \neq 1$, No zero divisors other than 0.

• (Maximal Ideal) R/I is a field when I is maximal.

↪ $I \neq R$ is maximal if for any ideal J, $I \subseteq J$ implies $I = J$ or $J = R$.

• (Prime Ideal) R/I is an integral domain

↪ Or, $I \neq R$, $ab \in I \Rightarrow a \in I$ or $b \in I$.

→ R/I is integral domain $\Leftrightarrow$ $[(a+I)(b+I) = I \Rightarrow a \in I$ or $b \in I]$

$\Leftrightarrow$ $[ab + I = I \Rightarrow a \in I$ or $b \in I]$

$\Leftrightarrow$ $[ab \in I \Rightarrow a \in I$ or $b \in I]$.

• Question: If I is maximal, of S is $f^{-1}(I)$ maximal? ($f \in \text{RingHom}(R, S)$)

↪ No, but we do preserve primeness.

Proof:

$\frac{R}{f^{-1}(I)} \subseteq \frac{S}{I}$, an integral domain, so $R/f^{-1}(I)$ is an integral domain as a subring. ■

• Problem: If R is a nonzero ring, does it have prime / maximal ideals?
Yes, if you assume Zorn's Lemma.

• Localization: Constructing $\mathbb{Q}$ from $\mathbb{Z}$.

(1) Equivalence relation $(a,b) = (c,d)$ if $ad = bc$

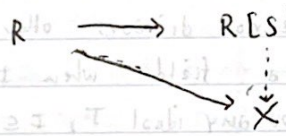
(2) $(a,b) + (c,d) = (ad+bc, bd)$

$(a,b) \times (c,d) = (ac, bd)$ Check operations are well-defined.

(3) Check field axioms.

• We can localize in general, for rings R and closed sets S containing
1. If S has no zero divisors, we copy the construction above.
2. If not, we force S to have no zero divisors by quotienting out by the ideal of elements $xs = 0$ for $s \in S$.
↳ If we do have zero divisors, the equivalence relation need not be transitive.

Properties of $R[S^{-1}]$:
- There is a homomorphism from $R \to R[S^{-1}]$
- All elements of S are invertible in $R[S^{-1}]$.
- $R[S^{-1}]$ is universal, i.e.



What is really going on here? We are forcing R to be a field by giving it inverses.

MODULES: "Vector Space over a Ring"

• (Module) A (left) module M over a ring R is an abelian group with a map from $R \times M \to M$ sending $(r,m) \mapsto r \cdot m$ such that for $r,s \in R$, $x,y \in M$

(1) $r \cdot (x+y) = rx + ry$

(2) $(r+s) \cdot x = rx + sx$

(3) $(rs) \cdot x = r \cdot (s \cdot x)$

(4) $1_R \cdot x = x$

A right module is the same but map is from $M \times R \to M$.

- (Module Homomorphism) $f: M_1 \to M_2$ w/
  (1) $f(m_1+m_2) = f(m_1) + f(m_2)$
  (2) $f(r \cdot m) = r \cdot f(m)$.
- Left <=> Right?
  - Yes, for commutative rings
  - If a module has a transpose operation, you can turn a left module into a right module:
    - R is commutative: $A^T = A$
    - $R = M_n(k)$: $A^T :=$ matrix ~~transpose~~ transpose
    - $R = \mathbb{Q}_8$: $(a+bi+cj+dk)^T = a-bi-cj-dk$
    - $R = \mathbb{Z}[G]$: $(\sum m_i g_i)^T = \sum m_i g_i^T = \sum m_i g_i^{-1}$.

Exercise: Suppose $0 \to A \xrightarrow{\phi} B \xrightarrow{\psi} C \to 0$ is exact. Show that (a) $0 \to \mathrm{Hom}_R(M,A) \to \mathrm{Hom}_R(M,B) \to \mathrm{Hom}_R(M,C)$ and (b) $\mathrm{Hom}_R(A,N) \leftarrow \mathrm{Hom}_R(B,N) \leftarrow \mathrm{Hom}_R(C,N) \leftarrow 0$ are exact, where M,N are modules over R.

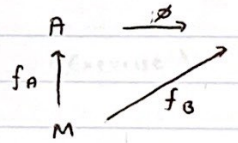
(Bimodule) A Left module over one ring and a right module over another, where the right and left actions commute.

- M is a left module over R $\Rightarrow$ M is a right module over $\mathrm{End}_R(M) = \mathrm{Hom}_R(M,M)$.

Proof:
R acts on left, $\mathrm{Hom}_R(M,M)$ acts on right. Furthermore
$(r \times m) f = r(mf)$ for $f \in \mathrm{End}_R(M)$, so the actions commute. ∎

- (Free Module) A Module M over R is free if it can be written as
$\underbrace{R \oplus R \oplus \cdots \oplus R}$
possibly infinite.

several Work:
ϕ injective, ψ surjective,
$\mathrm{im}\,\phi = \ker\psi$



$\phi(f_A) = (f_B)$
$\phi(f_A(x)) = \phi(f_B(x))$
~~$\ker\phi_M = \{\phi_M\}$~~ $\Rightarrow f_A(x) = f_B(x)$

Take
WTS $\mathrm{im}\,\phi_* = \ker\psi_*$
$\Leftrightarrow \psi_* \circ \phi_* = 0$
But $\psi_* \circ \phi_* = (\psi \circ \phi)_* = 0$
$\Rightarrow \mathrm{im}\,\phi_* \subseteq \ker\psi_*$
If $g(h(A)) = 0$, then $\forall x \in A\ \exists y$ s.t. $h(x) = f(y_x)$

11/5/19 : Algebraic Extensions:

- Extension of field F is $E \geq F$. Consider E/F
- Degree $[E:F]$ = dim of E as a vector space over F
- $[\mathbb{C}:\mathbb{R}] = 2$,
- $[\mathbb{Q}(x):\mathbb{Q}] = \infty$
  ↳ Field of Fractions

Ex: $[\mathbb{Q}[e^{2\pi i/7}]:\mathbb{Q}]$

$a^7 = 1$ as a root of $x^7 - 1 = 0$

$= (x-1)(\underbrace{x^6 + x^5 + \dots + x + 1}_{f(x)})$

a is a root

$\frac{\mathbb{Q}[x]}{(f(x))}$ is a field as f is irreducible, and has dim 6 as basis : $(1, x, x^2, \dots, x^5)$

$x \mapsto e^{2\pi i x/7}$ is a field isomorphism.

$\mathbb{Q}[e^{2\pi i/7}]$

- Given E/F, $a \in E$ is "algebraic" if it is the root of some polynomial with coefficients in F.

Ex: - $\sqrt[3]{2}$: $x^3 - 2 = 0$
- π, e : Transendental
- x in $\mathbb{Q}(x)$ is transcendental (Exercise)

Lemma: $a \in E$ is algebraic over F $\Leftrightarrow$ a is contained in a finite degree extension of F

Proof : $\Rightarrow$: a is algebraic $\Rightarrow$ a is a root of $f(x) \in F[x]$

"assume f is irreducible

$\frac{F[x]}{f(x)}$ is a field, finite over F,

$\frac{F[x]}{f(x)} \xrightarrow{x \mapsto a} E$, so the image is a finite extension of F contains

$\Leftarrow$: If a $\in$ Finite extension K over F, $[K:F] = n$.

Look at $\underbrace{1, a, \ldots, a^n}_{n+1 \text{ elements}}$ so there is a nontrivial linear relation

$b_0 + b_1 a + \cdots + b_n a^n = 0$, so a is a root of a polynomial.

Degree of a is defined as degree of $F[a]$.

Remark: What is $\frac{F[x]}{f(x)}$ if f is not irreducible?

Suppose $f = gh$, where $(g,h) = 1$. Then $\frac{F[x]}{f(x)} = \frac{F[x]}{g(x)} \times \frac{F[x]}{h(x)}$

"Chinese Remainder Theorem"

Put $F = p_1^{e_1} p_2^{e_2} \cdots p_i^{e_i}$ irreducible.

Then $\frac{F(x)}{f(x)} = \prod \frac{F[x]}{p_i^{n_i}}$. If $n_i = 1$, we have a product of fields.

If $n_i > 1$, $\frac{F(x)}{(\cdot)^n}$ has nilpotent elements.

("nilpotent": $a^n = 0$ for some n.)

- Degree is Multiplicative - if $K \subset L \subset M$ are fields,

$[M:K] = [M:L][L:K]$

Proof: Pick basis $\alpha_1, \ldots, \alpha_m$ for L/K

$\beta_1, \ldots, \beta_n$ for M/L

check that pairwise products $\alpha_i \beta_j$ form a basis for $[M:K]$ M/K.

If E/F is an extension, the set of algebraic elements form a "field".

(Ex: elements of $\mathbb{C}$ over $\mathbb{Q}$ form a "field of algebraic numbers")

If α, β algebraic, so are $\alpha+\beta$, $\alpha\beta$, $-\alpha$, $\frac{1}{\alpha}$.

trivial

An (Finite) algebraic extension of an (Finite) algebraic extension is algebraic.

$\underbrace{K \subset L}_{\text{alg}} \underbrace{\subset M}_{\text{alg}}$ Suppose $a \in M$ so a is root of $f \in L[x]$

finite # of coefficients

So we can find finite extension L_0 of K containing F $\Rightarrow$ $\underbrace{K \subset L_0}_{\text{finite}} \subset \underbrace{L_0(a)}_{\text{finite}}$ so a is algebraic

If α, β alg. over K

$$\underbrace{K \subset K(\alpha)}_{\text{finite}} \underbrace{\subset K(\alpha,\beta)}_{\text{Finite, degree} \leq [K(\beta):K]}$$

So α, β contained in finite extension s.t. $\alpha+\beta$, $\alpha\beta$ are algebraic.

Ex: $\sqrt[2]{2} + \sqrt[3]{2} + \sqrt[3]{5} = a$. Find Polynomial with $f(a) = 0$.

($\sqrt[2]{2}$: x^2-2; $\sqrt[3]{2}$: x^3-2; $\sqrt[3]{5}$: x^5-2)

The polynomial has degree 30, it's a hard problem.

Similarly, suppose a is a root of $x^n + b_{n-1}x^{n-1} + \cdots + b_0$, with b_0 algebraic $\Rightarrow$ a is algebraic.

Proof: Take finite extension

$$K \subseteq \underbrace{K[b_0, \ldots, b_{n-1}]}_{\deg \leq \deg b_0 \cdot \deg b_1 \cdots \deg b_{n-1}} \subseteq \overbrace{K[b_0, \ldots, b_{n-1}][a]}^{\deg \leq n}$$

So a is in a finite extension $\Rightarrow$ it is algebraic.

Example: $e+\pi$ or $e\pi$ is transcendental.

If they are both algebraic, then e is algebraic $\lightning$ (e is a root of $x^2 - (e+\pi)x + e\pi$)

Splitting Fields: Suppose F is a field, $f \in F[x]$.

The splitting field is a field E/F such that

(1) f splits into linear factors $(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$, $\alpha_i \in E$

(2) E is generated by roots α_i.

Ex: • $F = \mathbb{R}$, $f = x^2+1 \Rightarrow E = \mathbb{C}$ $(x^2+1 = (x+i)(x-i))$

• $F = \mathbb{Q}$, $f = x^4+x^3+x^2+x+1$ Roots: $\{e^{2\pi i n/5} : n = 1,2,3,4\}$

$E = \mathbb{Q}[e^{\pm 2\pi i/5}]$

• $F = \mathbb{Q}$, $f = x^3 - 2$

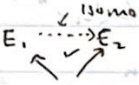
Consider $\mathbb{Q}[\sqrt[3]{2}]$ containing one of roots. It obviously has $\sqrt[3]{2}$, but not $\sqrt[3]{2}\,w$ $\sqrt[3]{2}\,w^2$ (where $w = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$), since those are complex.

$\mathbb{Q}[\sqrt[3]{2},\ \sqrt[3]{2}\,w]$ is the splitting field.

$\mathbb{Q} \subseteq \mathbb{Q}[\sqrt[3]{2}] \subseteq \mathbb{Q}[\sqrt[3]{2},\ \sqrt[3]{2}\,w]$ so overall degree 6.

(deg 3; deg 2)

Theorem: Splitting fields exist, and are "unique"

if 

are splitting fields, there is an isomorphism from $E_1 \to E_2$, making diagram commute.

Remark: the isomorphism isn't always unique.

Proof (Induction on degree of f): Pick irreducible factor of f, $f(x) = p(x)\,g(x)$.

Then force p to have a root: $F \subseteq \frac{F(x)}{p(x)}$, so p has a root α.

so it factors as (linear)(poly deg n-1)

s.o

$$F \subseteq \frac{F(x)}{p(x)} \subseteq \text{Split field of degree } n-1 \text{ poly}$$

Degree is $\leq n!$

Part 2: Suppose E_1, E_2 are splitting fields of f. Pick irreducible factor p.

Pick root α of p in E_1, β of p in E_2. "choices are not unique, so no canonical isomorphism"

map $F(\alpha) \longmapsto F(\beta)$ by mapping $\alpha \longmapsto \beta$

since $\frac{F[x]}{p(x)} \longrightarrow \frac{F[x]}{p(x)}$ and repeat.

Similarly, we can form splitting fields of any set of polynomials, $\{f_1, f_2, \dots\}$. (If the set is uncountable, need Axiom of Choice).

Application: Splitting field of all Polynomials, $\bar{F}$, "Algebraic Closure" (unique up to isomorphism)

$$F \leq \bar{F}$$

- Every polynomial in $F[x]$ splits in $\bar{F}$.
- Every polynomial in $\bar{F}[x]$ splits in $\bar{F}$.
  - ↳ called algebraically closed.

$F \leq \bar{F} \leq \bar{F}(\alpha)$ ← root of some polynomial in $\bar{F}$. But then, α is algebraic over F, so α is root of poly. in $F[x]$, so $\alpha \in \bar{F}$ as poly. splits in $\bar{F}$.

Finite Fields [Fields with finite # of elements]:

- "Characteristic": Smallest integer $p > 0$ with $p = 0$ in Field
  - p must be prime, so ~~$F \subset \mathbb{Z}$~~ field contains $F_p = \mathbb{Z}/p\mathbb{Z}$, so F is a vector space over F_p, of dim $n > 0$, so number of elements is p^n (p prime, $n > 0$).

Theorem: (1) Fields of order p^n exist.
(2) Any 2 of same order are isomorphic.

Theorem: F is a field of order p^n $\Leftrightarrow$ F is ~~polynomial~~ splitting field of $x^{p^n} - x$.
"This completes the proof since splitting field exist and are unique"

Proof: $\Rightarrow$: If F has order p^n, Multiplicative group F^* is cyclic of order $p^n - 1$, so all elements satisfy $x^{p^n-1} = 1$ (Lagrange).
0 is a root of $x = 0$, so all elements are roots of $x^{p^n} - x = 0$.
The roots are distinct since derivative -1 (coprime to derivative).
All p^n elements are roots of $x^{p^n} - x = 0$, so F is a splitting field.

$\Leftarrow$: Suppose E is a splitting field of $x^{p^n} - x = 0$.

Look at ~~Frobenious~~ Frobenius Automorphism $\Phi(a) = a^p$.

$\Phi(a+b) = \Phi(a) + \Phi(b) \Rightarrow (a+b)^p = a^p + b^p$

$\Phi(ab) = \Phi(a)\,\Phi(b)$

The elements fixed by Φ^n form a field.

$\Phi^n(a) = a \iff a^{p^n} = a$, so p^n roots of $x^{p^n} - x = 0$ form a field.

"There are p^{n-1} since all roots are distinct because derivative $= 1$, so must be E as E is generated by roots."

Construct Field of order p^n : Take irreducible polynomial $f(x) \in F_p[x]$.

$\frac{F_{p^n}[x]}{(f)}$ $\frac{F_p[x]}{(f)}$ is a field of order p^n, containing the roots of any irred. polynomial of degree n (by uniqueness)

So we can factor $x^{p^n} - x$.

- $x^{16} - x$ over $F_2[x]$

Product of all irreducible polynomials of degree dividing 4.

$x^{16} - x = (x^4+x^3+1)(x^4+x^3+x^2+x+1)(x^4+x+1)(x^2+x+1)(x+1)\,x$

So pick irreducible polynomial of degree 4.

$\frac{F_2[x]}{(x^4+x^3+1)}$, but you could choose $\frac{F_2[x]}{(x^4+x^3+x^2+x+1)}$; however, they are isomorphic. ($\xleftrightarrow{\text{isomorphism}}$, ✓?)

But they could pick $\frac{F_2[x]}{(x^4+x+1)}$ ($\xleftrightarrow{\text{isomorphism}}$) are these compatible?

Problem: Find the "best" description of the finite field of order p^n!

(Schelling Points)

$[K_{f(f)} : K] = [K_{f(f)} : K_{f(g)}]\,[K_{f(g)} : K]$

Ex: (# of irreducible polynomials) # of irreducible deg 6. over F_2?

A: $x^{2^6} - x$ = product of (irreducible of deg 6) × (deg 3) × (deg 2) × (deg 1)

$$2^6 = 6n_6 + 3n_3 + 2n_2 + n_1 \longrightarrow n_6 = 9$$

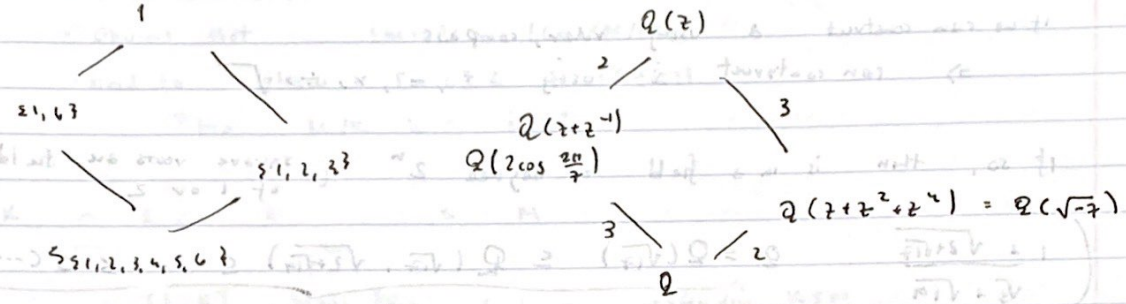
$$2^3 = 3n_3 + n_1 \longrightarrow n_3 = 2$$

$$2^2 = 2n_2 + n_1 \longrightarrow n_2 = 1$$

$$2 = n_1 \longrightarrow n_1 = 2$$

11/14/19: Continued: Subfields of $\mathbb{Q}(\zeta)$, $\zeta^7 = 1$

Gal ois Group $= (\mathbb{Z}/7\mathbb{Z})^\times$



$x = \zeta + \zeta^{-1}$ Degree 3

x^0 1

x^1 $\zeta^{-1} + \zeta$

x^2 $\zeta^{-2} + 2 + \zeta^2$

x^3 $\zeta^{-3} + 3\zeta^{-1} + 3\zeta + \zeta^3$

$x^3 + x^2 - 2x - 1 = (\zeta^{-3} + \dots) = 0$

irreducible polynomial, $2\cos\frac{2\pi}{7}$, $2\cos\frac{4\pi}{7}$, $2\cos\frac{6\pi}{7}$.

"Gauss Sum"

$y = \zeta + \zeta^2 + \zeta^4$ $y' = \zeta^3 + \zeta^5 + \zeta^6$ under $\zeta \to \zeta^{-1}$

$y + y' = \zeta + \zeta^2 + \dots + \zeta^6 = -1$

$y \cdot y' = \zeta^4 + \zeta^6 + 1 + \zeta^5 + \zeta = 2$ "Just Bash this"

$\Rightarrow y^2 + y + 2 = 0$ $\Rightarrow y = \frac{-1 \pm \sqrt{-7}}{2}$

Application: cannot construct 7-gon w/ ruler, compass
$\Leftrightarrow$ constructing $\cos\frac{2\pi}{7}$ w/ ruler and compass

If we can construct a using ruler, compass
$\Rightarrow$ can construct a using $+, -, \times, \div, \sqrt{}$

If so, then a is in a field of degree 2^n (square roots are field extensions of 1 or 2)

$\left(\frac{1+\sqrt{2+\sqrt{17}}}{\sqrt{5}+\sqrt{19}} \quad \mathbb{Q} \subseteq \mathbb{Q}(\sqrt{17}) \subseteq \mathbb{Q}(\sqrt{17}, \sqrt{2+\sqrt{19}}) \subseteq \cdots \subseteq \mathbb{Q}(\cdots\sqrt{5})\right)$

degree 16

$\Rightarrow$ If irreducible poly has degree 2^m for $m \geq n$.
But Polynomial has degree 3.

Main Theorem: M/K with $\mathrm{Gal}(L,K) = G$

$M^H \leftarrow H$

Consider $K \subseteq L \subseteq M$, Subgroups $H \leq G$

Claim:
These two maps are inverses.

$L \mapsto \mathrm{Gal}(M/L) = H$
elements of G fixing all elements of L.

L
$\cap$ is clear
M^H

$\mathrm{Gal}(M/L) = H$

$L = M^H$

H
$\cap$ is clear
$\mathrm{Gal}(M/L)$

Want to show $L = M^H$, $H = \mathrm{Gal}(M/L)$.

It suffices to show they are the same "size"

- $|H| = |\mathrm{Gal}(M/K)|$
- $[M : M^H] = [M : H]$

$\Leftarrow$ (1) M^H has same size as H ($|H|$)
(2) $\mathrm{Gal}(M/L)$ has same size as $([M:L])$

(1) $[M : M^H] = |H|$, we did this in characterization of Galois extensions

(2) Given L, $[M:L] = |\mathrm{Gal}(M/L)|$

- Obvious that $[M:L] \geq |\mathrm{Gal}(M/L)|$
- Need to show $[M:L] \leq |\mathrm{Gal}(M/L)|$

"use M/K is Galois"

$K \leq L \leq M$

$\leq [L:K]$ maps from L to M extending $K \subset M$

$\leq \mathrm{Gal}(M/L)$ ways to extend each to these to map $M \to M$

As M/K is Galois, there are $[M:K] = [M:L][L:K]$ ways to map $M \to M$

This implies $|\mathrm{Gal}[M/L]| \geq [M:L]$. ■

Gauss's construction of 17-sided Polygon:

Look at $\mathbb{Q}(z)$ where $z^{17} = 1$, $z = e^{2\pi i/17}$

The irreducible polynomial is $1 + z + \cdots + z^{16}$, roots $z, z^2, \ldots, z^{16}$

Gal Group is $(\mathbb{Z}/17\mathbb{Z})^* = \mathbb{Z}/16\mathbb{Z}$

1 3 9 10 13 5 15 11 16 14 8 7 4 12 2 6

Subgroups of $(\mathbb{Z}/17\mathbb{Z})^*$

1: $\{1\}$

2: $\{1, 16\}$

4: $\{1, 13, 16, 4\}$

8: $\{1, 9, 13, 15, 16, 8, 4, 2\}$

16: $\{1, 3, 9, \ldots, 2, 6\}$

Problem: Write z with $+ - \times \div \sqrt{\ }$

$\mathbb{Q}(z)$

$\cup 1$

$\mathbb{Q}(z + z^{-1})$

$\cup 1$

$\mathbb{Q}(z + z^{13} + z^{16} + z^4)$

$\cup 1$

$\mathbb{Q}(z + z^9 + \ldots)$

$\cup 1$

$\mathbb{Q}(z + z^3 + \ldots) = \mathbb{Q}$

Each field has index 2 in next.

Problem: find explicit degree 2 poly satisfied by

Galois conjugates $\begin{cases} \alpha = z + z^9 + z^{13} + \cdots & (8 \text{ terms}) \\ \beta = z^3 + z^{10} + \cdots & (8 \text{ terms not in } \alpha) \end{cases}$

rational $\begin{cases} \alpha + \beta = -1 \\ \alpha\beta = \underbrace{\textstyle\sum 64 \text{ terms}}_{\text{rational}} \end{cases}$ z^i with $i \neq 0$

$= \text{constant}\,(z^1 + \cdots + z^{16})$ "Wow"

$\Rightarrow 4(-1) = -4$

α, β are roots of $z^2 + z - 4 = 0$.

$= \frac{-1 \pm \sqrt{17}}{2}$.

Next case: $\gamma = z + z^{13} + z^{16} + z^4$ $\quad \delta =$ conjugate : $z^9 + z^{15} + z^8 + z^2$

$\gamma + \delta$, $\gamma\delta$ should be in $\mathbb{Q}(z + z^9 + z^{13} + \dots) = \mathbb{Q}(\alpha)$

$\gamma + \delta = z + z^9 + \dots = \alpha$

$\gamma\delta = -1$ (obvious tedious)

γ, δ roots of

$x^2 - \alpha x - 1 = 0$.

$\gamma, \delta = \frac{\alpha \pm \sqrt{\alpha^2 - 4}}{2}$

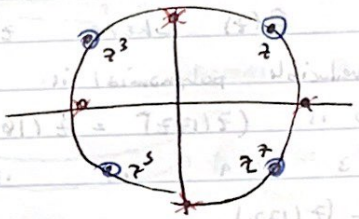
"Same procedure for any Fermat prime $p = 2^{2^n} + 1$"

$z^0 + 1$
$z^1 + 1$ } cheeks
$z^2 + 1$
$z^4 + 1$
$z^8 + 1$
$z^{16} + 1$ — Kernels

$x^4 + 1$, $x^4 + 2$, $x^4 + 4$

$x^8 - 1 = (x^4 + 1)(x^4 - 1)$

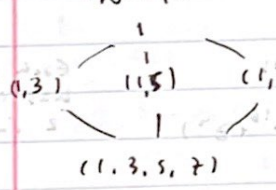
$x^4 + 1$: $\sim 8^{th}$ roots of unity



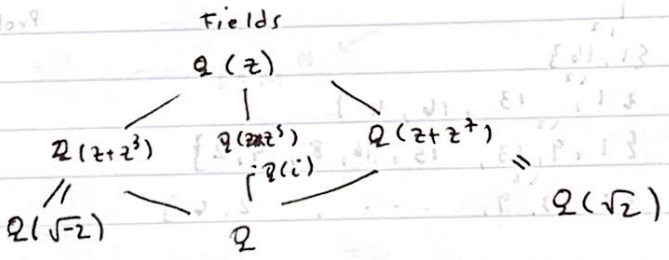
Galois Group $(\mathbb{Z}/8\mathbb{Z})^* = \{1, 3, 5, 7\}$

noncyclic $\quad 3^2 = 5^2 = 7^2 = 1$

Subgroups



Fields



$x^4 + 4$: $\sqrt{2} \cdot 8^{th}$ roots of unity

$= (z^2 + 2z + 2)(z^2 - 2z + 2)$ $\quad = \pm 1 \pm i$

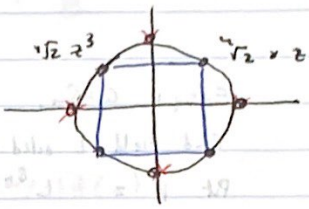
Splitting field is $\mathbb{Q}[i]$ degree 2.

x^4+2 : Splitting field , Roots : $\sqrt[4]{2}$, primitive 8th root of 1

Field generated by $(\sqrt[4]{-2}, i)$

$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{-2}) \subseteq \mathbb{Q}(\sqrt[4]{-2}, i)$

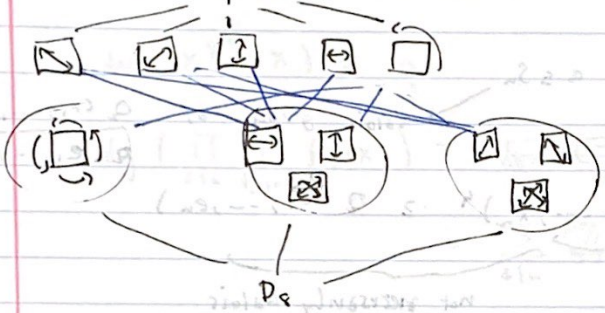
4 2 SF has degree 8.

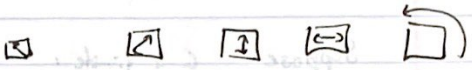


Sum of diagonal pair is 0.

Galois Group = D_8 = symmetries of square

Subgroups of D_8





Fields

$\mathbb{Q}(\sqrt[4]{-2}, i)$

$\mathbb{Q}(\sqrt[4]{-2}), \mathbb{Q}(\sqrt[4]{-2}\,i), \mathbb{Q}(i, \sqrt{2})$

$\mathbb{Q}((1+i)\sqrt[4]{-2}), \mathbb{Q}((1-i)\sqrt[4]{-2})$

$\mathbb{Q}(i)$ $\mathbb{Q}(\sqrt{2})$ $\mathbb{Q}(\sqrt{-2})$

$\mathbb{Q}$

Subgroups of G $\Leftrightarrow$ Subextensions $K \subseteq L \subseteq M$ (G/H, H)

H is normal $\Leftrightarrow$ Extension $K \subseteq L$ Normal

$\mathrm{Gal}(L/K) = G/H$

$\mathrm{Gal}(M/L) = H$ (even if H not normal)

Subgroups conjugate under G $\Rightarrow$ Subfields conjugate under G.

Inverse Problem: Given G (finite) find extension $K \subseteq L$ with Galois group G.

Easy: $G = S_n$.

Find field L acted on by S_n — just find this.

Put $K = L^{S_n}$ $\quad \mathbb{Q}(x_1, \dots, x_n)$ rational functions in n-vars

Fixed Fields $= \mathbb{Q}(e_1, \dots, e_n)$ e_i is elementary symmetry functions.

Suppose G is finite: Embed $G \subseteq S_n$ → Galois group of $\frac{\mathbb{Q}(x_1, \dots, x_n)}{\mathbb{Q}(e_1, \dots, e_n)}$

Look at fixed field under G:

$$\mathbb{Q}(x_1, \dots, x_n) \supseteq \mathbb{Q}(x_1, \dots, x_n)^G \supseteq \mathbb{Q}(e_1, \dots, e_n)$$

Galois group G — not necessarily Galois

Much harder Problem: Given G (finite) find Galois Extension $K/\mathbb{Q}$ ⇑ fix base field.
with Galois Group G.

Examples: $G = \mathbb{Z}/5\mathbb{Z}$. Find Gal. extension w/ quotient G. of group B

$\mathbb{Q} \subseteq L \subseteq M$ — M fixed field of B. $G = H/B$

A

$A = \mathbb{Z}/10\mathbb{Z}$: $\mathbb{Q}(e^{2\pi i/11})$

↓

$\mathbb{Z}/5\mathbb{Z}$ by $B = \{1, 10\} \in (\mathbb{Z}/11\mathbb{Z})^*$

Take $L = \mathbb{Q}(e^{2\pi i/11})$ fixed field under $z \mapsto z^{-1}$

$\mathrm{Gal}(L/\mathbb{Q}) = \frac{\mathbb{Z}/10\mathbb{Z}}{\mathbb{Z}/2\mathbb{Z}} = \mathbb{Z}/5\mathbb{Z}$

$L = \mathbb{Q}(z + z^{-1}) = \mathbb{Q}(2\cos\frac{2\pi}{11})$.

11/19/19

1. $\Delta = -4b^3 - 27c^2$ $= +4 - 27 = -23$ so S_3

Applications of Galois Theory, Cyclic Extensions

Q: Given G find extension L/k with $Gal(L/k) = G$.

A: $L = k(x_1, \dots, x_n)$, $K = L^G$ where $G = S_n$.

Can we take $k = \mathbb{R}$? Example $G = \mathbb{Z}/5\mathbb{Z}$.

Example: $G \cong S_5$ (order 120) Find $L/\mathbb{Q}$ with Galois group S_5

$x^5 - 4x + 2$

Properties: (1) Irreducible, Eisenstein

(2) Exactly 2 nonreal roots, calculus

Note: 1) Gal group is a subgroup of S_5 (perms of roots)

2) $|G|$ divisible by 5 since $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$ (α = root) (follows from irreducible)

3) G contains a 5 cycle

4) G contains TRANSPOSITION (swaps 2 roots) (conjugation)

Implies $G = S_5$:

Take roots $(\alpha, \beta, \gamma, \delta, \varepsilon)$

G contains $(\alpha\beta)$ "Transposition"

Some power of 5 cycle takes α to β

assume G contains $(\alpha\beta)$ & $(\alpha\ \beta\ \gamma\ \delta\ \varepsilon)$ "might need renumbering"

From multiplying $(\alpha\beta)$ by $(\alpha\ \beta\ \gamma\ \delta\ \varepsilon)$

$(\alpha\beta)$, $(\beta\gamma)$, $(\gamma\delta)$, $(\delta\varepsilon)$, $(\varepsilon\alpha)$.

This generates S_5 by bubble sort.

Same works for any prime p "Exertion $L/\mathbb{Q}$ w/ $Gal(L/\mathbb{Q}) \cong S_p$.

So can find L/k for any Galois group for L/k being finite extensions of $\mathbb{Q}$

$Gal(L/\mathbb{Q}) \cong S_p$, $G \leq S_p$, $K = L^G$.

"Subfield Diagram $\leftrightarrow$ Gal. correspondence"

Degree 3 Polynomials $f(x)$, irreducible:

(1) Gal. $\leq S_3$ (permutations)

(2) order divisible by 3. Splitting field contains $k(\alpha)$ (α root) $[k(\alpha) : k] = 3$

2 possibilities: (1) $G \cong S_3$ ex. $x^3 - 2$ over $\mathbb{Q}$

(2) $G \cong A_3 = \mathbb{Z}/3\mathbb{Z}$. ex. $x^3 + x + 1$ over $\mathbb{Z}/2\mathbb{Z}$

~~Examples:~~

Suppose roots α, β, γ.

Look at $(\alpha-\beta)(\beta-\gamma)(\gamma-\alpha) = \Delta$.

Δ is fixed by A_3.

Δ changes sign under odd permutations. (assume char $\neq 2$)

So if $Gal = A_3$, Δ is in base field, since fixed by Galois group

$\rightarrow \Delta^2$ is a square:

Suppose Polynomial is $f(x) = x^3 + bx + c$ char $\neq 2, \neq 3$

$\Delta^2 = -4b^3 - 27c^2$

is a square, then Galois group is A_3

otherwise S_3

Examples: $x^3 - 3x - 1$ $-4b^3 - 27c^2 = 81$ A^3

$x^3 - 3x + 1$ $-4b^3 - 27c^2 = 135$ S^3

Ex: $\mathbb{C}$ is algebraically closed.

Need 2 Facts: (1) Any poly. of odd degree over $\mathbb{R}$ has a root. "Intermediate value theorem"

(2) Any degree 2 polynomial over $\mathbb{C}$ has a root

($\mathbb{C}$ has $\sqrt{\text{elements}}$)

Pick finite Galois extension L of $\mathbb{R}$ containing $\mathbb{C}$ ($\mathbb{R} \leq \mathbb{C} \leq L$)

Want to show $L = \mathbb{C}$.

Look at $Gal(L/\mathbb{R})$.

(1) G has ~~order~~ no subgroups of odd index other than G { If had H, L^H is extension of odd degree, so $\neq \mathbb{R}$ by (1) }

(2) Sylow 2-subgroup has odd index so is equal to G, so G has order 2^n.

So $|Gal(L/\mathbb{C})| = 2^{n-1}$.

But any subgroup of order $2^{n-1} > 1$ has subgroup of index 2.

"nilpotent groups"

Then $L^H/\mathbb{C}$ has degree 2, but $\mathbb{C}$ has $\sqrt{\ }$

so $|Gal(L/\mathbb{C})| = 1 \Rightarrow \mathbb{C}$ is algebraically closed.

Ex:

Q. Suppose L/K is a finite extension. $L = K(\alpha_1, \ldots, \alpha_n)$.

Is L of form $K(\alpha)$ for some $\alpha \in L$?

A. Sometimes.

$K = \text{char } p^2 > 0$

$L = K(t, u)$ Rational functions in 2 vars

$k = K(t^p, u^p)$ $L = K(t,u)$ $t^p \in k$, $u^p \in k$.

$[L:K] = p^2$.

Is $L = K(\alpha)$? No. If $\alpha \in L$, $\alpha^p \in K$ since for generators u, t

and $(x+y)^p = x^p + y^p$, $(xy)^p = x^p y^p$

So every element α is root of $x^p - a = 0$.

So $K(\alpha)/K = 1$, p or $\leq p$ so $K(\alpha) \neq L$.

so K cannot be generated by 1 element.

always true in char 0.

If L/K is separable and finite, then $L = K(\alpha)$ for some α.

Case 1: K is finite field. L^* is cyclic, so generated by 1 element

Case 2: K infinite.

(2) any finite number of extensions $K \leq J \leq L$ between K and L.

Gal Theory: corresponds to subgroups of $G = Gal(M/K)$. ← splitting field M.

Lemma: Suppose K is infinite, L a vector space, $L \neq 0$

L is not union of finite number of proper subspaces.

Proof: Suppose $L_1, \ldots, L_n$ are proper subspaces. Pick $x \neq 0 \in L$.

~~Pick~~ x not in $L_2, \ldots, L_n$ by induction.

Pick $y \notin L_1$. look at $x + \lambda y$. at most 1 value of λ

which this is in some L_i, so since K is finite can find λ such

that $x + \lambda y$ is not in L_i.

Then, we can pick α, not in any proper subextension so $L = K(\alpha)$.

Problem: Given $G = Gal(L/K)$, describe L in terms of K.

Easy case: G is cyclic, prime order, $\mathbb{Z}/p\mathbb{Z}$.

$p = 2$. L/K degree 2. root α satisfying $x^2 + bx + c = 0$

$$(x + b/2)^2 + \left(c - \frac{b^2}{4}\right) = 0$$

so $L = K\left(\sqrt{\frac{b^2}{4} - c}\right)$? ⇑ Fails in char 2.

Suppose $[L:K] = 2$.

$x^2 - a$ is α root $\Rightarrow$ so is $-\alpha$

char $\neq 2$: $L = K[\sqrt{a}]$ for $a \in K$

char $= 2$: $x^2 + bx + c = 0$ — if $b = 0$, then $x^2 + c = 0$

$\rightarrow$ so $L = K[\sqrt{c}]$.

But this isn't a galois extension, because its not separable.

"$\sqrt{}$ in char 2 is bad"

separable since derivative $= -1$

$b \neq 0$. $y = x/b$, $y^2 + y + d = 0$

"Artin - Schreier Equation"

if α is a root, so is $\alpha + 1$.

Other primes: Suppose char $\neq p$ $\quad [L:K] = p$

Find a nice element of L.

Idea: $x^3 + ax^2 + bx + c = 0$

$\Rightarrow$ $x^3 + bx + c = 0$ "complete cube"

$\approx$ "hard to get rid of"

Key Idea: **Eigenvectors**. If G generated by σ with $\sigma^p = 1$.

L is vector space over K acted on by σ (Linear Transformation)

look for eigenvectors of σ acting on L.

Eigenvalues? $\sigma^p = 1$ so eigenvalues are $1, \#, \#^2, \ldots, \#^{p-1}$

Assume p^{th} roots are in K. $\quad \therefore$ p^{th} root of 1

If not, see CLASS FIELD THEORY.

Every element of L is sum of eigenvectors.

Explicit formula: Given a, $\frac{a + \sigma(a)}{2}$ is fixed by σ, so eigenvalue 1

$p \neq 2$.

$\frac{a - \sigma(a)}{2}$ eigenvalue -1.

$$a = \frac{a + \sigma(a)}{2} + \frac{a - \sigma(a)}{2}.$$

$p = 3$: $a = \frac{a + \sigma(a) + \sigma^2(a)}{3}^{1} + \frac{a + \omega\sigma(a) + \omega^2\sigma(a)}{3}\omega^{-1}$

$$+ \frac{a + \omega^2\sigma(a) + \omega\sigma^2(a)}{3}\omega^{-2}$$

Same for $p > 3$.

Pick any eigenvector α with $\zeta^p = 1$ eigenvalue ζ.

simple $\Rightarrow$ $\sigma(\alpha) = \zeta\alpha$

$\sigma^{\#}(\alpha^p) = \zeta^p\alpha = \alpha$ so $\sigma^{\#}(\alpha^p) \in K$

α is root of $x^p - a = 0$ (over K) so L is generated by p^{th} root of elemt of K.

Char $K = p$? Previous argument fails.

(1) cannot divide by p

(2) No complex roots of unity. (only $x = 1$)

(3) $X^p - a$ is inseparable, so doesn't give galois extensions.

σ acts on vector space L.

Look for eigenvectors: only eigenvalue is 1 ✓ only eigenvectors.

only eigenspace is things fixed by $\sigma = K$.

Generalized Eigenvectors: Eigenvector $(\sigma - \lambda)v = 0$

"Generalized" $(\sigma - \lambda)^n v = 0$.

$\sigma = \begin{pmatrix} \lambda & 1 & 0 & 0 \\ 0 & \lambda & 1 & 0 \\ 0 & 0 & \lambda & 1 \\ 0 & 0 & 0 & \lambda \end{pmatrix}$ Jordan

$\sigma - \lambda = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} = N$ nilpotent

Put $N = \sigma - 1$, so $N^p = 0$. $\quad N v = 0 \iff v \in K$

Look for vectors with $N^2 v = 0$

(Put any v with $N^k v = 0$ $\quad N^2(N^{k-2} v) = 0$ $\quad N^{k-1} v \neq v$)

This means $\sigma v - v$ is fixed by σ

so is in K.

$\sigma v = v + a \quad (a \in K)$

Divide v by a, $w = \frac{v}{a}$, $\boxed{\sigma w = w + 1}$ (easy formula)

(analog of $\sigma(\alpha) = \zeta \alpha$)

$\sigma(w^p) = (w+1)^p = w^p + 1$

so $\sigma(w^p - w) = w^p - w$ — either irreducible or splits into linear factors. So $w^p - w \in K$ for $a \in K$

w is root of $x^p - x - a = 0$

"Artin-Schreier" (analog of $x^p - a = 0$)

v is root, so is $\alpha + 1$. $\quad$ if α is root, so is $\zeta \alpha$.

Action of Gal group $\mathbb{Z}/p\mathbb{Z}$ on α

Application: When can polynomial $f(x) = 0$ be "solved by radicals"?

Roots written using $+ \; - \; \times \; / \; \sqrt[n]{}$

Quadratic $\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$

Answer: If Gal group of splitting field is solvable, then roots can be written using radicals, artin-schreier extensions for char > 0.

Proof: If L is splitting field, G is Gal. group. G is solvable,

$G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_n$

(normal; $\frac{G_{i+1}}{G_i}$ cyclic of prime order.)

(Assume K has roots of unity)

$L_0 \supseteq L_1 \supseteq L_2 \supseteq \cdots \supseteq L_n = K$

factors of extension is Gal, with Gal group $\mathbb{Z}/p\mathbb{Z}$. so $L_{i+1} = L_i(\alpha)$ where α root of $x^p - x - a = 0$

So day $f \leq 4$, can be solved (Artin Schreier)

Galois groups $\leq S_3, S_4$ solvable.

$1 \leq \mathbb{Z}_2 \times \mathbb{Z}_2 \leq A_4 \leq S_4$

9/21/19: Recall: L/K finite Galois, w/ $Gal(L/K) = G$, if G is solvable, we can write elements of L using $+ - \times / \sqrt[n]{}$, AS-extensions.

Converse: if L/K finite and elements can be written as above, then $Gal(L/K)$ is solvable.

Idea: look at $K \subseteq K[$ roots of unity $]$

$K_0 \subseteq K_1 \subseteq K_2 = K_1[\sqrt[m]{z}] \subseteq K_3 = K_2[\sqrt[n]{t}] \subseteq \cdots$

$K_0 \subseteq K_1$: abelian

$K_2 = K_1[\sqrt[m]{z}] \subseteq K_3$: cyclic; $Gal \subseteq \mathbb{Z}/n\mathbb{Z}$

$\sqrt[m]{z} \longrightarrow \sqrt[m]{z}$ (root of unity)

$G \trianglerighteq G_0 \trianglerighteq G_1 \trianglerighteq G_2 \cdots$ so: G_0 is solvable.

$G \trianglerighteq G_0$: abelian; $G_1 \trianglerighteq G_2$: cyclic

Example: $x^5 - 4x + 2$ has Galois group S_5: Not solvable

cannot be solved by radicals

(Although, some can be solved: $x^5 - 2$, Gal group $\subseteq S_5$ ↙ Solvable, order 20

$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[5]{\ }) \subseteq \mathbb{Q}(\sqrt[5]{1}, \sqrt[5]{2})$

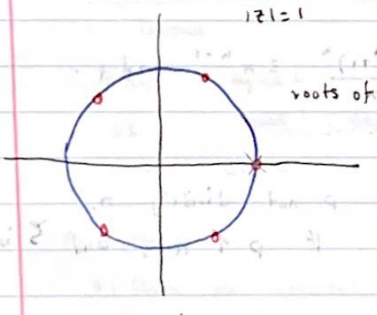
order 4; order 5

Recall Problem: Find irreducible polynomial of degree n over $\mathbb{F}_p$.

Easy to find, but not a canonical choice.

Solution (if $n = p$): $x^p - x - 1 = 0$

Cyclotomic Fields: Generated by Roots of Unity.

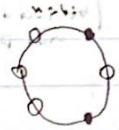


Cyclotomic Field over $\mathbb{Q}$ is the splitting field of $x^n - 1$. Some small cases:

		Deg
$n=1$:	$x - 1 \Rightarrow$ SF: $\mathbb{Q}$	1
$n=2$:	$x^2 - 1 = (x-1)(x+1) \Rightarrow$ SF: $\mathbb{Q}$	1
$n=3$:	$x^3 - 1 = (x-1)(x^2+x+1) \Rightarrow$ SF: $\mathbb{Q}\left(\frac{-1+\sqrt{-3}}{2}\right)$	2
$n=4$:	$x^4 - 1 = (x^2+1)(x+1)(x-1) \Rightarrow$ SF: $\mathbb{Q}(i)$	2
$n=5$:	$x^5 - 1 = (x-1)(x^4+x^3+x^2+x+1)$	4

$n=6$: $x^6 - 1 = (x-1)(x+1)(x^2+x+1)(x^2-x+1)$ — same field as $n=3$

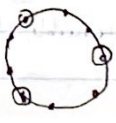
1st root; 2nd root; cube roots; 6th roots (Primitive)



$n=7$: $x^7 - 1$ similar to 5 — 6

$n=8$:

$n=9$:



$(x-1)(x^2+x+1)$
(x^6+x^3+1)

$n = 10$ $(x-1)(x+1)(x^4+x^3+x^2+x+1)(x^4-x^3+x^2-x+1)$

12:

$x^{12}-1 = (x-1)(x+1)(x^2+x+1)(x^2+1)$
$(x^2-x+1)(x^4-x^2+1)$

$\Phi_n(x)$: Primitive n^{th} Roots of 1, cyclotomic Polynomial

$x^{12}-1 = \Phi_1(x)\,\Phi_2(x)\,\Phi_3(x)\,\Phi_4(x)\,\Phi_6(x)\,\Phi_{12}(x)$

$$x^n - 1 = \prod_{d \mid n} \Phi_d(x)$$

(*) Exercise: Find smallest n s.t. $\Phi_n(x)$ has a coefficient that is not $0, \pm 1$ (Wlog $n \geq 100$)

Möbius Inversion: If $F(n) = \sum_{d \mid n} g(d)$ then $g(n) = \sum_{d \mid n} f(d)\,\mu(n/d)$

μ: möbius function $\mu(p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}) = \begin{cases} 0 & \text{if some } n_i > 1 \\ (-1)^k & \text{all } n_i = 1 \end{cases}$

$$\Rightarrow \Phi_n(x) = \prod_{d \mid n} (x^d - 1)^{\mu(n/d)}$$

$\Phi_{15} = \dfrac{(x^{15}-1)(x-1)}{(x^3-1)(x^5-1)}$ removed 1 twice so add it back

$= x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$.

Thm: $\Phi_n(x)$ is IRREDUCIBLE over $\mathbb{Q}$.

(1) n = prime, eisenstein $\Phi_n(x) = \dfrac{x^n-1}{x-1}$

$\Phi_n(x+1) = \dfrac{(x^n+1)^n}{x} \equiv x^{n-1} \mod p$.

(2) n = prime power, similar proof

General case: Key Idea: reduce mod p for p not dividing n.

Lemma: Suppose f is irreducible and divides $x^n - 1$. If $p \nmid n$, and ζ is root of f, so is ζ^p.

Proof:

$\mathbb{Z}[\zeta] = \dfrac{\mathbb{Z}[x]}{f(x)}$ ~~reduce mod~~ Look at f in $\mathbb{F}_p[x]$ (need not be irreducible mod p)

Pick irreducible factor g of f.

Form field $F_p[\zeta] = \frac{F_p[x]}{g(x)}$. We have a map $\mathbb{Z}[\zeta] \to F_p[x]/g(x)$, $\zeta \mapsto x$

Notice all roots of x^n-1 have distinct images in $F_p(\zeta)$.

KEY POINT: Roots of x^n-1 are distinct mod p.

↪ derivative nx^{n-1} coprime to x^n-1 as $(n,p)=1$.

Roots of g are closed under $\underbrace{F(z)=z^p}_{\text{homomorphism of } F_p[\zeta]}$ $(a+b)^p = a^p+b^p \bmod p$, $(ab)^p = a^p b^p \bmod p$

We can identify roots of x^n-1 over $\mathbb{Z}$ w/ roots over F_p (injective) this shows ζ^p has image root of g, so is root of f in $\mathbb{Z}[x]$. □

Now look at $L/\mathbb{Q}$, L = splitting field of Φ_n. Let ζ be primitive n^{th} root of unity (others $1, \zeta, \zeta^2, \dots, \zeta^{n-1}$)

G = Galois group. Clear that $G \subseteq (\mathbb{Z}/n\mathbb{Z})^*$ since element of G takes ζ to ζ^k, $k \in (\mathbb{Z}/n\mathbb{Z})^*$

Problem: Show G is whole $(\mathbb{Z}/n\mathbb{Z})^*$

If p is coprime, G takes ζ to ζ^p (lemma)

So Gal group = $(\mathbb{Z}/n\mathbb{Z})^*$ which has order $\phi(n)$.

Deg $\Phi_n(x) = \phi(n)$ so n^{th} root generates extension equal to degree of Φ_n, so $\Phi_n(x)$ irreducible.

Gal. Theory

Easy	degree 2	$x^n - a$
OK	degree 3, degree 4	
Hard	degree >4	

Cyclotomic Fields are Easy though Finite Fields

Applications:

(1) There are infinitely many primes $\equiv 1 \pmod n$

(Dirichlet: ∞-many primes $\equiv a \bmod N$ if $(a,N)=1$)

Proof: Suppose $p \mid \Phi_n(a)$, $(n,p)=1 \Rightarrow$ roots of Φ_n are distinct mod p. So x^n-1 has n roots over $\mathbb{F}_p$.

So element a has order n mod p, so $n \mid \underbrace{(p-1)}_{|(\mathbb{Z}/p\mathbb{Z})^*|}$ by Lagrange

So $p \equiv 1 \pmod n$

So just pick $p \mid \Phi_n(a)$, a divisible by all known $\bmod p$ primes and by n.

Example: $n=4$ Pick $p \mid a^2+1$, a divisible by 4, all known primes $\equiv 1 \pmod 4$.

(2) Suppose G is finite, abelian. can find extention $K/\mathbb{Q}$ with Galois group G.

Proof: write G as a quotient of $(\mathbb{Z}/n\mathbb{Z})^*$ for primes n, k

Pick primes $p_1, \dots, p_k$, $p_i \equiv 1 \pmod n$

$(\mathbb{Z}/(p_1, \dots, p_k)\mathbb{Z})^* = \prod (\mathbb{Z}/p_i\mathbb{Z})^*$ which has $(\mathbb{Z}/n\mathbb{Z})^k$ as quotient

or for $\left(\left(\frac{\mathbb{Z}}{p_1 \cdots p_k \mathbb{Z}}\right)^* \longrightarrow G\right)$ so has G as quotient.

So take $K = \mathbb{Q}[\zeta]^H$ (ζ primitive n^{th} root of 1)

so $Gal(K/\mathbb{Q}) = G$.

Ex: (Kronecker, Weber, Hilbert) if $K/\mathbb{Q}$ is abelian extension of $\mathbb{Q}$, K is contained in some cyclotomic field. (Class field Theory)

Describe Abelian Extensions of ANF.

Shafarevich: If G is solvable, G is a Galois group of $L/\mathbb{Q}$

Suppose G is solvable, normal subgroup H, $1 \subsetneq H \subsetneq G$.

IDEA: (1) find extension $L/\mathbb{Q}$, Galois group: G/H.

(2) Extend to $M/\mathbb{Q}$ M Galois Group: G ($\mathbb{Q} \subseteq L \subseteq M$, G over $\mathbb{Q} \subseteq L$, H over $L \subseteq M$)

This fails: $G = \mathbb{Z}/4\mathbb{Z}$

$1 \subseteq \mathbb{Z}/2\mathbb{Z} \subseteq \mathbb{Z}/4\mathbb{Z}$

$L = \mathbb{Q}(\omega)$, $\omega^3 = 1$.

There is no extension $\mathbb{Q} \subseteq L \subseteq M$ with $[M:\mathbb{Q}] = 4$, $Gal(M/\mathbb{Q}) = \mathbb{Z}/4\mathbb{Z}$.

Point: look at $(\mathbb{Z}/n\mathbb{Z})^* \longrightarrow (\mathbb{Z}/3\mathbb{Z})^*$ ($\cong Gal(L/\mathbb{Q})$)

This map always splits as

$(\mathbb{Z}/n\mathbb{Z})^* = G \times H$

$G \cong \prod (\mathbb{Z}/p^i\mathbb{Z})^*$, $(\mathbb{Z}/p^i\mathbb{Z})^* \to 1$ in $\mathbb{Z}/3\mathbb{Z}$

$H \to (\mathbb{Z}/3\mathbb{Z})^*$

$(\mathbb{Z}/3^n\mathbb{Z})^* = (\mathbb{Z}/3\mathbb{Z})^* \times (\ )$

If M is abelian extension, $M \subseteq$ cyclotomic extension,

$Gal(M/\mathbb{Q}) =$ quotient of $(\mathbb{Z}/n\mathbb{Z})^*$

so $Gal(M/\mathbb{Q}) \hookrightarrow Gal(L/\mathbb{Q}) = (\mathbb{Z}/3\mathbb{Z})^*$ Always Splits!

but $1 \le 7127 \le 7147$ doesn't split.

Ex: $\mathbb{H}$ is a division algebra over $\mathbb{R}$.

Problem: Find finite division algebras: (WEDDERBURN) All finite division algebras are fields.

$\Leftarrow$ Brauer Group of Finite Field is Trivial

group whose elements are f.d. central simple division algebras.

Let L be a finite division algebra, K = center = finite field order q

L is vector space over K with dimension m.

WTS $m = 1$. Look at L^* — $q^m - 1$

Pick α in L s.t. things commuting with it form a vector space, so order $q^{k|m}$ for some k. So $\alpha \in L^*$, then subgroup of L^* commuting with it has order $q^k - 1$ for some k.

So number of conjugates of α is $\frac{q^m-1}{q^k-1}$, $k|m$.

$$L^\times = \text{center of } L^* \cup \text{conjugacy classes}$$

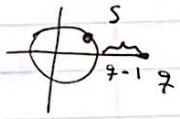
$$q^m - 1 \text{ elements} = q - 1 + \frac{q^m-1}{q^k-1}$$

divisible by $\Phi_m(q)$

so $q-1$ divisible by $\Phi_m(q)$.

$$\Phi_m(q) = \prod_{\substack{\text{primitive} \\ m^{th} \text{ roots of} \\ 1}} (q - \zeta)$$

if $q \neq 1$, $|q - \zeta| > q - 1$



so $|\Phi_m(q)| > |q - 1|$ if $m > 1$ so $m = 1$.

(Brauer Group) if A, B are central simple algebras, so is $A \otimes B$. (center is k)

so we get a product on set of central simple algebras.

We identify A with $M_n(A)$ for any n. For FD algebra A, $A \otimes A^{op} \cong M_n(k)$ so A^* becomes "A^{-1}" so we get a group.

(A^{op}: opposite algebra)

11/26/19 Norms and Traces

$\det = \sum_{\sigma \in S_n} \varepsilon(\sigma)\, a_{1,\sigma(1)} a_{2,\sigma(2)} \cdots$

Method: Exterior Powers:

Any vector space has ext. powers, $\Lambda^0(V) = k$, $\Lambda^1(V) = V$, $\Lambda^2(V)$, ..., $\Lambda^n(V)$ (Top EP, analog of volume)

Take tensor algebra of V, TV. Take basis $v_1, \ldots, v_n$

$T(V)$ = free alg. generated by $v_1, \ldots, v_n$

$T(V) = k \oplus V \oplus V \otimes V \oplus \cdots$ Basis $1, v_1, \ldots, v_n, v_i \otimes v_j, v_i \otimes v_j \otimes v_k, \ldots$

EXTERIOR ALGEBRA

Then $\frac{T(V)}{v_i \otimes v_j + v_j \otimes v_i} \hookrightarrow$ $v_i \otimes v_j = -v_j \otimes v_i$

$\in \Lambda(V)$: $1, v_1, \ldots, v_n$ (deg 1), $v_i \otimes v_j$ ($i < j$) (deg 2), $v_i \otimes v_j \otimes v_k$, $i < j < k$, ...

↑ Graded

$\Rightarrow \Lambda^0(V) \oplus \Lambda^0(V) \oplus \cdots \oplus \Lambda^i(V)$

Dim $= \binom{n}{i}$, $n = \dim(V)$.

$\dim(\Lambda^n(V)) = \binom{n}{n} = 1$. If $T \in \mathrm{Hom}(V, W)$ induces map $\Lambda(V) \to \Lambda(W)$

$T \in \mathrm{Hom}\, V \to V$ induces $\Lambda^n(V) \to \Lambda^n(V)$ (scalar)

The scalar ends up being the determinant.

Trace: Suppose T is linear transformation. How does $1 + \varepsilon T$ rescale volumes where ε is infinitesimal?

A: By a factor of $1 + \varepsilon T_r(T)$, $T_r(T) = \sum T_{ii}$

$\det(1 + \varepsilon T) = 1 + \varepsilon \sum T_{ii} + \varepsilon^2(\cdots)$

"Taylor approximation"

$Tr(AB) = Tr(BA)$

Example: "Heisenberg Commutation Relations" $AB - BA = I$ (position, momentum)

Find Solutions:

$\underbrace{Tr(AB - BA)}_{0} = \underbrace{Tr(I)}_{} = \dim(V)$

Only solution: V is 0-dim? Not True...

✓Tr defined

If $\dim(V) < \infty$ and $\text{char} = 0$, $V \neq 0$.

Take $V = k[x]$, $A = \frac{d}{dx}$, $B =$ multiplication by x in (char 0)

$V = \frac{k[x]}{(x^p)}$ $\quad \frac{d}{dx}(x^p) = p x^{p-1} = 0$

$\uparrow_{\dim p = 0}$

Norm & Trace of L/K, finite extension

Take $\alpha \in L$. Multiplication by α is a linear transformation from $L \to L$, think of L as a vector space over K.

Trace, det of α is called trace, and norm of α.

Properties: 1. $\text{Tr}(\alpha+\beta) = \text{Tr}(\alpha) + \text{Tr}(\beta)$ $\quad \text{Tr}: L \to K$ "homomorphisms of"

$N(\alpha\beta) = N(\alpha)N(\beta)$ $\quad N: L^* \to K^*$ groups

Tr, Sp

Ex: $\mathbb{C}/\mathbb{R}$, $\alpha = x + iy$, Basis for $\mathbb{C}$: $1, i$

Matrix of α: $\begin{pmatrix} x & y \\ -y & x \end{pmatrix}$ so Trace: $x+x = 2\text{Re}(\alpha)$

det: $x^2+y^2 = |\alpha|^2$

Suppose $\alpha \in L$, what is $\text{Tr}, N(\alpha)$?

Suppose $L = K(\alpha)$, α is root of $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$.

Basis for L/K: $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$

Matrix of α:
$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 & \cdots \\ 0 & 0 & 1 & 0 & 0 & 0 \\ & & & \vdots & & \\ 0 & 0 & \cdots & \cdots & 0 & 1 \\ -a_0 & \cdots & \cdots & \cdots & -a_{n-1} & \end{pmatrix}$$

$\alpha(1) = \alpha$

$\alpha(\alpha) = \alpha^2$

$\text{Tr} = -a_{n-1}$

$\det = (-1)^n a_0$

$\text{Tr}(\alpha) = -a_{n-1} = \sum$ roots of polynomial $= \sum$ conjugates of α

$N(\alpha) = \pm a_0 = \prod$ roots of polynomial

if $L \neq K(\alpha)$, $\quad K \subseteq K(\alpha) \subseteq L$

Then $\mathrm{Tr}_L(\alpha) = \mathrm{Tr}_{K(\alpha)}(\alpha) \times [L : K(\alpha)]$

$[L : K(\alpha)]$

$N_L(\alpha) = N_{K(\alpha)}(\alpha)$

For Galois Extensions w/ $\mathrm{Gal}(L/K) = G$,

$$\mathrm{Tr}(\alpha) = \sum_{\sigma \in G} \sigma(\alpha),$$

$$N(\alpha) = \prod_{\sigma \in G} \sigma(\alpha).$$

Applications: Integers of Quadratic Fields.

Suppose K is a finite extension of $\mathbb{Q}$. "$K = \mathbb{Q}[i]$"

An alg integer in K is element of K s.t. (1) minimal polynomial is $x^{n-1} + \underbrace{a_{n-1}x^{n-1} + \cdots + a_0}_{a_i \in \mathbb{Z}}$, (2) α maps some $\mathbb{Z}$-module to itself.

(1) $\Rightarrow$ (2): Take $\mathbb{Z}$-module to be spanned by $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$

$\alpha(\alpha^{n-1}) \in$ space spanned by $1, \ldots, \alpha^{n-1}$.

(2) $\Rightarrow$ (1): Exercise

(2): Alg integers are closed under $+, -, \times$ (same proof as for alg. numbers)

Problem: Find Alg. Ints. in $\mathbb{Q}[\sqrt{-2}]$: $\mathbb{Z}[\sqrt{-2}]$: $x^2 + 2$

$\mathbb{Q}[\sqrt{-3}]$: ~~$\mathbb{Z}[\sqrt{-3}]$~~ There are more!

$\frac{\sqrt{-3}-1}{2} = \omega$, $\omega^2 + \omega + 1 = 0$ so algebraic.

Problem: find all alg. integers of $\mathbb{Z}[\sqrt{-3}]$.

Suppose α is alg. $\mathrm{Tr}(\alpha)$, $N(\alpha)$ are both algebraic, rational

so are integers

Suppose $\alpha = x + y\sqrt{-3}$, $x, y \in \mathbb{Q}$. Then $\mathrm{Tr}(\alpha)$ is integer

$= 2x$ so $2x \in \mathbb{Z}$

So can add multiple of $\frac{-1+\sqrt{-3}}{2}$ to α to make $x = 0$

$\alpha = y\sqrt{-3}$, $\quad N(\alpha) = 3y^2 \in \mathbb{Z}$ (if $x = 0$)

$\Rightarrow y \in \mathbb{Z}$ so alg integers in $\mathbb{Q}[\sqrt{-3}]$ gen by $\frac{-1+\sqrt{-3}}{2}$.

Discriminant of L/K:

L (as vector space over K) has a Symmetric Bilinear Form given by:

$(\alpha, \beta) = \mathrm{Tr}(\alpha\beta)$.

Example: ($\mathbb{C}/\mathbb{R}$) Obvious Bilinear Form, $(1,1)=1$ $(i,i)=1$, $(1,i)=0$

Norm gives Quadratic form $N(1)=1$ $N(i)=(i,i)=1$ $(1,i)=0$

$\mathrm{Tr}(\alpha\beta)$ & $\mathrm{Tr}(1,1)=2$, $\mathrm{Tr}(i,i)=-2$

↑ indefinite

Problem: Is this BLF non-degenerate?

Yes: $(a, a^{-1}) = \mathrm{Tr}(a\,a^{-1}) = \mathrm{Tr}(1) \neq 0$ True in char 0 $= [L:K]$

look at $L = K(t)$, $K = k(t^p)$ char $k = p > 0$.

rational functions

$\mathrm{Tr}(1) = p = 0$, $\mathrm{Tr}(t) = 0$, since t is root of $x^p - t^p = 0$.

$\mathrm{Tr}(\alpha) = 0$ $\forall\ \alpha \in L$.

Theorem: If L/K is Galois (separable as well if char $= p > 0$) then

(1) Tr is not identically 0

(2) BLF is non-degenerate.

Artin's Lemma: Suppose G is monoid. Character of G is homomorphism from G to L^*. Artin's thm: Characters are independent.

If $\sigma_1, \ldots, \sigma_n$ are distinct characters,

$a_1\sigma_1(g) + \cdots + a_n\sigma_n(g) = 0$ for all $g \in G$

Then all $a_i = 0$.

Proof: Take n minimal w/ non-trivial relation.

Change g to gh so

① $a_1\sigma_1(gh) + a_2\sigma_2(gh) + \cdots = 0$

② $a_1\sigma_1(g)\sigma_1(h) + \cdots = 0$

Pick h s.t. $\sigma_1(h) \neq \sigma_2(h)$

$\sigma_1(h)$ ① $-$ ② : $a_2\sigma_2(g)\underbrace{(\sigma_1(h) - \sigma_2(h) + \cdots)}_{\text{non zero}} = 0$

so smaller relation, contradiction.

Trace matters for L/K Galois.

$$Tr(\alpha) = \sigma_1(\alpha) + \sigma_2(\alpha) + \cdots + \sigma_n(\alpha)$$

Take $G = L^*$. σ_i are homomorphisms from G to L^*. so characters of $G\ (= L^*)$

If $Tr(\alpha) = 0$ $\forall \alpha$, then gives linear relation between $\sigma_1, \ldots, \sigma_n$, impossible by Artin's lemma.

Discriminant of L/K. = discriminant of Bilinear form $Tr(\alpha\beta)$.

Recall discriminant of sym bilin form: Pick base $v_1, \ldots, v_n$

look at $\text{disc} = \begin{vmatrix} (v_1, v_1) & (v_1, v_2) & \cdots & (v_1, v_n) \\ \vdots & & & \vdots \\ (v_n, v_1) & \cdots & \cdots & (v_n, v_n) \end{vmatrix}$, (not well defined, depends on choice of basis)

For basis $w_1, \ldots, w_n$, $\text{disc}(w_1, \ldots, w_n) = \text{disc}(v_1, \ldots, v_n) \cdot (\det(T))^2$

where $T: v_i \to w_i$.

It is well defined modulo squares! in $K^*/(K^*)^2$.
↑ subgroup of squares.

Application: look at $x^3 + x + 1$, $x^3 - x + 1$.

Extensions: $\mathbb{Q}(\alpha)$, $\mathbb{Q}(\beta)$ of $\mathbb{Q}$, α, β are roots.

Is $\mathbb{Q}(\alpha) \cong \mathbb{Q}(\beta)$? No, look at disc:

disc of $x^3 + x + 1 = -4b^3 - 27c^2 = -4 - 27 = -31$ } not the same in $\frac{\mathbb{Q}^*}{(\mathbb{Q}^*)^2}$.
disc of $x^3 - x + 1 = \quad = 4 - 27 = -23$

Theorem: Suppose F is an irreducible poly, $x^n + d_{n-1}x^{n-1} + \cdots + d_0$

root α. $\frac{K[\alpha]}{K}$ Disc of this $=$ disc of $\prod_{i<j} (\alpha_i - \alpha_j)^2$

$\det Tr(v_i v_j)$

Vandermonde:

$$\begin{vmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \cdots & \cdots & \alpha_n^2 \\ \vdots & & & \\ \alpha_1^{n-1} & \cdots & \cdots & \alpha_n^{n-1} \end{vmatrix} = \pm \prod_{i<j} (\alpha_i - \alpha_j)$$

poly in $\alpha_1, \ldots, \alpha_n$ degree $\frac{(n-1)n}{2}$

so $\begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \cdots & \cdots & \\ \vdots & & & \end{pmatrix} \times \begin{pmatrix} 1 & \alpha_1 & \cdots \\ 1 & \alpha_2 & \cdots \\ \vdots & & \end{pmatrix} = \begin{pmatrix} Tr(1\cdot 1) & Tr(1\cdot\alpha_1) & \cdots \\ \vdots & & \end{pmatrix}$

12/3/19 : Consider L/K, $N(\alpha) = \det$, $Tr(\alpha)$ Trace of linear map $\beta \mapsto \alpha\beta$, $L \to L$.

$N \in \mathrm{Hom}(L^*, K^*)$:

Ex: • For $\mathbb{C}/\mathbb{R}$, $N(\alpha) = |\alpha|^2$, $\alpha = x+iy$, $\mathbb{C}^* \longrightarrow \mathbb{R}^*$, $\alpha \longmapsto |\alpha|^2$ Image is $\mathbb{R}^+$

• For $\mathbb{Q}[i]/\mathbb{Q}$, $N(x+iy) = x^2+y^2$, Image: rationals that are sums of 2 squares.

• Given L/K, what is $\mathrm{Im}(L^*)$ in K^* (under N), i.e. what is the group $K^*/N(L^*)$?

Easy case: L/K are finite fields.

Answer: All of them, the norm is onto.

Proof. Galois Group of L/K, L, K finite.

$|K| = q$ (prime power)

$|L| = q^n$, $n = [L:K]$.

Obvious element of Galois Group: $F : (\alpha) = \alpha^q$

$\alpha \longmapsto \alpha^p$ is endomorphic for field of characteristic p

$\alpha = \alpha^q$ for all $\alpha \in K$.

Fixed Field of F on L is K.

So Galois Group of L/K is generated by F.

and $F^n(\alpha) = \alpha^{q^n} = \alpha$ so F has order n. ✓ L/K is always Galois

Finite Fields are easy → So $\mathrm{Gal}(L/K) = \mathbb{Z}/n\mathbb{Z}$, generated by $(\alpha \longmapsto \alpha^q)$.

Recall

$$N(\alpha) = \prod_{\sigma \in G} \sigma(\alpha) \quad , \text{ where } \alpha \in L/K, \quad G = \mathrm{Gal}(L/K).$$

For finite fields, $N(\alpha) = \alpha \times \alpha^q \cdot \alpha^{q^2} \times \cdots \times \alpha^{q^{n-1}}$

$$= \alpha^{1+q+\cdots+q^{n-1}}$$

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

$$= \alpha^{\frac{q^n-1}{q-1}}$$

How many elements of norm 1? (Solve $\alpha^{\frac{q^n-1}{q-1}} = 1$)

At most $\frac{q^n-1}{q-1}$ solutions...

Hierarchy of Fields

Finite Fields

Local fields: $\mathbb{R}$, $\mathbb{C}$, p-adic

Global fields: $\mathbb{Q}[i]$

Consider $1 \longrightarrow$ (Elements of Norm 1) $\longrightarrow L^* \xrightarrow{N} K^*$

# of elements : $\frac{q^n-1}{q-1}$ $\quad q^n-1$ $\quad q-1$

So image of norm has $\geq \dfrac{q^n-1}{\left(\frac{q^n-1}{q-1}\right)} = q-1$

So the map is onto.

Thus, (1) $N: L^* \longrightarrow K^*$ is onto, and (2) $N(\alpha)=1 \iff \alpha^{\frac{q^n-1}{q-1}} = 1$.

$\iff \mathrm{ord}_{L^*}\alpha \mid \frac{q^n-1}{q-1}$

Hilbert's Theorem 90:

Suppose L is a cyclic extension of K. Then $N(\beta)=1$ iff $\beta = \alpha/\sigma(\alpha)$, where $\alpha \in L$, σ generator of $\mathrm{Gal}(L/K)$.

[if $[L:K]=p$, $L \neq$ char p, K contains p^{th} roots of 1, $L = K[\alpha^{1/p}]$ some $\alpha \in L$]

Proof. Think of $\beta\sigma$ as a linear transformation from $L \longrightarrow L$ (L is a vector space over K). Want to solve: $\beta\sigma(\alpha) = \alpha$.

$\iff$ α is an eigenvector w/ eigenvalue 1.

How to find fixed point α of $\beta\sigma$? Pick $\theta \in L$, form

$\alpha = \theta + \beta\sigma\theta + (\beta\sigma)\theta^2 + \cdots = \sum_{g \in G} g\theta$.

Problem: α might be 0! (crux of the problem)

α is not always 0 by artin's lemma: $1, \beta\sigma, \ldots$ are linearly independent, so $1 + \beta\sigma + (\beta\sigma)^2 + \cdots \neq 0$, so must be non-zero on some θ. □

Ex: L/K is cyclic, $[L:K]=p$, K contains a nontrivial pth root of 1. ζ

Then $N(\zeta) = \zeta \cdot \sigma(\zeta) \cdots \sigma^{p-1}(\zeta) = \zeta^p = 1$, so by HT 90, $\zeta = \alpha/\sigma\alpha$ so $\sigma\alpha = \zeta\alpha$ so $\alpha^p \in K$, so $L = K[\alpha^{1/p}]$

Explicit Solution of Cubic: Solve $x^3 + x + 1 = 0$

$\mathbb{Q}((1+i)\varepsilon,\ i\varepsilon^2,\ (1-\zeta)\varepsilon^3)$

$x^3+bx+c=0$, Galois Group $\leq S_3$ $\quad 1 \underset{3}{\leq} A_3 \underset{2}{\leq} S_3$

Roots α,β,γ

$\mathbb{Q}(\alpha,\beta,\gamma) \overset{3}{\geq} L \overset{2}{\geq} \mathbb{Q}$

↑ Things fixed by A_3 $\quad \alpha \to \beta \to \gamma \to \alpha$

L is generated by some poly. in α,β,γ fixed under A_3 but not S_3.

$\Delta = (\alpha-\beta)(\beta-\gamma)(\gamma-\alpha)$, $\Delta^2 = (\alpha-\beta)^2(\beta-\gamma)^2(\gamma-\alpha)^2 \in \mathbb{Q}$ fixed by S_3,

$= -4b^3 - 27c^2$.

So $\Delta^2 = -4 - 27 = -31$.

Now, find α,β,γ by taking $\sqrt[3]{\ }$ something in L:

Look for eigenvectors of σ, σ is element of order 3 of Gal

Throw in cube root of 1. $\quad \mathbb{Q}[\omega,\alpha,\beta,\gamma] \geq L[\omega] \geq \mathbb{Q}[\omega] \quad \omega^3 = 1$,

$\sigma(\alpha)=\beta \quad \sigma(\beta)=\gamma \quad \sigma(\gamma)=\alpha$

Eigenvalues of σ : $1, \omega, \omega^2$, $\quad 1: x+\sigma x+\sigma^2 x$, $\quad \alpha+\beta+\gamma = 0$ ✓ symmetric

$\omega: x + \omega^{-1}\sigma x + \omega^{-2}\sigma^2 x \qquad \alpha+\omega^{-1}\beta+\omega^{-2}\gamma = y$

$\omega^2: x + \omega\sigma x + \omega^2\sigma^2 x \qquad \alpha+\omega\beta+\omega^2\gamma = z$

So y^3, z^3 fixed by σ, so in $L(\omega)$

y^3+z^3, $y^3z^3 \in \mathbb{Q}$.

$y^3+z^3 = -27c \qquad y^3z^3 = -27b^3 \qquad x^3+bx+c=0$

algebra w/ symmetric functions

y^3, z^3 are now roots of quadratic, $\in L(\omega)$

$\Rightarrow y^3 = \frac{27}{2}c + \frac{3\sqrt{3}i}{2}S$, $S = \sqrt{-4b^3-27c^2}$

$z^3 = \frac{27}{2}c - \frac{3\sqrt{3}i}{2}S$

$\alpha = \frac{y+z}{3}$, x^3+x+1, $S = \sqrt{-31} = 5.57i$ $\quad y = -3.04$, $z = .99$

$\alpha = -.68\ldots$

Sketch for Degree 4 case:

$x^4 + bx^2 + cx + d = 0$, Gal group $\leq S_4$ — first solve some cubic

$S_4/(\mathbb{Z}/2\mathbb{Z})^2 = S_3$

$1 \leq \mathbb{Z}/2\mathbb{Z} \leq (\mathbb{Z}/2\mathbb{Z})^2 \leq A_4 \leq S_4$

$\sqrt{a}$ (deg 2) $\quad \sqrt{m}$ (deg 2) $\quad \| \quad \sqrt[3]{t}$ (deg 3) $\quad \sqrt{v}$ (deg 2)

L (roots of poly)

$\mathbb{Q}[\sqrt[3]{1}, \sqrt{1}, \sqrt[4]{1}, \alpha, \beta, \gamma, \delta]$, Put L = fixed field by $(\mathbb{Z}/2\mathbb{Z})^2$

What is L generated by? Find Polynomials $\alpha, \beta, \gamma, \delta$ fixed by $(\mathbb{Z}/2\mathbb{Z})^2$

$\alpha \to \beta, \ \gamma \to \delta$

$\alpha \to \gamma \quad \beta \to \delta$

$\alpha \to \delta \quad \beta \to \gamma$

$y_1 \quad (\alpha + \beta - \gamma - \delta)^2 \in L$

$y_2 \quad (\alpha + \gamma - \beta - \delta)^2 \in L$

$y_3 \quad (\alpha - \delta - \beta - \gamma)^2 \in L$

y_1, y_2, y_3 permuted by $S_3 = S_4/(\mathbb{Z}/2\mathbb{Z})^2$

so are roots of some cubic w/ coefficients in $\mathbb{Q}$.

$\Rightarrow y^3 - 2by^2 + (b^2 - d)y + c^2 = 0$

So (1) Solve cubic

(2) Find $\sqrt{y_1}, \sqrt{y_2}, \sqrt{y_3}$ so $\alpha + \beta + \gamma + \delta = 0$

$\alpha + \beta - \gamma - \delta$

$\alpha - \beta + \gamma - \delta$

$\alpha - \beta - \gamma + \delta$

$\alpha, \beta, \gamma, \delta$ are linear combinations of these.

GALOIS COHOMOLOGY: Motivation, suppose G is a group (Galois group $\mathrm{Gal}(L/K)$ / number fields) G acts on things: L, L^*, p-adic fields, adeles, ideles.

Problem: Suppose G acts on X. What is X^G? = Largest submodule of X on which G acts trivially.

What is X_G, largest quotient module on which G is trivial

$= \dfrac{X}{(\text{all things of form } x - gx,\ x \in X, g \in G)}$

Suppose $0 \to A \to B \to C \to 0$ is exact.

is $0 \to A^G \to B^G \to C^G \to 0$ exact? No.

$0 \to A_G \to B_G \to C_G \to 0$ exact?

$0 \to \mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$

$G = \mathbb{Z}/2\mathbb{Z}$ on $\mathbb{Z}$: $0 \to 0 \to 0 \to \mathbb{Z}/2\mathbb{Z} \to 0$ ✗ (Fixed Points)

(G acts as -1; not exact)

on $\mathbb{Z}, \mathbb{Z}$: $0 \to \mathbb{Z}/2\mathbb{Z} \xrightarrow{\times 2} \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$ ✗ (quotients)

(not exact)

Galois Cohomology: What is obstruction to these sequences being exact?

Overview:

$H_0(X) = X_G$ (zero'th Homology)

$H^0(X) = X^G$ (zeroth Cohomology)

Galois cohomology constructs groups $H_i(X)$, $H^i(X)$, $i \in \mathbb{N}_0$

($H_i(X)$: Homology Groups; $H^i(X)$: Galois Cohomology Groups)

G-modules

If $0 \to A \to B \to C \to 0$ is exact, so is

$0 \to H^0(A) \to H^0(B) \to H^0(C) \to H^1(A) \to H^1(B) \to H^1(C)$

$\cdots \leftarrow H^2(C) \leftarrow H^2(B) \leftarrow H^2(A)$

$H_1(C) \to H_0(A) \to H_0(B) \to H_0(C) \to 0$

$H_1(B) \leftarrow H_1(A) \leftarrow \cdots$

↑ LONG exact sequences.

How do we define H_i, H^i? Turn it into ring theory.

Group acted on by G = $\mathbb{Z}[G]$ module ($\mathbb{Z}[G]$ = group ring)

what is A^G, A_G? $A^G = \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, A)$

$\mathbb{Z}$ is $\mathbb{Z}[G]$ module on which $\mathbb{Z}$ acts trivially

$A_G = \boxed{\mathbb{Z} \otimes_{\mathbb{Z}[G]} A}$

$\mathrm{Tor}_2(G,M)$

$\mathrm{Tor}_1(G,M)$

$\mathrm{Tor}_1(B,M)$

Hom and $\otimes$ are not exact. For any module over ring R,

$0 \to A \to B \to C \to 0$, M,

$\mathrm{Tor}_1(A,M) \to A \otimes M \to B \otimes M \to C \otimes M \to 0$ exact

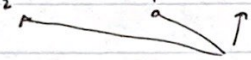
long exact. (↑ not injective)

What is $\mathrm{Tor}_i(A, M)$?

Definition:

(1) Take free resolution of M

$$\cdots \longrightarrow F_2 \longrightarrow F_1 \longrightarrow F_0 \longrightarrow 0$$



free modules, Exact.

(2) Tensor w/ A,

$$\cdots \longrightarrow A \otimes F_2 \longrightarrow A \otimes F_1 \xrightarrow{f} A \otimes F_0 \longrightarrow 0 \quad \text{not exact.}$$

(3) Take Homology (Failure to be exact)

$$\frac{\ker(A \otimes F_1 \longrightarrow A \otimes F_0)}{\mathrm{Im}(A \otimes F_2 \longrightarrow A \otimes F_1)} = \mathrm{Tor}_1(A, M)$$

Galois Cohomology: 12/5/19

$H^0(M) = M^G$, $H_0(M) = M_G$ (3) $H^i(M) = H_i(M) = 0$ if $i > 0$, M is free as a $\mathbb{Z}$-module

u1

Cheat: Only care about H^1 for this course:

- H^1 given as follows: $\frac{Z^1(M)}{B^1(M)}$

  - $Z^1(M)$ are crossed homomorphisms $G \to M$
  - $B^1(M)$ crossed principal homomorphisms $G \to M$

Crossed Homomorphism $G \to M$: taking $\sigma \longrightarrow a_\sigma$ such that $a_{\sigma\tau} = a_\sigma + \sigma a_\tau$. f additive (charge if M_x).

Suppose action of G on M is Trivial: $\sigma(m) = m \quad \forall m$

$\Rightarrow a_{\sigma\tau} = a_\sigma + a_\tau$, so is a homomorphism from $G \to M$.

Principal Crossed Homomorphism: $a_\sigma = b - \sigma b$ for some fixed $b \in M$

G acts trivially: $a_\sigma = 0$, so if G trivially acts on M, $H^1(G, M) \cong \mathrm{Hom}(G, M)$

- If $0 \to A \to B \to C \to 0$ exact, so is

$$0 \to H^0(A) \to H^0(B) \to H^0(C) \to H^1(A) \to H^1(B) \to H^1(C)$$

Pick $c \in H^0(C)$ (so c fixed by G). Lift c to $b \in B$ (b need not be fixed) Dr $b \neq \sigma b$. Define $\dagger$ homomorphism $a_\sigma = b - \sigma b$ ($a_\sigma \in H^1(A)$). This does not depend on choice of b, since it only varies by a principal crossed homomorphism.

- Check if Exact "EXERCISE"

Theorem: Suppose L/K is a finite galois extension, $G = \mathrm{Gal}(L/K)$.

(1) $H^1(G, L^*) = 1$.

(2) $H^i(G, L) = 0$ if $i > 0$.

↳ L is a free module over $\mathbb{Z}G$, Normal Basis Theorem

↳ $H^2(G, L^*) \neq 1$ in general, Relative Brauer Group.

Proof (1): We have elements $a_\sigma \in L^*$ for $\sigma \in G$, where

$a_{\sigma\tau} = a_\sigma \cdot \sigma(a_\tau)$.

Meaning: Look at $F(\sigma) = a_\sigma \cdot \sigma$: a linear transformation from $L \to L$.

(↑ action of σ on L)

$\Rightarrow F(\sigma\tau) = F(\sigma)F(\tau) \iff a_{\sigma\tau} = a_\sigma \cdot \sigma(a_\tau)$

"meaning of 1-cocycle condition"

WTS a_σ is principal: $a_\sigma = b/\sigma b$ for all b, so find b.

$\Rightarrow a_\sigma \cdot \sigma b = b$

twisted action, $\Rightarrow b$ fixed under ↑

$\iff F(\sigma) b = b$ for all σ.

Want to find fixed point of twisted action.

Fixed Points: Try $\beta = \sum_{\sigma \in G} F(\sigma) a$, $a \in L^*$

fixed by twisted action, and need $\beta \neq 0$, which is true for some a by Artin's lemma.

Examples of $H^1(L) = 0$.

(1) Suppose L/K is Galois, $G = Gal(L/K)$ cyclic of order p.

Suppose $\zeta_p \in L \neq 1$. Then if $G = \langle\sigma\rangle$, $\sigma^p = 1$, then put $a_{\sigma^i} = \zeta^i$ (check this is crossed)

$H^1(L) = 1$, so is principal, $a_\sigma = b/\sigma b$ for some b

~~(2) Let L = Algebraic Number~~ $\Rightarrow \sigma b = \zeta b \Rightarrow b^n \in K$ so $L = K(\sqrt[n]{b})$

(2) L = Alg. number field (L/K Galois)

$$1 \to L^* \to I^* \to I_L \to 1$$

(Idele Group ↑, Idele Class Group ↑)

Acted on by $G = Gal(L/K)$, what is I_L^G?

$$1 \to H^0(L^*) \to H^0(I^*) \to H^0(I_L) \to H^1(L^*) \to \cdots$$

$$1 \to K^* \to I_K \to I_L^G \to H^1(L^*) \to$$

($H^0(I^*) = I_K$, $H^0(I_L) = I_L^G$, $H^1(L^*) = L$)

So $I_L^G = Im(I_K)$

INFINITE EXTENSIONS

Ex: alg. (1) $F_p \leq \bar{F}_p$ (alg closure of F_p)

(2) $\mathbb{Q} \leq \bar{\mathbb{Q}}$ (" " $\mathbb{Q}$)

trans (3) $K \leq K(t)$ (rational functions over K)

$K \leq L$ is algebraic if all elements of L algebraic over K.

transcendental if no elements of L algebraic over K (other than K)

purely transcendental if $L \cong K(t_1, t_2, \ldots)$ rational functions in $t_1, t_2, \ldots$

i.e. no relations

Given $K \leq M$, can find L with $K \leq L \leq M$ (alg; purely trans; Zorn's Lemma)

Proof: Take maximal set of alg. independent elements $t_1, t_2, \ldots$ of M and let $L = K(t_1, t_2, \ldots)$

Warning: L is not Unique

$K \leq K(t) \leq K(t)$

$K \leq K(t^2) \underset{2}{\leq} K(t)$

The number of independent generators of $L = K(t_1, \ldots)$ is independent of L "Transcendence Degree of L/K"

Suppose $t_1, t_2, \ldots$ and $s_1, s_2, \ldots$ 2 max alg. ind sets (assume finite)

s_1 depends algebraically on $t_1, t_2, \ldots$ as $t_1, t_2, \ldots$ is maximal.

$f(s_1, t_1, t_2, \ldots) = 0$ for some f (must involve some t_i)

Now choose $(s_1, t_2, t_3, \ldots)$ is new basis.

Continue like This.

Application: Classify Alg. Closed Fields M.

Characteristic $= 0$ or $p > 0$.

so field contains either $\mathbb{Q}$ or F_p

$\mathbb{Q} \leq M$ or $F_p \leq M$

$\underbrace{\mathbb{Q} \leq L}_{\text{p.t.}} \underbrace{\leq M}_{\text{alg}}$ or $F_p \leq L \leq M$

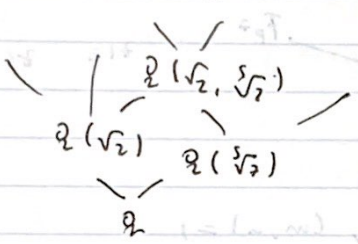
Thus $M = \bar{L}$, $L = \mathbb{Q}(t_1, t_2, \ldots)$ or $F_p(t_1, t_2, \ldots)$ determined by $\mathbb{Q}$ or F_p, number of generators

So M determined by (1) Characteristic and (2) Transcendence Degree

Example $\mathbb{C}$: Char 0, $\mathbb{C}$ = cardinality of continuum

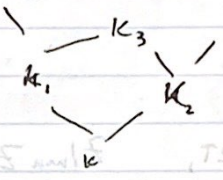
L/K Infinite extension, Algebraic, Separable, Normal,

$L = \bigcup_{\text{Directed}}$ Finite Extensions $\bar{\mathbb{Q}}$



Take $L = \bigcup_{\text{Div}}$ Finite Galois Extensions of K contained in Galois one

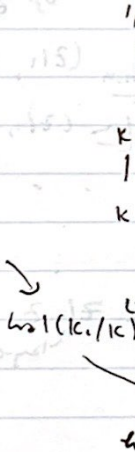
What is $\underline{Gal(L/K)}$ acts on $Gal(K_1/K)$, $\underline{Gal(K_2/K)}$ Finite Groups



finite

We get map $Gal(L/K) \longrightarrow \prod Gal(K_i/K)$

NOT an isomorphism since



must have $\text{Im} \cdots \sigma \in Gal(K_1/K)$

must be τ

~~We get $Gal(K/K)$~~

An element of $Gal(L/K)$ is same as compatible choice of elements of $Gal(K_i/K)$

= inverse limit of $Gal(K_i/K)$

restriction maps

Do subfields of L/K correspond to subgroups of $Gal(L/K)$? No ☹

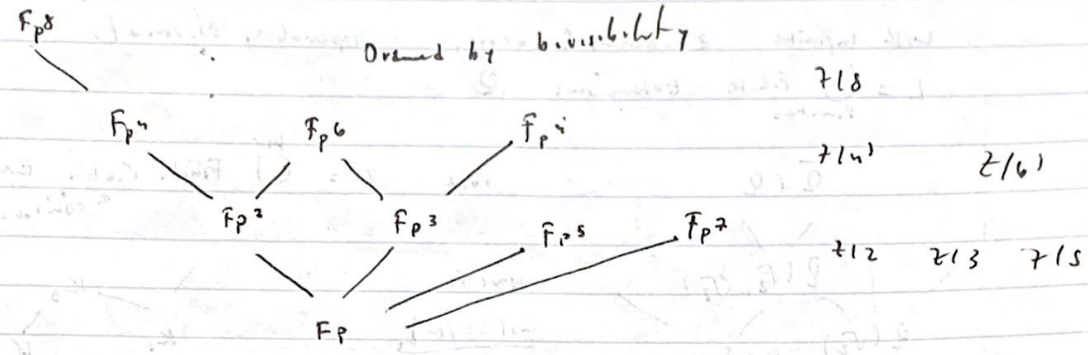
↑ Has a topology

Take $\prod Gal(K_i/K)$ has Product Topology,

$Gal(L/K) \leq \prod Gal(K_i/K)$, subfields of L/K correspond to closed subgroups of $Gal(L/K)$.

Examples: $Gal(\bar{F}_p / F_p)$?

Finite Extensions are $F_p \subseteq F_{p^n}$, Gal group $\mathbb{Z}/n\mathbb{Z}$.



By CRT, $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, $(m,n)=1$

$\Rightarrow \varprojlim$ All finite quotients of $\mathbb{Z}$

$(\mathbb{Z}/2^n\mathbb{Z}) \times (\mathbb{Z}/3^n\mathbb{Z})$

$\mathbb{Z}/8\mathbb{Z}$
$\mathbb{Z}/4\mathbb{Z}$
$\mathbb{Z}/12\mathbb{Z} - \mathbb{Z}/6\mathbb{Z}$
$\mathbb{Z} - \mathbb{Z}/3\mathbb{Z} - \mathbb{Z}/9\mathbb{Z}$

$\hat{\mathbb{Z}} = \varprojlim (\mathbb{Z}/1, \mathbb{Z}/2, \mathbb{Z}/4, \ldots$
$\times \varprojlim (\mathbb{Z}/1, \mathbb{Z}/3, \mathbb{Z}/9, \ldots$
$\times \ldots$
$\times \ldots$
$\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$
n large

$\hat{\mathbb{Z}} = \prod_{p \text{ prime}} \mathbb{Z}_p = Gal(\bar{F}_p / F_p)$

Profinite completion ($\hat{G} = \varprojlim \prod G/H$)
of $\mathbb{Z}$.

Try to describe $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$: Very Hard "Langlands Program"